ISSN 2686-9136 (Online)

DIGITAL LAW JOURNAL

Vol. 6, No. 2, 2025

DIGITAL LAW JOURNAL

DIGITAL LAW JOURNAL

Journal of research and practice

Published since 2020
4 issues per year

Vol. 6, No. 2, 2025

ЦИФРОВОЕ ПРАВО

Научно-практический журнал

Журнал издается с 2020 г.
4 выпуска в год

Том 6, № 2, 2025

Contents

Essays

Articles

Review Articles

Содержание

Эссе

Статьи

Обзорные статьи

DIGITAL LAW JOURNAL

AIMS AND SCOPE

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

The journal establishes the following objectives:

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

The journal publishes 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

Founded:	The journal has been published since 2020
Frequency:	4 issues per year
DOI Prefix:	10.38044
ISSN online:	2686-9136
Mass Media Registration Certificate:	ЭЛ № ФС 77-76948 of 9 Oct. 2019 (Roskomnadzor)
Distribution:	Content is distributed under Creative Commons Attribution 4.0 License
Editorial Office:	76, ave. Vernadsky, Moscow, Russia, 119454, +7 (495) 229-41-78, digitallawjornal.org, dlj@digitallawjournal.org
Published online:	30 June 2025
Copyright:	© Digital Law Journal, 2025
Price:	Free

REGION GROUP OF COMPANIES With support of REGION Group of Companies

ЦИФРОВОЕ ПРАВО

ЦЕЛИ И ЗАДАЧИ

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

Задачами журнала являются:

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

В журнале публикуются 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 экономикой в контексте интеграционных процессов.
9. Комплексные исследования правовых и этических аспектов, связанных с разработкой и применением систем искусственного интеллекта и робототехники.
10. Изменение подходов к подготовке и переподготовке юридических кадров в условиях развития цифровых технологий. Новые требования к навыкам и квалификации юристов.

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

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:	30.06.2025
Копирайт:	© Цифровое право, 2025
Цена:	Свободная

РЕГИОН ГРУППА КОМПАНИЙ При поддержке Группы компаний «РЕГИОН»

https://doi.org/10.38044/2686-9136-2025-6-2-8-27

ESSAYS

CRITICAL VIEW OF THE INTRODUCTION OF ARTIFICIAL INTELLIGENCE IN THE ADMINISTRATIVE PROCEDURE: RECEPTION OF THE EU AI ACT IN ITALY

Michele Di Salvo

National Agency for Artificial Intelligence Foundation
16, Via Giuseppe Revere, Milano, Italy, 20123

Abstract

This article offers a critical examination of Italy's initial legislative efforts to transpose the European Union's Artificial Intelligence Act. Employing a methodological approach of argumentative-critical commentary, the analysis dissects the bill's text to uncover the Italian government's underlying philosophy and regulatory strategy. The study argues that the proposed framework suffers from a significant lack of overall vision, mistakenly treating AI as a non-penetrating technological tool and reducing its risks primarily to data privacy concerns, all while prioritizing industrial growth. The article critiques key provisions, including the ambiguous "anthropocentric" principle, the superficial regulations governing AI in information, healthcare, intellectual professions, and the judiciary, and the creation of new criminal offences. It further analyzes preliminary projects for integrating AI into administrative justice and explores the profound procedural implications of extending AI into areas of technical discretion, highlighting the potential for a paradigm shift in judicial review. By juxtaposing the Italian approach with a documented case of algorithmic discrimination in the UK, the research underscores the concrete risks to fundamental rights and the rule of law. The conclusion emphatically calls for a more technically competent and critically aware involvement from legal scholars and practitioners to safeguard citizens from the uncritical and pervasive adoption of AI in public administration and justice, warning against the shortcomings of the current fragmented and constitutionally superficial regulatory proposal.

Keywords

administrative law, data privacy, AI in justice, algorithmic bias, digital governance, public administration

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Di Salvo, M. (2025). Critical view of the introduction of artificial intelligence in the administrative procedure: Reception of the EU AI Act in Italy. *Digital Law Journal, 6*(2), 8–27. https://doi.org/10.38044/2686-9136-2025-6-2-8-27

Submitted: 8 Apr. 2025, accepted: 30 May 2025, published: 30 June 2025

ЭССЕ

КРИТИЧЕСКИЙ ВЗГЛЯД НА ВВЕДЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В АДМИНИСТРАТИВНЫЙ ПРОЦЕСС В ИТАЛИИ: РЕЦЕПЦИЯ ЕВРОПЕЙСКОГО АКТА ОБ ИИ

М. Ди Сальво

Национальное агентство по искусственному интеллекту
20123, Италия, Милан, ул. Джузеппе Реверe, 16

Аннотация

В данном эссе представлен критический анализ первых усилий Италии по транспонированию европейского Регламента об искусственном интеллекте. Автор анализирует текст законопроекта, чтобы выявить лежащую в его основе философию и регуляторную стратегию итальянского правительства. Исследование доказывает, что предлагаемая правовая рамка страдает от значительного недостатка общего видения, ошибочно трактуя ИИ как неинвазивный технологический инструмент и сводя его риски в основном к вопросам защиты данных, одновременно делая приоритетом стимулирование промышленности. В эссе последовательно критикуются ключевые положения законопроекта правительства, включая неопределенный «антропоцентрический» принцип, поверхностное регулирование использования ИИ в сфере информационных технологий, здравоохранения, интеллектуального труда и правосудия, а также закрепление составов новых уголовных преступлений. Далее анализируются проекты по интеграции ИИ в административное судопроизводство и рассматриваются глубокие процессуальные последствия расширения сферы технического усмотрения. Сопоставляя итальянский подход с задокументированным в Великобритании случаем алгоритмической дискриминации, когда ИИ под влиянием больших статистических данных дискриминирует против отдельных категорий людей, исследование выявляет конкретные риски для прав человека и верховенства права. В заключение автор призывает к более компетентному и критически осмысленному участию правоведов и практиков для защиты граждан от необдуманного и повсеместного внедрения ИИ в государственное управление и правосудие.

Ключевые слова

административное право, конфиденциальность данных, искусственный интеллект в правосудии, алгоритмическая предвзятость, цифровое управление, государственное управление

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

Для цитирования Ди Сальво, М. (2025). Критический взгляд на введение искусственного интеллекта в административный процесс в Италии: рецепция европейского Акта об ИИ. *Цифровое право, 6*(2), 8–27. https://doi.org/10.38044/2686-9136-2025-6-2-8-27

Поступило: 08.04.25, принято в печать: 30.05.25, опубликовано: 30.06.2025

Introduction

This article offers a preliminary examination of how the EU AI Act[1] has been introduced into Italy's legal and administrative system. It analyses Bill No. 1066AS, entitled "Regulations for the development and adoption of artificial intelligence technologies',[2] from a methodological perspective. According to the government, this bill is intended to be the first in a series of measures designed to implement the mandates that must be fulfilled within twelve months.

The analysis proceeds thematically, seeking to understand how the Italian government has interpreted and regulated them, based on the issues addressed in the legislative text. Methodologically, this is therefore an argumentative and critical commentary. Accordingly, the regulatory references are integrated into the text rather than placed in a bibliography, and the analysis is confined to the decree itself, without exploring the individual topics it raises, as each of them would require a separate article, if not a monograph. The aim is to outline from the outset the general level of critical concern, thereby encouraging specialized reflection on each of the specific issues identified both for research and analytical purposes and to suggest possible improvements in the relevant technical domains.

Overall, the analysis reveals a lack of strategic vision. The decree treats AI as a simple, non-invasive technological innovation, reduces risk considerations primarily to privacy, and presents the regulatory process chiefly as a driver of industrial growth.

Neither the form chosen for the text—issued directly by the government rather than examined by an *ad hoc* parliamentary committee with broader participation—nor the adopted solutions, which often reflect the European regulations uncritically and without sufficient detail, address these specific risks in a meaningful way, particularly in the context of a constitutionally oriented rule of law.

Italian Standards or Developing and Adopting Artificial Intelligence Technologies

Italy is a founding member of the European Union and, like all member states, must transpose EU regulations into its own legal system. On 23 April 2024, the Council of Ministers approved Bill No. 1066AS, entitled "Regulations for the development and adoption of artificial intelligence technologies".[3] According to the government, this bill is the first in a series of specific measures to be implemented over the next twelve months.

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (text with EEA relevance), O.J. L, 2024/1689, 12.7.2024, https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[2] Disegno di legge "Norme per lo sviluppo e l'adozione di tecnologie di intelligenza artificiale" [Bill "on the development and adoption of AI technoligies], n. 1066AS, 23 April 2024 https://www.senato.it/service/PDF/PDFServer/BGT/01411729.pdf (It.)

[3] Ibid.

Responsibility for developing artificial intelligence systems is assigned to a strategy prepared by a special unit within the Prime Minister's Office, in cooperation with the national authorities responsible for technological innovation, the Ministry of Enterprise and Made in Italy, and the Ministry of Universities. This institutional design reflects the government's intention to play a central role in the development of AI systems. This is further demonstrated by the decision to entrust *AgID* (*Agency for Digital Italy*) and the *National Cybersecurity Agency*—both technical bodies under the Prime Minister's Office—with applying national and European regulations.

However, the risk is that an overly national approach will clash with Italy's technological and research-investment gap. In the author's view, it would have been preferable for a program that exercises close supervision and coordination of development, while also regulating the use of AI and data management, to be oriented towards specialized collaboration. Concrete models exist: CERN, Airbus, or the European Space Agency, all of which demonstrate effective, efficient, and goal-oriented organizational structures. The not-so-subtle concern is that this process of nationalization and centralization may conceal an eagerness to control and distribute the substantial resources expected to flood the sector, including for patronage and electoral purposes.

The government's strategy for AI development also includes venture capital activities by the Ministry of Enterprise and Made in Italy, involving the acquisition of stakes of up to €1 billion in SMEs operating in new technologies, quantum computing, or telecommunications, and demonstrating high growth potential.

Curiously, the government has chosen to prioritize suppliers operating on Italian territory rather than those more broadly within the European market.[4]

Particularly noteworthy is the definition contained in Article 1 of the Bill on "Provisions and powers delegated to the Government regarding artificial intelligence",[5] which states that the bill aims to promote *"the correct, transparent, and responsible use of artificial intelligence, within an anthropocentric framework, aimed at seizing its opportunities."*

The "Anthropocentric" Approach

This conception of artificial intelligence is articulated in Article 3, which states that the use of this technology must respect the fundamental rights laid down in the Constitution[6] and in European law, as well as the principles of transparency and proportionality of processes, while ensuring the reliability and accuracy of the data used to develop AI systems. Yet, beyond the ambiguity of the term "anthropocentric"—a notion whose meaning is unclear, since every human-made tool is anthropocentric by definition (even the ergonomics of a hammer is designed for human use)—Article 3 raises several concerns.

Substantively, the article's purpose is not clear. Having established that an activity must not be "contrary to the fundamental rights provided for by the Constitution and European law and also to the principles of transparency and proportionality of the processes, reliability and correctness of the data used for the development of artificial intelligence systems," nothing is said about how exactly these rights, which are already established and inalienable, are to be defended, enhanced, and protected.

---

4 Disegno di Legge "Disposizioni e deleghe al Governo in materia di intelligenza artificiale" [Bill "on the Provisions and powers delegated to the Government regarding artificial intelligence"] [D.d.l. Intelligenza artificiale], A. S. 1146, Legislatura XIX, Art. 5. https://www.senato.it/leggi-e-documenti/disegni-di-legge/scheda-ddl?did=59313 (It.).

5 D.d.l. Intelligenza artificiale, A. S. 1146, Legislatura XIX, Art. 1 (It.).

6 Costituzione Italiana [Constitution of the Italian Republic] (It.).

Given that such rights are becoming increasingly shaky, if not reduced to mere statements of principle in an era marked by liberalism and globalization, where the core infrastructures of AI are controlled predominantly by non-European multinationals,[7] it might have been appropriate to dedicate more attention to active, preventive, and precautionary protection measures, rather than simply asserting that "everything must be controlled by the government."

The Bill then goes on to outline a series of principles to be applied across various sectors: information, economic development, healthcare, professional services, the judiciary, user protection, copyright, and, finally, criminal law.

AI and Information

Article 4 addresses the use of AI systems in the information sector, providing for the protection of media pluralism and the democratic nature of the press. It also requires that information on the processing of personal data be clear and accessible to everyone, so that individuals may exercise their right to object to the sharing of their data. However, the remedies, instruments, and mechanisms available for safeguarding these rights are neither specified nor explained. A quick comparison between the speed of AI systems and the sluggishness of Italy's civil justice system perfectly illustrates the inadequacy of the current protections.[8] The real source of uncertainty, however, lies in the lack of clarity regarding the nature of the issue itself.

Artificial intelligence is a system of hyper-computation combined with machine-learning technologies. To function, it must continuously process vast quantities of data. Without such data processing, it is difficult to understand how generative AI could evolve, as these systems obtain data from across the web. Since the most authoritative websites, including major and reputable broadcasters, have restricted access to their content, generative AI models (such as *ChatGPT*) often rely on platforms like *Quora* or *Facebook** as sources. This is not an abstract concern, but a concrete reality.

Against this backdrop, the generic statement in Article 5, which stipulates that companies operating in the sector must be granted access to "high-quality data," is insufficient. The bill does not regulate how such access will be ensured, nor does it define what constitutes "high quality"—a concept that is not easily determined in advance. Moreover, this provision cannot override intellectual property rights, nor violate industrial or research-related copyright protections.[9]

Article 23 provides that, within *regulation of audiovisual services*, subject to the acquisition of consent from rights holders, content created or modified through AI systems "that are capable of presenting as real data, facts and information that are not"[10] must be marked with an appropriate identification mark. This provision responds to the concerns generated by so-called "deepfakes". The obligation of transparency is placed on the author or holder of the rights to such content, although the practical allocation of responsibility will depend on the implementing measures. The insertion of the identifying sign is excluded when the content forms part of a manifestly creative, satirical, artistic, or fictitious work or program, without prejudice to the protections for the rights and interests of

7 D.d.l. Intelligenza artificiale, A. S. 1146, Legislatura XIX, Art. 3 (It.).

8 In Italy civil proceedings on average take 7 years to complete the process.

* Ed. note: By decision of the authorities of the Russian Federation, *Meta Platforms, Inc.* has been declared an extremist organization, and its activities are prohibited on the territory of Russia.

9 The issue is linked to a broader one — too broad to be dealt with here: in order to verify the data, the algorithm would have to be made public, but if the algorithm is made public, private companies claim that this constitutes a violation of industrial property rights.

10 D.d.l. Intelligenza artificiale, A. S. 1146, Legislatura XIX, Art. 23.

third parties. The resolution of doubts as to the manner of implementation is left to self-regulatory and co-regulatory soft-law sources.

The government aims to foster the development of *Italian entrepreneurial fabric*; thus Article 5 stipulates that the state and other public bodies:

- promote the use of AI in production processes to improve human–machine interaction and increase productivity
- foster the development of an innovative and open Italian artificial intelligence market
- ensure that companies operating in the sector have access to high-quality data
- direct the digital procurement platforms used by public administrations so that preference is given to solutions that guarantee the localization and processing of critical data in data centers located throughout the country.[11]

No specific direction emerges, apart from reference to an "anthropocentric model that respects the Constitution." Beyond this, and aside from an explicitly 19th-century form of protectionism, the Bill's primary thrust appears to be the orientation of AI towards the technological transformation of production enterprises.

AI and Health

With regard to healthcare, the use of AI systems must not lead to discriminatory criteria in access to treatment and medical services. The principle of informed consent is reflected in the requirement to inform patients about the use of artificial intelligence systems. This is fine. But all of this is already provided for by general rules consolidated through extensive case law.[12] What is missing is any consideration of how to handle and protect the product generated by this use.

The issue first emerged in relation to metadata. *Google*, paradoxically and dramatically, states the truth when it refuses to provide users with much of the information requested about their own accounts: *Google* does not actually know certain things because once transformed and reassembled, the data becomes an articulated and amorphous metadata set in which the individual is no longer traceable.[13] The essential point was to standardize and protect metadata—a challenge that has not been met. An AI system may certainly require informed consent to acquire the first raw data that originate information, and existing norms already regulate such access.[14]

However, AI is not a cloud in which files are simply stored in separate and recognizable folders. For example, an AI analyzing one million ultrasound scans per month in Italy could decompose the data in multiple ways: a gynecologist might search only for the fetus's vital parameters, but a future AI system could extract macro-data on the microcirculation of the uterine wall. Twelve million scans per year of anonymized data can reveal an enormous amount of information.

Who manages and protects this data, and how? What about the economic dimension, given that pharmaceutical companies, medical device manufacturers, and others could make enormous profits

[11] Ibid., Art. 5.

[12] *See* Cass. Civ., Sez. III [Court of Cassation], 2023, n. 8771; Cass. Civ., Sez. III, 2022, n. 9143; Cass. Civ., Sez. III, 2021, n. 25672; Cass. Civ., Sez. III, 2020, n. 14437; Cass. Civ., Sez. III, 2019, n. 17483; Cass. Civ., Sez. III, 2017, n. 1218; Cass. Pen., Sez. IV, 2016, n. 4631; Cass. Civ., Sez. III, 2015, n. 19669; Cass. Civ., Sez. III, 2014, n. 21911; Cass. Civ., Sez. III, 2013, n. 1353.

[13] This was indicated to the author by *Google* in a personal communication upon inquiring.

[14] In Italy it's Legge "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio" [Law on "Protection of copyright and other rights related to its exercise"], n. 633, 16 July 1941 (It.)

from it? Who is entitled to access this data, or to request that AI analyze it for research purposes? For what objectives?

The problem here is not merely a lack of regulation that could be solved by an amendment. Rather, the issue is that the very nature of what must be regulated is not understood. At the root, it is not even clear what one is talking about.

AI, Intellectual Professions, and Copyright

The regulation of AI use is also crucial in the intellectual professions, where AI systems may be employed only to carry out activities that are instrumental and supportive of the professional task, and where the intellectual work performed by the professional must remain predominant. To preserve the relationship of trust between the professional and the client, information about artificial intelligence systems used must be communicated to the recipient of the service in clear, simple, and comprehensive language.

This immediately raises questions about the meaning to be attributed to *"instrumental and support activities"* and about how to measure the *"prevalence"* required by the rule.[15] It should be recalled that professionals compete with colleagues in other jurisdictions and with service companies that would not be subject to these limitations. The scarcely concealed assumption underlying this framework is that a professional commissioned to write a text merely sits in an armchair, submits a question to ChatGPT, and lets the system do the work. It is the anthropocentrism of a fraudulent human logic.

But how does this apply to designing a bridge or a tunnel, where all the calculations, virtual simulations, 3D processing, and structural analyses, including those of each individual component, are already performed by machine-learning systems with hyper-computational capacity?[16] Because this is already happening.

Since the use of artificial intelligence frequently intersects with user protection in audiovisual and radio services and with *copyright* matters, Article 23[17] of the bill states that any information content broadcast on any type of audiovisual or radio platform that has been entirely created or modified with AI systems must be made recognizable to users by the author or the owner of the economic exploitation rights through an identification sign or an embedded marking with the wording "I.A.".[18] With regard to copyright protection, Article 24 of the bill provides for the amendment of Article 1 of Law No. 633/1941, according to which works of the mind protected by that law also include those created with the use of artificial intelligence, where the human contribution is in any case *"creative, relevant and demonstrable."*[19]

Here again, anthropocentrism yields to a kind of "suspicion of man". Yet clear principles already exist and may be borrowed, for instance, from common-law systems which, for obvious historical reasons, have dealt with relevant cases for much longer. Copyright depends on the *threshold of*

[15] This is a requirement specified in the writ of summons. If this is not indicated, the case will be dismissed.

[16] Bridge Design is a legal-design model aimed at creating a transitional and functional link between an existing regulatory, contractual or factual situation and a new desired structure, overcoming a temporal, regulatory or resource "gap". The objective is to ensure continuity, stability and progressiveness in the transition, avoiding abrupt interruptions or regulatory gaps.

[17] D.d.l. Intelligenza artificiale, A. S. 1146, Legislatura XIX, Art. 23.

[18] Short for "Intelligenza Artificiale" (Artificial Intelligence) in Italian.

[19] Legge "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio" [Law on "Protection of copyright and other rights related to its exercise"], n. 633, 16 July 1941 (It.)

originality based on three assumptions: *skill* (creative competence), *labor* (commitment, work), and *judgement* (the ability to discern, distinguish, and select the distinctive elements of the work).[20]

In extremely concise terms, using this tripartite parameter, which must exist simultaneously, with each element at least equivalent, if not quantitatively comparable, Anglo-American jurisprudence recognizes that works produced with AI systems exhibit *skill and labor*. What is missing is judgement, which belongs exclusively to the human being.

These are principles of common sense, not as excessively flexible as they might seem, yet it appears evident that the authors of the provision failed to grasp the essential point.

Undersecretary Butti has clarified that, in the field of copyright law, competence lies with the EU, and EU rules already regulate the protection of content in cases of web scraping, establishing an opt-out mechanism for rights holders.[21]

The bill introduces two novelties and a reminder. The first novelty is the requirement of an identification mark for any content made or modified with AI. The second is copyright protection for works produced with AI, provided that the human contribution is creative, relevant and demonstrable. And the reminder is a reference to copyright rules on the reproduction and extraction of works or other materials through artificial intelligence models and systems, including generative systems, where permitted for research purposes or when the use of such materials has not been expressly reserved by copyright holders, related rights holders or database owners.

But here, practically speaking, there is nothing new or innovative. This has been expected for 70 years in relation to any printed work and always expressly stated in their disclaimers.

AI and Law

In the judiciary, artificial intelligence systems may be used exclusively for the organization and simplification of judicial work, as well as for jurisprudential and doctrinal research. The Ministry of Justice will regulate the use of artificial intelligence systems by ordinary judicial offices. For other jurisdictions, use will be regulated in accordance with their respective systems. The interpretation of the law, the assessment of facts and evidence, and the adoption of decisions remain the exclusive prerogative of the magistrate. The Civil Court will be the competent body to decide disputes relating to the operation of AI systems.

However, a fundamental uncertainty remains: if AI systems are employed in evidentiary activities, in court-appointed technical assessments (CTUs), in party-appointed technical reports (CTPs), in reconstructions, or in investigative processes, to what extent can the resulting judicial measure be considered "AI-free"? Above all, despite vast academic debate, there is no limitation or reference to criteria governing the programming of algorithms in judicial contexts, particularly for the purposes of verifying potentially discriminatory or prejudicial decision-making.

The government also intervenes **in criminal matters**, penalizing the distorted use of AI systems capable of harming legally protected interests such as the moral integrity of individuals.

A new offence is introduced by Article 612-quater of the Criminal Code, which punishes:

"Whoever, in order to cause damage to a person and without his consent, sends, delivers, assigns, publishes or in any case disseminates his image, video or voice, falsified or altered through the use

[20] The three requirements (skill, labour, and judgement) as the basis for assessing the originality of a work derive from a landmark ruling by the Supreme Court of Canada, which rejected the doctrine of "sweat of the brow" as a sufficient criterion for copyright protection (CCH Canadian Ltd. v. Law Society of Upper Canada, [2004] 1 S.C.R. 339).

[21] Dipartimento per la Trasformazione Digitale. (2024, April 23). *Conferenza stampa del Consiglio dei Ministri del 23 aprile 2024* [Video]. YouTube. https://www.youtube.com/watch?v=dnmckrKC-iM

of artificial intelligence systems and capable of misleading as to their genuineness"[22] with imprisonment of six months to three years, or from one to five years if unfair damage results from the act.

The offence is punishable upon complaint by the injured party, but prosecution proceeds *ex officio* if the act is linked to an offence prosecuted *ex officio*, or if committed against a person incapacitated due to age or infirmity, or against a public authority by reason of the functions exercised. Further aggravating circumstances concerning the use of artificial intelligence are also introduced in Articles 61(*11-novies*), 494 and 501 of the Criminal Code.[23]

More broadly, the use of AI systems becomes an aggravating circumstance for several offences, including substitution of person, fraudulent price manipulation, fraud, computer fraud, money laundering and self-laundering, and market rigging. Copyright protection is extended to cover reproduction or extraction of text or data from works or other materials on networks or in databases in violation of Articles 70-ter and 70-quater, including through AI systems.[24]

In this respect, the measure aligns with a long-standing governmental tradition whereby almost any regulatory intervention, even incidentally, affects criminal law.

Given the particular sensitivity of criminal law, this approach would require greater caution, not least in order to maintain the stylistic rigor of the Criminal Code, the primary instrument for guaranteeing the principle of "knowledge and discernment" of the criminal law as a prerequisite for awareness of wrongdoing.

Yet through the accumulation of bis, ter, quater articles and "x-nonies" paragraphs, the Italian Criminal Code has more than tripled in volume without contributing to a reduction in offences, with the exception of those abolished or converted into administrative violations. Instead, this legislative inflation produces less clarity, reduced intelligibility, and diminished legal certainty. Expanding the Criminal Code increases the risk of conflicts among norms, uncertainty in practical application, overlaps among offences, whether objective or interpretative, and broadens the margins of judicial discretion. These characteristics are ill-suited to Article 27 of the Constitution[25] and incompatible with a penal system that is truly guarantor-oriented, civil, and at least functional, if not effective.

There was no compelling need for Article 612-quater. The conduct could have been typified within Article 612,[26] and if a different penalty range was desired, that provision could have been amended. Treating the use of AI—a tool—as an aggravating element of punishment is more a political manifesto than an effective instrument of criminal policy. It is akin to holding that the crime of massacre under Article 422 of the Criminal Code[27]—one of the few offences without an "attempt" form, since planting a device, even without casualties, constitutes the offence—would be more serious if committed with a bomb rather than a machine gun, and less serious if committed with a pistol.

In criminal law, *which*, let us recall, directly affects personal liberty, the decisive factors should be "the fact" and the resulting harm to the protected right, serving as both aggravating and mitigating elements. Criminal law should be parsimonious, but this would run the serious risk of also becoming clear, certain, and stable, like any self-respecting criminal law.

Yet the entrenched vice of weak politics is to intervene strongly in criminal matters through legislative proclamations: a shortcut for claiming to have taken concrete action. Such concreteness is

22 Article 612-quater Codice Penale [Cod. Pen.] [Criminal Code] (It.).

23 Articles 61(11-novies), 494 and 501 Cod. Pen. [Criminal Code] (It.).

24 Amendment to Law No. 633 of 1941 (Copyright Law)

25 Costituzione Italiana [Constitution of the Italian Republic], Art. 27.

26 Article 612-quater Cod. Pen. [Criminal Code] (It.).

27 Article 422 Cod. Pen. [Criminal Code] (It.).

reified in a few lines of statutory text. And this is not the vice of a single political camp, but a bipartisan legislative habit.

AI in Training, Education, and Research

The bill also provides for the enhancement of customized teaching plans for students with high cognitive abilities through the integration of *AI training*, as well as for the use of AI systems to improve psychophysical well-being through sporting activity, including the development of innovative solutions aimed at greater inclusion of persons with disabilities in sport.

If this has escaped the reader's notice, let us make it explicit: AI is to be used to support customized educational plans for students with high cognitive abilities, whereas for people with disabilities, it is intended to generate innovative solutions for greater inclusion in sporting activities.

Is the underlying cultural model clearer now?

This formulation entirely overlooks decades of groundbreaking studies on the use of AI (today) and information technology (yesterday) for the cognitive development and support of differently abled, and indeed disabled, individuals.

Subject to the general principles set out in the bill, artificial intelligence systems may also be used for the organization of sports activities. With respect to *AI systems and minors*, the government introduces a series of limitations: for minors under 14, parental consent is required. Minors between 14 and 18 may consent to the processing of personal data related to AI use, provided that the information and communications (privacy notices) are easily accessible and understandable *(sic!)*. More generally, information about data-processing must be drafted in clear and simple language to ensure that users are fully aware of, and able to object to, improper processing of their personal data.

However, we were unable to achieve this with *Google*, *Facebook*,* and similar platforms regarding personal data; we completely failed to do so with metadata; and now we expect to apply these principles to AI, which has a computational capacity that is orders of magnitude greater? Clear and simple language is indeed desirable, but such clarity requires at least a basic understanding of the phenomenon in question. Here, that understanding is manifestly absent.

In what clear and simple language should it be explained that your data is taken from you, full stop, and that AI systems ultimately care little about whether they belong to Mario Rossi or Maria Bianchi? Names are merely extraneous elements that burden the process. This data will be broken apart, sifted, recombined, reshaped, and recontextualized. It is like demolishing three houses to construct one new building, using selected pieces while anonymizing their origins. That is how the process should be explained, and precisely how it will not be explained.

Article 8 appears to attempt to remove some of the obstacles imposed by the current legal framework on the use of health data for *scientific research*.[28] Among other things, it allows not-for-profit entities to make secondary use of personal data, including that in special categories, which has already been collected in previous research projects without obtaining additional consent from the data subjects.

Although this text will be debated and amended in Parliament, it already reveals potential incompatibilities with the *provisions of the GDPR*, as well as a regulatory gap concerning scientific research conducted by profit-making organizations. There is also a coordination issue with the provisions on scientific research in healthcare contained in the law converting the so-called PNRR decree,

* Ed. note: By decision of the authorities of the Russian Federation, *Meta Platforms, Inc.* has been declared an extremist organization, and its activities are prohibited on the territory of Russia.

[28] D.d.l. Intelligenza artificiale, A. S. 1146, Legislatura XIX, Art. 8.

which was definitively approved on April 23 (the same day as the approval of the DDL IA), which amends Article 110 of Legislative Decree No. 196/2003 (the Privacy Code).[29] These provisions, among other things, eliminate the obligation of prior consultation with the Garante[30] in cases of processing health-related data without the data subject's consent for medical scientific research.

In short, the minimal safeguard applicable to the most sensitive data is, therefore, effectively circumvented, while any reference to data-management rules for profit-making companies is omitted. Economic development and cybersecurity are presented as areas in which the provision of quality data and its storage in national data centers are valued, but these remain merely principles. Reading the provision multiple times reveals that it is so vague as to be absurd, and so devoid of substance that one cannot even say it is "wrong".

Article 6 then identifies activities carried out with the help of AI systems for purposes of national security and defense, including activities to protect national security in cyberspace, which are excluded from the scope of the bill.[31]

AI and Public Administration

Public administrations (PAs) may use artificial intelligence to increase the efficiency of their activities, reduce the time required to complete procedures, and improve both the quality and quantity of services provided to citizens and businesses, ensuring that users are informed of its operation and able to trace its use. The adoption of each measure remains the responsibility of officials and managers—a responsibility on which no further clarification is provided.

The text of 26 articles stipulates that its implementation, including by public administrations, must be financially neutral. No additional resources are allocated, apart from the one billion euros already earmarked for *CDP Venture Capital* and now differently channeled towards the entrepreneurial system—a sum that, according to the government, should leverage three billion euros of private investment.[32]

"*Italy is the first country to have launched an industrial policy on AI,*" stressed Butti[33]—an emphatic, disproportionate, and technically incorrect statement. The industrial focus is present in all sectoral

[29] The term "PNRR decree" refers to several decree-laws issued to implement the National Recovery and Resilience Plan (Piano nazionale di ripresa e resilienza), in particular those that introduced urgent measures in the areas of employment, education and universities. Among the most recent are Decreto Legge "Disposizioni urgenti in materia di lavoro, università, ricerca e istruzione per una migliore attuazione del Piano nazionale di ripresa e resilienza" [Decree-Law on "Urgent measures concerning employment, universities, research and education for better implementation of the National Recovery and Resilience Plan"], n. 160, 28 October 2024 (It.), and Decreto Legge "Ulteriori disposizioni urgenti in materia di attuazione delle misure del Piano nazionale di ripresa e resilienza e per l'avvio dell'anno scolastico 2025/2026" [Decree-Law on "Further urgent provisions regarding the implementation of measures under the National Recovery and Resilience Plan and the start of the 2025/2026 school year"], n. 45, 7 April 2025 (It.).

[30] The "Garante della Privacy" or Privacy Authority is the Italian independent administrative authority responsible for supervising, enforcing and providing guidance on the application of personal data protection legislation. Its authority derives mainly from 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), which in Article 51 provides for the establishment of independent supervisory authorities in each Member State, and specifically Decreto Legislativo [Legislative Decree], n. 101, 10 August 2018, the updated "Privacy Code", which defines in detail its organisation, powers and procedures.

[31] D.d.l. Intelligenza artificiale, A. S. 1146, Legislatura XIX, Art. 6

[32] D.d.l. Intelligenza artificiale, A. S. 1146, Legislatura XIX.

[33] Dipartimento per la Trasformazione Digitale. (2024, April 23). *Conferenza stampa del Consiglio dei Ministri del 23 aprile 2024* [Video]. YouTube. https://www.youtube.com/watch?v=dnmckrKC-iM

regulations. The real question is whether other ontologically more central aspects have been neglected in order to highlight and emphasize industrial development.

In this respect, it remains to be seen what the Italian Strategy will contain, since only an executive summary has been published so far, despite the fact that the bill dedicates Article 21 to it. The ten-page *AgID* document does, however, contain one revolutionary idea: the creation of a foundation to coordinate activities—that is, a new institution, conceived in the most traditional manner, though admittedly among the most organizationally flexible.

Another aspect of Butti's statement also merits attention: he implies the existence of an industrial policy isolated from resources. Someone should explain to him what industrial policy is and why this assertion is erroneous.

These provisions, as noted earlier, eliminate the requirement for prior consultation of the Garante when processing health-related data for medical scientific research purposes without the consent of the data subject. The real crux of this regulatory framework is the omission of any reference to the management of data by for-profit companies.

These arguments have been criticized by many authors.[34]

AI in Administrative Justice: First Projects and Notes

In October of 2024, the General Secretariat of Administrative Justice published a document outlining ongoing activities related to the introduction of artificial intelligence technologies in administrative justice.[35]

The aim is to provide preliminary information on developments initiated by the Secretariat at a time when interest in the use of these technologies has reached particularly high levels, both due to their spread and technological advancement and as a result of regulatory initiatives at EU and national level.

The document sets out strategies, methodologies and use cases for AI. AI implementation projects in administrative justice concern:

(a) the anonymization of measures
(b) supporting judges' work by searching and displaying content
(c) cyber resilience

On the first aspect, anonymization (a), the document explains the rationale adopted, emphasizing the need to reconcile two values: the confidentiality of the individuals concerned and the intelligibility of the measure, which could otherwise be compromised, including in its reasoning, by unsupervised anonymization.

"Achieving a balance between the two aspects (protection of confidentiality and comprehensibility of the text) in fact presupposes an interpretative activity that can only be carried out by judges,

[34] *See* Di Giacomo, L. (2024, August 6). *Intelligenza artificiale e il diritto: Un binomio in evoluzione*. https://www.diritto.it/intelligenza-artificiale-diritto-binomio-evoluzione/ ; Di Giacomo, L. (2025, June 26). *Disegno di legge n. 1146/2024 (Ddl Intelligenza Artificiale): Ok dalla Camera*. https://www.diritto.it/disegno-legge-n-1146-2024-intelligenza-artificiale/ ; Donini, F. (2024, July 16). *L'intelligenza artificiale ed il sistema di giustizia predittiva*. https://www.diritto.it/intelligenza-artificiale-sistema-giustizia/ ; Magnolo, F. (2025, January 16). *Intelligenza artificiale e copyright: Riflessioni sull'AI act*. https://www.diritto.it/intelligenza-artificiale-copyright-riflessioni-ai/ ; Sorrentino, C. (2025, January 7). *AI e Diritto alla spiegazione nell'uso degli algoritmi decisionali*. https://www.diritto.it/intelligenza-artificiale-diritto-spiegazione-uso/

[35] Segretariato Generale della Giustizia Amministrativa, Servizio per l'Informatica. (2024, October). *Intelligenza artificiale e giustizia amministrativa: Strategie di impiego, metodologie e sicurezza*. https://www.dirittobancario.it/wp-content/uploads/2024/10/Report-Segretariato-Generale-della-Giustizia-Amministrativa-ottobere-2024.pdf

who, at that stage, help to define the intrinsic value to be assigned to each piece of information, also considering its relationship with the context, distinguishing the nature and characteristics of the disputes. Artificial intelligence is thus modelled to suit the variability of the context, to then verify in the course of concrete use, thanks to the feedback received from users (feedback duly verified and administered to the AI itself), the correctness of the results obtained still under the control of judges, who, in this executive phase, monitor the development of the system, i. e. the way it responds to the feedback offered by users, supervising its evolutionary path."[36]

With regard to judicial support activities (b), those activities classified as high-risk under the AI Act are excluded from the scope of AI applications. Instead, the applications included are those intended to facilitate various judicial functions and which, as structured, "do not involve 'creative' activity."

These are, in particular:

- the identification of related or similar appeals pending before individual sections and to be scheduled for decision. As the report specifies, such identification makes it possible to achieve several objectives: optimizing study and analysis; assessing whether to discuss matters in the same hearing or in thematic hearings; avoiding conflicting decisions within individual sections; improving the distribution of workloads; and accelerating decision-making
- the search for case-law precedents using a tool based not only on keywords, as is currently the case, but also on the detection of semantic connections, thereby ensuring a higher degree of relevance in search results
- the detection and immediate visualization of the rules or case-law pronouncements cited, explicitly or implicitly, in a defense document, thus preventing the judge from interrupting the analysis to consult external databases, saving time, and avoiding unnecessary interruptions in concentration

As for cyber resilience, specific defense strategies have been implemented against internationally identified adversarial machine learning techniques. According to the document:

"The guideline followed is that of valorizing the positive impacts that can be derived from technological developments on the organization of work, but with clear attribution to this technology of an instrumental role, of support to the judge in the phase of study, updating and analysis. The processing activity remains exclusively entrusted to the judge. On a conceptual level, it is more appropriate to speak of 'accelerated intelligence' instead of 'artificial intelligence'."[37]

Machine learning models, especially deep learning models (i. e. models that simulate the action of the human brain through multilayer artificial neural networks, such as LLMs—large language models designed for linguistic purposes), are difficult to govern and may give rise to so-called hallucinations or to overfitting when the model adheres too closely to specific training data, or to overgeneralization, when the model extrapolates excessively.

Research in the field, notably at Stanford, has highlighted the difficulty these models encounter in performing legal reasoning, identifying negative impact factors such as a lack of uniformity and the excessive length of legal documents (Dahl et al., 2024). The approach must therefore be cautious: aware of risks, free from bias, yet characterized by critical scrutiny and constant supervision.

---

[36] Segretariato Generale della Giustizia Amministrativa, Servizio per l'Informatica. (2024, October). *Intelligenza artificiale e giustizia amministrativa: Strategie di impiego, metodologie e sicurezza*. https://www.dirittobancario.it/wp-content/uploads/2024/10/Report-Segretariato-Generale-della-Giustizia-Amministrativa-ottobere-2024.pdf

[37] Ibid.

In the Italian legal system in particular, the centrality of a "human" judge is constitutionally mandated: jurisdictional functions are, by the Constitution,[38] entrusted to a judge who is a natural person, pre-appointed by law, an impartial third party, and subject only to the law. Ethical values and the protection of rights cannot be delegated to technology; leadership cannot be automated. These considerations are reflected in the document itself. Nonetheless, the risk remains high due to the combination of uniform formats and AI applications integrated into *SIGA* (the administrative justice information system).

The use of standardized formats is, in itself, at odds with the originality inherent in the intellectual profession of the lawyer; with decorum; and, even more fundamentally, with the function of legal representation, which requires that the lawyer's role not be confined within rigid formal structures that would inevitably impair the effectiveness of the defense.

At a time when legal design is under discussion[39], these concerns require even greater emphasis as regards the format of judgments and legal acts.

A first step must be to guarantee cross-participation in decision-making processes concerning the introduction of AI in the administration of justice. This entails ensuring the participation of lawyers in regulating AI systems; regulating such systems at least through delegated legislation adopted after consultation with specialist legal associations; and involving experts from non-legal disciplines capable of identifying vulnerabilities and weaknesses that fall outside narrow procedural dynamics.

The use of artificial intelligence in administrative procedures should also be better regulated by imposing on public administrations the obligation to justify the recourse to AI as a function of real efficiency and improvement of specific services for citizens and businesses; guaranteeing users the knowability of its operation, the traceability of its use and, more generally, transparency; reserving autonomy and decision-making power to the official adopting the measure and/or to the person responsible for the procedure; and prohibiting the use of artificial intelligence for the generation of texts of any kind.

The subject is particularly delicate, especially in light of the repeal of the offence of abuse of office and the related cases before the Constitutional Court, because essential aspects remain undefined (Di Salvo, 2024b).

Justification of the procedure, an essential and central requirement under Law 241/1990,[40] must be human, specific to the individual measure, not "*per tabulas* or generalized," and must reflect and follow the entire procedural path anchored to the specific factual situation (Di Salvo, 2024a). Today, these intrinsic characteristics exclude the generic formula adopted via copy-paste, and, tomorrow, the mechanical delegation of reasoning to digital automatisms.

If motivation cannot, even when discretionary, devolve into arbitrariness when absent or merely "*per tabulas*," this applies even more strongly in the case of algorithmic decision-making, where the objective weighting of each factor is neither disclosed nor verifiable. Without absolute and verifiable ex-ante transparency, the use of AI should be excluded a priori.

This holds even more firmly with regard to the reasoning of judicial decisions. On the one hand, the integration of AI tools into legal research may be desirable. Indeed, to some extent, they are

[38] Costituzione Italiana [Constitution of the Italian Republic].

[39] Di Salvo, M. (2024, April 10). *Dalla chiarezza dell'atto al legal design*. https://www.diritto.it/dalla-chiarezza-dell-atto-al-legal-design/

[40] Legge "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" [Law on "New regulations governing administrative proceedings and the right of access to administrative documents"], n. 241, 18 August 1990 (It.)

already present in current search engines, which make extensive and often indiscriminate use of such systems. On the other hand, the nontransparent and unverifiable attribution of "weights" to results raises serious concerns: five precedents versus three, how are they weighted? How much weight is assigned to chronology, jurisdiction, or forum? What guarantees exist that arguments are traceable to the specific case? What *ex ante* safeguards against discrimination can be offered in a transparent manner?

These are merely preliminary observations, each of which would merit dedicated analysis involving expertise beyond the strictly legal domain.

Accordingly, the judge must articulate, fully and transparently, all aspects of this weighting process, beyond doubt and subject to verification. And in this sense, it is far from clear that the adoption of such systems will guarantee ex-post efficiency or procedural speed. It is more straightforward for a judge to clarify his own reasoning parameters than to explain those embedded in a programmed system, which may not be his own, and which he is not required to share, thereby triggering a new mechanism of counter-assessment.

AI and Judicial Review of Technical Discretion: The Possible Procedural Repercussions of a Massive Extension of AI in Administrative Activities Characterized by Technical Discretion

In recent years, we have witnessed increasing momentum toward the introduction of artificial intelligence in public administration (PA). In this context, we are not dealing with generative AI, but rather with a set of processes performed by an algorithmic system capable of going beyond the functioning of a "traditional" algorithm. AI-based systems rely on machine learning, enabling them to analyze data, make choices, and take decisions autonomously, even without human intervention.

Over time, the Council of State has expanded the circumstances in which public administrations may employ automated decision-making procedures. Whereas initially it was held that algorithms could be used only for activities of a binding nature, the judges have gradually adopted a more open position, concluding that:

"If recourse to computer tools may appear easier to use in relation to so-called binding activities, there is nothing to prevent [the purposes established by law], pursued with recourse to the computer algorithm, from also being pursued in relation to activities characterized by areas of discretion. Rather, if in the case of the bound activity much more relevant, both in quantitative and qualitative terms, may be the use of tools for the automation of data collection and evaluation, even the exercise of discretionary activity, especially technical, may in abstract benefit from the efficiencies and, more generally, the advantages offered by the tools themselves,"[41] and that: "there are no reasons of principle, or rather concrete reasons, for limiting the use to binding rather than discretionary administrative activity, both of which are expressions of authoritative activity carried out in pursuit of the public interest."[42]

It has been observed that extending automated administrative decisions to discretionary activities obliges the judge to verify the correctness and transparency of the procedure in all its components, thereby blurring the traditional distinction between legitimacy, which is subject to judicial review, and merit, which is not. In this manner, the automated decision reverses the relationship between the administration and the judge, strengthening the latter's role in scrutinizing the correctness of the intersubjective relationship between citizen and public authority.

41 Cons. Stato [Council of State], Sez. VI, 13 December 2019, no. 84723 (It.).

42 Cons. Stato [Council of State], Sez. VI, 4 February 2020, no. 881 (It.).

However, the Council of State has clarified that, to be legitimate, the PA's use of an algorithm must comply with three important principles.

- **The principle of knowability**: A reinforced expression of the principle of transparency according to which the PA must prepare instruments capable of clearly illustrating how the algorithm functions and how it affects the decision-making process in order to prevent citizens from being excluded from decisions that affect them. Otherwise, the correctness of the decision would be knowable only to a very small number of highly qualified individuals, and democracy would give way to technocracy.
- **The principle of algorithmic non-discrimination,** which requires the administrative officer responsible for configuring the system to verify the input data, so as to prevent discriminatory output. It is undeniable that, thanks to its ability to process large volumes of data, automate complex and repetitive procedures (thus reducing waiting times for citizens), and provide predictive analyses capable of anticipating needs, AI can improve the efficiency of public service management and delivery, making them increasingly interactive and personalized. However, these advantages are offset by numerous risks, since the use of AI projects the decision-making process into a "black box", an indecipherable dimension in which human beings find it difficult to orient themselves
- **The principle of non-exclusivity of the algorithmic decision**, meaning that the mediating and interest-balancing role of the administrative officer is always required upstream. The algorithm is merely a procedural and investigative instrument and, as such, remains subject to all the verifications typical of any administrative procedure. Therefore, rather than replacing indispensable human activity or disempowering administrative officials, the algorithm must operate solely as a modus operandi—in other words, the algorithm must assume a servant role with respect to human decision-makers, not the other way around.

In recent years, legal scholarship has addressed the thorny issue of attributing responsibility for algorithmic decisions when the system produces outputs that cannot be ascribed either to the intention of the public authority or to the programmer (Grimmelikhuijsen & Meijer, 2022, pp. 232–242). One thesis holds that the use of automated procedures does not alter the liability regime, with the consequence that the decision remains imputable to the officeholder. A second thesis proposes that, by separating the phase preceding the compilation of the software, in which the programming rules are established, from the software that issues the act, a dualistic approach whereby the official would be liable for errors in the pre-software stage and the programmer for damages caused by the software.

Starting from the premise that, at present, recourse to AI is deemed precluded where highly debatable or non-standardizable assessment criteria are involved, and therefore whenever a concrete evaluation by the official is required, it becomes particularly interesting to consider the possible procedural consequences of a substantial expansion of AI use in administrative activities marked by technical discretion. One may think, for instance, of drafting competition questions and identifying correct answers which, as case law has repeatedly clarified, are an expression of technical discretion and are beyond judicial review, in the sense that the judge cannot challenge the accuracy of the answers deemed correct by the commission of experts but must limit himself to detecting flaws of legitimacy in the presence of actual errors.[43]

[43] Tribunale Amministrativo Regionale Lazio [Tribunale Amministrativo Regionale Lazio], sez. Quarta Ter, 27 July 2023, Order no. 4567.

The real crux lies in the reviewability of the decision, which unfolds on several levels: the reviewability of the decision itself, of its "motivation", and above all, of the algorithm. This would imply recognizing a substitutional jurisdictional review whenever the technical assessment carried out by AI proves inadequate, unreliable, or incorrectly applied. In such cases, and only in such cases, the judge, assisted by technical expertise, could replace the AI's technical assessment with his own in order to avoid serious distortions of the constitutional framework.

This path appears to be the most rational and system-coherent. In the absence of effective ex-ante control by the administrative authority, an intensive ex-post review by the judiciary would become essential to correct the AI's technical assessment.

This line of reasoning undermines theoretical doctrinal constructions,[44] which claim that technical evaluations are reserved for the public administration. Among these stands the thesis that derives the existence of a reserve of technical assessment for the PA from the principle of good performance enshrined in Article 97 of the Constitution. Yet establishing that the PA must efficiently satisfy community needs does not mean excluding the possibility that other entities may be able to make technical assessments more efficiently. On the contrary, it is plausible that the Constituent Assembly introduced this rule precisely because the PA, as still happens today, struggled to guarantee an adequate standard of efficiency.

It follows that it would be unreasonable to assume a reservation of administrative authority over non-discretionary assessments. Even so, insofar as the adopted AI system forms part of the PA, such reservation would remain intact in a different form.

The principle of the fullness and effectiveness of judicial protection, derived from Articles 24 and 113 of the Italian Constitution,[45] and the principle of equality of the parties in proceedings under Article 111(2), a corollary of due process and a specification of the broader principle of equality in Article 3, require that *"all those judgments that do not impose the only choice reserved to the administration, which is that of opportunity/untimeliness, cannot be considered excluded from judicial review."*

This view has also been endorsed by the Strasbourg Court, which clarified that: *"in a given case where full jurisdiction is contested, the proceedings could still satisfy the requirements of Article 6 § 1 of the Convention if the court deciding the matter would examine all of the plaintiff's claims on the merits, point by point, without ever having to decline jurisdiction in answering the questions or establishing the facts. On the other hand, the Court has found violations of Article 6 § 1 of the Convention in other cases where national courts had considered themselves bound by the previous findings of administrative bodies, which were decisive for the outcome of the cases before them, without independently examining the relevant issues."*[46]

Thus, the judge could fully replicate the technical assessment carried out by the AI, even if complex, and would not be bound by it in any way. A judicial review limited to the verification of legitimacy or manifest unreasonableness of the robo-decision would contravene constitutional and European principles, as well as the case law of the European Court of Human Rights.

Recognizing the power of technical assessment in the hands of the public authority would require abandoning the traditional doctrine of weak intrinsic review, inaugurated by the Council of State in 2001. That doctrine permitted judges in the general jurisdiction of legitimacy to verify the suitability

[44] This is the general orientation of the Council of State in Italy.

[45] Costituzione Italiana [Constitution of the Italian Republic], Art. 23, 113.

[46] Družstevní Záložna Pria & Others v. Czech Republic, App. No. 72034/01 (Eur. Ct. H.R. July 31, 2008), https://hudoc.echr.coe.int/eng?i=001-87882

of the technical criterion used by the PA and the correctness of its application, but, applying the principle of separation of powers, not to replace the PA's assessment. To uphold AI-based decisions, one would instead have to move toward strong intrinsic (and thus substitutive) review, which is currently considered admissible only in relation to sanctions imposed by the Competition and Market Authority.[47]

When PA Discrimination Comes from AI: An English case

In the UK, the AI system used to detect benefit fraud has proven discriminatory. The machine-learning program used to examine Universal Credit claims incorrectly targets individuals from certain groups more than others. This was recently revealed in an investigation published in The Guardian by Robert Booth on December 6, 2024: the AI system employed by the UK government to detect welfare fraud exhibits discrimination based on age, disability, marital status, and nationality.[48]

An internal evaluation of the machine-learning program used to analyze Universal Credit claims in England found that it disproportionately selected individuals from specific groups for investigation. In practice, the system disadvantaged particular racial communities when identifying alleged abuses of the welfare system.

The issue emerged following a records request submitted to the Department for Work and Pensions. Although the final decision on whether a person will receive unemployment benefits remains in the hands of a human decision-maker, officials maintain that continued use of the system, which aims to save approximately £8 billion per year lost to fraud and error, is "reasonable and proportionate."

Activists responded by criticizing the government for adopting a policy of "first do wrong, then fix it" and called on ministers to ensure greater fairness toward groups that the algorithm wrongly suspects of attempting to cheat the system.

Recognition of disparities in the way the automated system assesses fraud risks is also likely to intensify government scrutiny of AI tools, while simultaneously fueling demands for greater transparency.

There are currently 55 automated tools used by public authorities in the UK that may influence decisions affecting millions of people, despite the fact that only nine are listed in the government's register.

In recent years, government departments, including the Home Office, have been reluctant to disclose information about their use of artificial intelligence, justifying this secrecy on the grounds that increased transparency could enable malicious actors to manipulate the systems.

The British case is neither unique nor isolated. It stems from a well-known, but difficult-to-eliminate bias in the programming and weighting of data—a problem originating not from machines, but from human decision-making. Similar phenomena have already been identified in numerous predictive systems used in the United States.[49]

---

47 Cons. Stato [Council of State], Sez. VI, 2019, n. 4990 (It.).

48 Booth, R. (2024, December 6). Revealed: Bias found in AI system used to detect UK benefits fraud. *The Guardian.* https://www.theguardian.com/society/2024/dec/06/revealed-bias-found-in-ai-system-used-to-detect-uk-benefits

49 Johnson, K. (2023, January 21). Gli algoritmi che discriminano chi cerca casa negli Stati Uniti. *Wired Italia*. https://www.wired.it/article/intelligenza-artificiale-stati-uniti-discriminazione-casa/ ; Verga, E. (2023, October 10). *Algoritmi discriminatori, da New York una legge che potrebbe influenzare le future applicazioni di intelligenza artificiale*. https://tech4future.info/algoritmi-discriminatori/ ; Meo (2021); Falchi (2020).

In this respect, adopting standardized models on the pretext that they are cheaper than developing new ones does not resolve the problem. Rather, like a virus, it spreads from one jurisdiction to another and into heterogeneous administrative settings.

It is clear that the historical configuration of a neighborhood in major urban centers often reflects the convergence of racial, social, and educational factors, which in turn affect income levels, access to healthcare, and employment types. An algorithm designed without correcting for these elements will inevitably assign greater risk scores to certain neighborhoods and social classes—precisely those where the need for subsidies is concentrated.

As the number of applications increases, so does the risk of fraud: if district A receives 10 applications and district B receives 100, it is statistically more likely that district B will show a higher incidence of fraud. However, this phenomenon must be interpreted socio-racially.

This bias was first detected in algorithms used to predict and determine health insurance premiums in the United States. Subsequent verification has shown that the same distortions and arbitrary weightings occur in numerous systems adopted by public administrations. This highlights the profound difficulty in identifying the root cause of the error and reprogramming the system of weights using non-discriminatory predictive models.

The problem lies in the uncritical adoption of pre-set products, rather than in the careful construction of specific, contextually grounded weighting systems.

Conclusions

In this article, I have examined the Italian context concerning the introduction of artificial intelligence into the legal sphere, and in particular, into administrative proceedings. This topic intersects with the even more delicate issue of the relationship between AI and criminal justice (Di Salvo, 2024a). While several stakeholders highlight the undeniable advantages associated with machine learning, hyper-computational capacity, and advanced research systems, the legal domain remains an exceptionally sensitive environment in which to test such innovations. The need for careful decision-making, for individualized reasoning on a case-by-case basis, and, above all, for the human point of view is central to decisions that are fair, just, and tailored to the individual.

I have critically discussed the newly introduced Italian legislation on AI to provide an overall framework, and I have illustrated the initial plans for integrating AI into the administrative sector. In the third section, I focused on the connection between AI and judicial review of technical discretion, highlighting the potential procedural implications of an extensive deployment of AI in administrative activities characterized by such discretion. Finally, in the fourth section, I analyzed a case of discriminatory administrative practice resulting from the use of AI systems by a public authority.

Taken together, these reflections reveal a clear need for jurists, first and foremost, to intervene with the technical competence and critical approach inherent in their profession in order to identify the concrete risks that uncritical and pervasive use of AI systems may pose to citizens' rights within the sensitive context of justice and litigation.

References

1. Dahl, M., Magesh, V., Suzgun, M., & Ho, D. E. (2024). Large legal fictions: Profiling legal hallucinations in large language models. *Journal of Legal Analysis*, *16*(1), 64–93. https://doi.org/10.1093/jla/laae003
2. Di Salvo, M. (2024a). Artificial Intelligence and the cyber utopianism of justice. Why AI is not intelligence and man's struggle to survive himself. *Russian Journal of Economics and Law*, *18*(1), 264–279. https://doi.org/10.21202/2782-2923.2024.1.264-279
3. Di Salvo, M. (2024b). Sull'abolizione del reato di abuso d'ufficio. *Salvis Juribus.* http://www.salvisjuribus.it/sullabolizione-del-reato-di-abuso-dufficio
4. Falchi, M. C. (2020). Intelligenza artificiale: Se l'algoritmo è discriminatorio. *Ius in Itinere*. https://iusinitinere.it/intelligenza-artificiale-se-lalgoritmo-e-discriminatorio/
5. Grimmelikhuijsen, S., & Meijer, A. (2022). Legitimacy of Algorithmic Decision-Making: Six Threats and the Need for a Calibrated Institutional Response. *Perspectives on Public Management and Governance*, *5*(3), 232–242. https://doi.org/10.1093/ppmgov/gvac008
6. Meo, M. (2021). L'intelligenza artificiale discrimina, eccome. Ecco perché e come rimediare. *Agenda Digitale*. https://www.agendadigitale.eu/cultura-digitale/lintelligenza-artificiale-discrimina-eccome-ecco-perche-e-come-rimediare/

Information about the author:

Michele Di Salvo — Doctor of Law (University Naples Federico II), Research Coordinator, National Agency for Artificial Intelligence Foundation, Milan, Italy.
mik.disalvo@gmail.com
ORCID: https://orcid.org/0000-0002-9531-0591

Сведения об авторе:

Ди Сальво М. — доктор права (Неаполитанский университет имени Фридриха II), координатор исследований, Национальное агентство искусственного интеллекта, Милан, Италия.
mik.disalvo@gmail.com
ORCID: https://orcid.org/0000-0002-9531-0591

https://doi.org/10.38044/2686-9136-2025-6-2-28-43

ARTICLES

GENDER INEQUALITY IN INTERNET ACCESS DURING COVID-19 IN SOUTH ASIA: EVIDENCE FROM PAKISTAN

Sadaf Qadir[1,*], Zainab Iqbal[2]

[1]Fatima Jinnah Women University
Old Presidency, The Mall, Rawalpindi, Pakistan, 460000

[2]National Counter Terrorism Authority (NACTA)
1, Khayaban-e-Suhrwardy, Islamabad, Pakistan, 440001

Abstract

Advances in technology have introduced relentless competition and increasing demands to everyday life. These pressures particularly intensified during the COVID-19 pandemic, especially in countries where Internet access remains spotty. The right to Internet access ensures connectivity through broadband, and those without such access fall into the digital divide. South Asia, and Pakistan in particular, offers a striking case study of digital inequities, whose impact has been magnified by the global pandemic. Recent studies confirm a persistent gender digital divide in Pakistan and South Asia, where women are significantly less likely to own a mobile phone, access the Internet, or use digital services than men. Against this backdrop of a pronounced gender digital divide, this paper argues that the digital divide, particularly in the South Asian context, constitutes a violation of the fundamental right to Internet access. It seeks to substantiate this claim through an analysis of legal instruments and empirical data on exclusion. It explores the gendered dimensions of this divide in Pakistan, considers the relevant constitutional provisions, and analyzes its broader implications for national development within Pakistan, as well as for regional progress in South Asia. Building on this analysis, the paper concludes by formulating actionable legal and policy remedies, advocating for a multi-level approach that combines constitutional recognition, gender-inclusive governance, strategic partnerships, and targeted empowerment initiatives to bridge the digital gender divide in Pakistan and South Asia.

Keywords

right to Internet access, global pandemic, gender digital divide, South Asia, Pakistan

Conflict of interest	The authors declare no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Qadir, S., & Iqbal, Z. (2025). Gender inequality in Internet access during COVID-19 in South Asia: Evidence from Pakistan. *Digital Law Journal, 6*(2), 28–43. https://doi.org/10.38044/2686-9136-2025-6-2-28-43

* Corresponding author

Submitted: 12 April 2025, accepted: 15 May 2025, published: 30 June 2025

СТАТЬИ

ГЕНДЕРНОЕ НЕРАВЕНСТВО В ДОСТУПЕ К ИНТЕРНЕТУ В ПЕРИОД ПАНДЕМИИ COVID-19 В ЮЖНОЙ АЗИИ: ОПЫТ ПАКИСТАНА

С. Кадир[1,*], З. Икбал[2]

[1]Женский университет имени Фатимы Джинны
460000, Пакистан, Равалпинди, Молл, Олд Президенси

[2]Национальное управление по борьбе с терроризмом
440001, Пакистан, Исламабад, Хайябан-и-Сухраварди, 1

Аннотация

Современные технологические успехи человечества вместе с господством идеи прогресса приводят к усилению социальной конкуренции и требований к квалификации членов общества не только в профессиональной, но и в повседневной жизни. Пандемия COVID-19 особенно ярко проявила это напряжение в странах, где доступ к интернету остается технически нестабильным и недоступным отдельным категориям граждан. Право на доступ к сети интернет предполагает подключение посредством определенной инфраструктуры (широкополосных каналов связи), ограничение доступа к которой приводит к цифровому неравенству. Южная Азия, и особенно Пакистан, представляет собой показательный пример цифрового неравенства, последствия которого были существенно усугублены глобальной пандемией. Современные исследования подтверждают устойчивое существование гендерного цифрового разрыва в Пакистане и странах Южной Азии, где женщины значительно реже, чем мужчины, владеют мобильными телефонами, имеют доступ к интернету и пользуются цифровыми услугами. На фоне выраженного гендерного цифрового неравенства в статье обосновывается тезис о том, что цифровой разрыв, особенно в южноазиатском контексте, представляет собой нарушение фундаментального права на доступ к интернету. Для подтверждения данного утверждения проводится анализ международных и национальных правовых актов, а также эмпирических данных, свидетельствующих об исключенности из цифровой среды. В работе исследуются гендерные аспекты цифрового разрыва в Пакистане, рассматриваются соответствующие конституционные положения и анализируются более широкие последствия этого явления для национального развития Пакистана и регионального прогресса в Южной Азии. На основе проведённого анализа в заключении формулируются практико-ориентированные правовые и политические рекомендации, предполагающие многоуровневый подход, сочетающий конституционное признание права на доступ к интернету, гендерно инклюзивное управление, стратегические партнерства и целевые программы расширения прав и возможностей, направленные на преодоление гендерного цифрового разрыва в Пакистане и странах Южной Азии.

Ключевые слова

право на доступ к интернету, пандемия, гендерное цифровое неравенство, Южная Азия, Пакистан

Конфликт интересов	Авторы сообщают об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.
Для цитирования	Кадир, С., Икбал, З. (2025). Гендерное неравенство в доступе к интернету в период пандемии COVID-19 в Южной Азии: опыт Пакистана. *Цифровое право, 6*(2), 28–43. https://doi.org/10.38044/2686-9136-2025-6-2-28-43

* Автор, ответственный за переписку

Поступила: 12.04.2025, принята в печать: 15.05.2025, опубликована: 30.06.2025

Introduction

Information and Communication Technology (ICT) permeates every aspect of socio-economic and political life. By 2020, more than 4.54 billion people worldwide were using the Internet.[1] The steady increase in Internet users enhances digital literacy, which in turn promotes human development. Owing to its significance, digital literacy has been formally recognized by the United Nations (UN) as an indicator of human development. The United Nations Educational, Scientific and Cultural Organization (UNESCO) defines digital literacy as "the ability to access, manage, understand, integrate, communicate, evaluate and create information safely and appropriately through digital devices and networked technologies for participation in economic and social life. It includes competencies that are variously referred to as computer literacy, ICT literacy, information literacy, and media literacy".[2]

In sum, those who fail to meet these criteria are considered to fall within the digital divide. This paper examines the digital divide as an infringement of the right to Internet access, with a particular focus on South Asia in general and Pakistan in particular.

Discussion

Digital Divide and its Determinants

Scholars have long attempted to define the term *digital divide*, and three main schools of thought can be identified: technological determinism, economic and sociological perspectives (Srinuan & Bohlin, 2011, pp. 5–6).

From the technological determinist view, the digital divide arises from the absence of physical means of access or supporting infrastructure. Within this framework, liberalization and market expansion are seen as responses necessitated by technological change in order to close the divide. The implication is that all individuals possess equal potential to use technology and benefit from ICTs, provided they are granted access. This theory can be subdivided into hard and soft determinism: according to hard determinism, technology inevitably drives social change, while soft determinism

[1] Kemp, S. (2020, January 30). *Digital 2020: Global digital overview.* Datareportal. https://datareportal.com/reports/digital-2020-global-digital-overview

[2] UNESCO. (n.d.). *What you need to know about literacy.* Retrieved April 12, 2025 from https://www.unesco.org/en/literacy/need-know#:~:text=UNESCO%20defines%20digital%20literacy%20as,employment%2C%20decent%20jobs%20and%20entrepreneurship

maintains that technology may facilitate, but does not guarantee, such change (Srinuan & Bohlin, 2011, pp. 2–6).

The economic perspective interprets the digital divide primarily in terms of affordability. Individuals may not be able to pay for Internet access at all, or may only be able to afford cheaper, more limited options, such as mobile data. This divide must be understood in the context of both developed and developing nations (David & Phillips, 2022, pp. 2072–2076).

Finally, the sociological perspective emphasizes the socio-cultural causes of the digital divide, such as migration, illiteracy, unemployment, disability, and gender inequality (OECD, 2021, p. 5). This approach resonates with structuration theory, which posits that individuals are constrained by social structures. For example, public access to computers in libraries or community centers is shaped both by librarians, who regulate access, and by users, who in turn reshape the system through their own choice of how to use the technology (Dixon et al., 2014, pp. 991–1009).

Taken together, these perspectives suggest that the digital divide manifests both as a *divide of access* and a *divide of use*. Divide of access refers to limited availability of hardware, software, broadband connectivity, and related infrastructure. By contrast, divide of use concerns disparities in skills, literacy, abilities, and actual practices of use. Ultimately, the digital divide cannot be reduced to a purely technological, social, or economic phenomenon; rather, it encompasses elements of each. Moreover, it operates across multiple levels: between individuals and households, among communities, and even between countries in terms of ICT access and utilization (Srinuan & Bohlin, 2011, pp. 7–9).

Digital Divide and Gender Inequality in the New Normal

It is often emphasized that the world has become a global village, where people and information are accessible with a single click. Yet the pandemic revealed that this notion is not absolute: many still lack the digital connectivity necessary to participate in this global village. These inequities existed prior to the pandemic, but as public life shifted into virtual spaces, they became even more pronounced. The consequences were particularly severe in sectors such as education and healthcare, compared to other sectors that could more readily transition to remote work. Similarly, the impact varied across regions, with South Asia among the most affected due to its extremely high population density and its status as the region with the second-highest rate of extreme poverty.[3]

Understanding the risks and factors underlying the digital divide is crucial, for although the pandemic has ended, dependence on digital technologies continues to grow. Four distinct types of divides must be considered collectively. The first is the *digital usage gap*, which refers to insufficient digital skills at both the personal and professional levels. The second is the *digital access gap*, where certain groups are excluded from Internet access primarily due to socio-economic inequalities. The third is the *digital generation gap*: Eurostat data shows that nearly half of individuals between the ages of 65 and 74 possess low digital skills, a disparity highlighted during the COVID-19 pandemic. Finally, the *gender-based digital gap*—the focus of this paper—remains a persistent challenge.[4]

According to a report by the Alliance for Affordable Internet (2022), four indicators are essential for achieving meaningful connectivity. The absence of one or more of these factors often underlies the gendered digital divide.

[3] Economic and Social Commission for Asia and the Pacific. (2020). COVID-19 and South Asia: National strategies and subregional cooperation for accelerating inclusive, sustainable and resilient recovery (pp. 1–14). United Nations. https://repository.unescap.org/server/api/core/bitstreams/4f86fbd5-7444-455e-9c8a-24704053e3cd/content

[4] Repsol. (n.d.). *What is the digital divide and how can we address it? A gap that must be bridged.* Retrieved April 12, 2025 from https://www.repsol.com/en/energy-and-the-future/people/digital-divide/index.cshtml

These indicators are:

1) regular use of the Internet, with the minimum threshold being daily use;
2) access to an appropriate device, most commonly a smartphone;
3) sufficient data access;
4) a fast and reliable connection, typically defined as 4G.[5]

Significance of Internet Access: A Legal Framework

The Internet is a transformative tool that has greatly expanded global communication. As a medium, it serves as a driver of economic prosperity and sustainable social development. It plays a vital role in poverty reduction by enhancing access to education and healthcare, while also creating new avenues for employment and income generation for low- and middle-income households. Over the past decade, the Internet has also become a cornerstone of democracy and human rights by facilitating the free flow of ideas and opinions. It has revolutionized opportunities for citizen participation in policymaking, enhancing transparency and accountability. Given its contribution to securing political rights and enabling civic engagement, it is in the broader public interest to recognize Internet access as a human right.

Legal recognition of the right to Internet access must also be understood in terms of its role in promoting national development. In 2016, UN member states adopted 17 Sustainable Development Goals (SDGs) aimed at creating a more just, sustainable, and peaceful world by 2030.[6] Internet access directly contributes to achieving SDGs linked to economic and social development (Goals 8–11) as well as those promoting partnerships and inclusive institutions (Goals 16–17). In 2016, the UN General Assembly passed a resolution declaring that Internet access is a human right. While the resolution is non-binding, its adoption marks an important milestone in the early stages of global recognition.[7]

Other international legal instruments reinforce this recognition. Article 19 of the *Universal Declaration of Human Rights* guarantees freedom of opinion and expression "through any media and regardless of frontiers."[8] Similarly, Articles 2, 19, 22, and 25 of the *International Covenant on Civil and Political Rights*[9] are relevant to Internet access (Pollicino, 2020). Furthermore, the Human Rights Committee's General Comment No. 34 emphasizes the obligation of countries to ensure this right.[10]

There is a growing belief that the right to Internet access may eventually acquire the status of customary international law. This would require not only widespread *opinio juris* but also consistent state practice. Several countries have already recognized Internet access as a legal right, including Estonia (2001)[11] and Finland (2009)[12]. While global consensus is still developing, the increasing

5 Alliances for Affordable Internet. (n.d.). *Meaningful connectivity — unlocking the full power of Internet access.* Retrieved April 12, 2025 from https://a4ai.org/meaningful-connectivity

6 Howell, C., & West, D. M. (2016, November 7). *The Internet as a human right.* Brookings. https://www.brookings.edu/blog/techtank/2016/11/07/the-Internet-as-a-human-right/

7 Barry, J. J. (2020, May 26). *COVID-19 exposes why access to the Internet is a human right*. Open Global Rights. https://www.openglobalrights.org/COVID-19-exposes-why-access-to-Internet-is-human-right/

8 Universal Declaration of Human Rights, art. 19, G.A. Res. 217 (III) A, U.N. Doc. A/810, at 71 (Dec. 10, 1948).

9 International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.

10 U.N. Human Rights Committee, General comment No. 34, Article 19, Freedoms of opinion and expression, U.N. Doc. CCPR/C/GC/34 (12 Sept. 12, 2011), https://www.refworld.org/legal/general/hrc/2011/en/83764

11 Est. Sup. Ct. (Const. Rev. Ch.), Constitutional Judgment, May 23, 2016, para. 23.

12 Electronic Communications Services Act (Tietoyhteiskuntakaari) ch. 7, pt. 3, Act No. 1207/2020 (Fin.).

acknowledgment of Internet access as a human right signals a move toward its eventual codification under customary international law, provided sufficient international cooperation emerges (Reglitz, 2020, pp. 13-14).

Right to Internet Access: South Asia

Globally, men are 21% more likely than women to be online, and in the world's Least Developed Countries (LDCs), this gap widens to 52%.[13] Internet usage is lowest in South Asia, followed by Sub-Saharan Africa, where only 28% of women, compared to 38% of men have Internet connectivity.[14] The digitalization trends during COVID-19 further highlighted gender inequality in South Asia. According to the United Nations Economic and Social Commission for Asia and the Pacific, the average fixed broadband and mobile broadband speeds in the region are 17 Mbps and 15 Mbps, respectively.[15] These speeds declined during the pandemic as daily Internet use increased by 10% among urban users. The causes are multifaceted, including financial crises, low literacy levels, rural-urban disparities, poor security provisions, and entrenched gender-based digital divides.[16]

It is noteworthy that while the *coverage gap* in South Asia has narrowed over time, the *usage gap* remains significant.[17] Around 18% of women in the region have Internet access, compared to 37% of men. Women are particularly disadvantaged in terms of access to global markets, hindered by lower rates of phone ownership, limited access to mobile Internet, and fewer opportunities to develop digital skills. The pandemic and subsequent lockdowns further reduced women's participation in the labor force, with a sharper shift from formal to informal employment compared to men (91% versus 87%).[18]

The GSMA *Mobile Gender Gap Report* (2021) found that, despite the digital inclusion initiatives introduced during the pandemic, a 36% gender gap in broadband access persists in South Asia. While 38% of women in the region use mobile Internet, approximately 372 million women remain unconnected. The report identified the main reasons women cited for not using mobile Internet as lack of literacy and digital skills, followed by affordability constraints. Additional challenges to digital equality include inadequate digital infrastructure, persistent financial barriers, concerns over data privacy and online harassment, limited interest, and perceptions of irrelevance, as well as broader socio-cultural and institutional obstacles.[19]

---

13 Ibarz, G. D. (2022, January 24). *Towards gender equality: The digital rights of girls and women.* International Institute for Environment and Development. https://www.iied.org/towards-gender-equality-digital-rights-girls-women

14 Sarpong, E. (2020, April 15). *COVID-19 shows why Internet access is a basic right. We must get everyone connected.* Web Foundation. https://webfoundation.org/2020/04/COVID-19-shows-why-Internet-access-is-a-basic-right-we-must-get-everyone-connected/

15 Internet Society. (2020). *Impact of COVID-19 on the Internet Ecosystem in Bangladesh, Bhutan, and Pakistan.* https://www.Internetsociety.org/resources/doc/2022/impact-of-COVID-19-on-the-Internet-ecosystem-in-bangladesh-bhutan-and-pakistan/

16 United Nations. (2020, August 18). *Bridging Asia-Pacific 'digital divide' vital to realize tech benefits*. UN News. https://news.un.org/en/story/2020/08/1070502

17 Jefferie, N. (2025, 10 April). *The state of mobile Internet connectivity in South Asia: The coverage gap is narrowing but the usage gap remains the largest in the world*. GSMA. https://www.gsma.com/mobilefordevelopment/blog/the-state-of-mobile-Internet-connectivity-in-south-asia/

18 Okuda, A., & Bell, J. (2022, May 23). *Tackling the digital gender divide in Asia*. The UN agency for digital technologies. https://www.itu.int/hub/2022/05/digital-gender-divide-asia-unicef-rosa/

19 GSMA Connected Women. The Mobile Gender Gap Report. GSMA Intelligence. https://www.gsmaintelligence.com/research/the-mobile-gender-gap-report-2021

Right to Internet Access: A Case Study of Pakistan

According to the Pakistan Bureau of Statistics, the country's population stands at 241.50 million, nearly half of which is women (48.51%).[20] These 101.34 million women were among the most vulnerable populations during the COVID-19 pandemic. Even prior to the pandemic, a digital gender divide existed in Pakistan, and COVID-19 further exposed and exacerbated these disparities. Research on regions with the most frequent Internet shutdowns globally classifies that none of the countries in Southeast Asia are free with respect to Internet freedom.[21]

Within Pakistan, the Digital Rights Foundation has highlighted the inequalities women face in digital space. Its research indicates that women's underrepresentation online is shaped by multiple factors, including cultural and stereotypical expectations, threats of online harassment, and sexualized violence.[22] The gender divide is particularly pronounced on social media platforms. A 2018 report revealed that of 35 million social media users in Pakistan, only 23% were women, and many of these women did not maintain their own accounts but instead shared accounts with male family members.[23]

This pattern is further supported by a telephonic survey of 900 mobile users in Punjab conducted by Emrys Schoemaker. His analysis identified patriarchal attitudes as a key factor shaping men's and women's differential use of social media. The survey found that 85% of Facebook users were male, compared to just 47% of women respondents. Conversely, women showed higher levels of activity on WhatsApp than men.* One interviewee explained this by describing WhatsApp as *ghar ki baat* (a domestic matter), suggesting that it was perceived as a more private platform. Unlike other social media applications, WhatsApp enables more limited interaction and restricts contact with strangers, making it appear more socially acceptable for women. Schoemaker criticizes such selective use of technology, arguing that it reinforces societal stereotypes rather than challenging them.[24]

The following section evaluates the gender-based digital divide across various sectors in Pakistan and assesses its broader impact.

Access to Necessary Information

In Pakistan, as in Bangladesh, women were found to be 15% less likely than men to have access to potentially lifesaving information during the pandemic. This disparity is linked to factors

---

20 Government of Pakistan, Ministry of Planning Development, & Pakistan Bureau of Statistics. (2023). 7th Population and Housing Census: National census report (p. 7). https://www.pbs.gov.pk/wp-content/uploads/2020/07/National-Census-Report-2023.pdf

21 Gomez, J. (2021). Internet censorship deteriorates press freedoms in Southeast Asia. Human Rights in the 21st Century. http://humanrights21.eu/Internet-censorship-deteriorates-press-freedoms-in-southeast-asia/

22 Digital Rights Foundation & BoloBhi. (2020, March 31). The digital gap during the COVID-19 pandemic is exasperating inequalities. *Digital Rights Foundation*. https://digitalrightsfoundation.pk/joint-statement-by-digital-rights-foundation-and-bolobhi-the-digital-gap-during-the-COVID-19-pandemic-is-exasperating-inequalities/

23 Farooq, M. (2018, April 18). *Pakistan's social media landscape dominated by males, females lag behind: Report*. Profit. https://profit.pakistantoday.com.pk/2018/04/18/pakistans-social-media-landscape-dominated-by-males-females-lag-behind-report/

* Ed. note: By decision of the authorities of the Russian Federation, *Meta Platforms, Inc.* has been declared an extremist organization, and its activities are prohibited on the territory of Russia.

24 Schoemaker, E. (2015, August 3). Pakistan's 'digital purdah': How gender segregation persists in social media. *LSE*. https://blogs.lse.ac.uk/southasia/2015/08/03/pakistans-digital-purdah-how-gender-segregation-persists-in-social-media/

such as low rates of mobile phone ownership and limited literacy.[25] Pakistan already faces a high maternal mortality rate, with estimates indicating that at least 140 women die during childbirth for every 100,000 live births (Shaeen et al., 2022). Limited access to essential information has only worsened women's health outcomes. A survey by UN Women revealed that 32% of women in Pakistan reported receiving no information to help them prepare for COVID-19, compared with 21% of men. In Bangladesh, 29% of women reported being out of reach of such information, versus only 15% of men.[26]

Although the Pakistani government did take steps to address these challenges, a survey conducted by the Internet Society found that 80% of respondents were unaware of these initiatives. Significantly, 78% of these respondents were male, suggesting that the proportion of women excluded from access to necessary information was even higher.[27]

The gender gap is also evident in women's use of digital platforms that function as major sources of information and space for socio-political engagement. A survey conducted by Punjab University found Facebook usage to be 80.8% among men but only 19.2% among women.* Similarly, women lagged 16.3% behind on LinkedIn, where men represented 83.7% of users.[28] Women's participation was also notably lower on X (formerly Twitter).[29] These disparities are particularly significant given that social media platforms play a central role in shaping socio-political opinion and enabling the global exchange of ideas and expression.

Provisions for Mental and Emotional Health

The impact of COVID-19 on women experiencing the digital gender gap has been profound. Many have faced unemployment or been confined to lower-paying jobs, while simultaneously shouldering increased domestic responsibilities and encountering rising levels of domestic and gender-based violence. As a result, women have borne a disproportionate burden, which is reflected in heightened stress, anxiety, and other mental health conditions.

A United Nations survey found that 63% of men in Pakistan reported suffering from mental and emotional health conditions, compared to 66% of women. In Bangladesh, the figures were similar, with 62% of women and an equal percentage of men reporting mental health challenges.

---

25 Aggarwal, A. (2020, November 11). *How COVID-19 fuels the digital gender divide.* Friedrich Ebert Stiftung. https://asia.fes.de/news/digital-gender-divide/

26 UN Women Regional Office for Asia and the Pacific. (2020). *Unlocking the lockdown: The gendered effects of COVID-19 on achieving the SDGS in Asia and the Pacific*. UN Women. https://data.unwomen.org/sites/default/files/documents/COVID19/Unlocking_the_lockdown_UNWomen_2020.pdf

27 Agha, R. J., Qaisrani, A. A., Mughal, M. L., & Asif, S. (2020). *COVID-19 and disaster vulnerability in Pakistan: A Human Rights Based Analysis*. Ministry of Human Rights, Government of Pakistan; United Nations Development Programme. https://files.acquia.undp.org/public/migration/pk/COVID-19-and-Disaster-Vulnerability-in-Pakistan---Revised-28_01_2021.pdf

* Ed. note: By decision of the authorities of the Russian Federation, *Meta Platforms, Inc.* has been declared an extremist organization, and its activities are prohibited on the territory of Russia.

28 Velasco, B. (2022, 21 April). *Gender justice through digital rights and data*. Friedrich Ebert Stiftung. https://www.fes.de/en/iez/international-week-of-justice/article-in-gerechtigkeitswoche/geschlechtergerechtigkeit-durch-digitale-rechte-und-daten-governance

29 Farooq, M. (2018, April 18). *Pakistan's social media landscape dominated by males, females lag behind: Report.* Profit. https://profit.pakistantoday.com.pk/2018/04/18/pakistans-social-media-landscape-dominated-by-males-females-lag-behind-report/

Compounding the problem is a lack of health insurance coverage: only 3% of women and 13% of men in Pakistan were found to have such coverage.[30]

Shift in Informal and Formal Employment

When considering the impact of the digital divide on employment during COVID-19, men were reported to have suffered greater losses than women in both formal and informal sectors. In the informal sector, 33% of women lost their jobs, compared to 56% of men. In the formal sector, the disparity was narrower, with 31% of women excluded from employment compared to 33% of men.

A regional comparison further illustrates the imbalance: in Bangladesh, women were six times less likely than men to be employed in the formal sector during the pandemic.[31]

Digital Gender Gap and the Education Sector in the Pandemic

The history of Pakistan's education sector has long been marked by challenges, ranging from health crises and financial constraints to natural disasters, such as the 2005 earthquake, the 2010 and 2022 floods, and military operations in Swat and other northern areas. COVID-19 emerged as yet another crisis, further undermining an already fragile education system. Gender disparity in education predated the pandemic: 22.8 million children were already out of school, of which 32% were primary-school-age girls compared to 21% boys. This disparity is even more pronounced in higher education, where only 13% of girls are enrolled in secondary education. At the national level, 55% of women over the age of 15 remain illiterate.[32]

Against this backdrop, when classrooms abruptly shifted to digital platforms during the pandemic, existing gender disparities deepened. With inadequate digital connectivity, Pakistan's students faced significant obstacles, sparking widespread protests across the country. Students demanded recognition of the structural inequalities that made online learning inaccessible, exposing the stark realities of the state's inability to provide equal education opportunities.

Access to online education depends on reliable electricity, yet in Pakistan, load-shedding in some areas lasts 16 to 18 hours a day, often during working hours. In remote regions, students lack access to highspeed Internet altogether, forcing many to travel long distances to find stable connections, at considerable financial and personal cost. Female students, in particular, face greater restrictions on mobility, adding health and safety burdens to the existing educational divide. The Human Rights Commission of Pakistan has reported that Internet services are routinely suspended in some areas of Pakistan, and such practices persist to this day.[33] Rather than addressing these systemic issues, the government responded to student protests by arresting peaceful demonstrators, thereby infringing their constitutional rights to peaceful assembly under Article 16[34] and freedom of speech and

30 UN Women Regional Office for Asia and the Pacific. (2020). *Unlocking the lockdown: The gendered effects of COVID-19 on achieving the SDGS in Asia and the Pacific.* UN Women. https://data.unwomen.org/sites/default/files/documents/COVID19/Unlocking_the_lockdown_UNWomen_2020.pdf

31 UN Women Regional Office for Asia and the Pacific. (2020). *Unlocking the lockdown: The gendered effects of COVID-19 on achieving the SDGS in Asia and the Pacific.* UN Women. https://data.unwomen.org/sites/default/files/documents/COVID19/Unlocking_the_lockdown_UNWomen_2020.pdf

32 Agha, R. J., Qaisrani, A. A., Mughal, M. L., & Asif, S. (2020). *COVID-19 and disaster vulnerability in Pakistan: A Human Rights Based Analysis.* Ministry of Human Rights, Government of Pakistan; United Nations Development Programme. https://files.acquia.undp.org/public/migration/pk/COVID-19-and-Disaster-Vulnerability-in-Pakistan---Revised-28_01_2021.pdf

33 Human Rights Commission of Pakistan. (2024). *State of human rights in Pakistan*. https://hrcp-web.org/hrcpweb/wp-content/uploads/2020/09/2024-State-of-human-rights-in-2023-EN.pdf

34 Pakistan Const. art.16.

expression under Article 19 of the Constitution of Pakistan (1973).[35] Furthermore, the state neglected its obligation under Article 37 to provide free and compulsory education and to eliminate illiteracy.[36]

A survey conducted by the Internet Society found that the majority of respondents (78%) were male, including 28% male students who reported difficulties in performing routine academic tasks. Specifically, 67% expressed challenges in attending online classes, citing low download speeds (54%), slow browsing (50%), and frequent disconnections (40%) as the main causes. The financial burden further exacerbated the divide, as respondents reported paying more than $10 on average for Internet services during the pandemic—an amount disproportionately high in Pakistan's economic context.[37]

Steady Shift in Digital Gender Gap in Post-Pandemic Era

According to a recent report by the Global System for Mobile Communications Association (GSMA), the gender gap among mobile Internet users in Pakistan has narrowed for the first time since 2021. While men continue to dominate overall usage, the gap declined from 38% in 2023 to 25% in 2024. However, this data must be critically assessed, as it reflects only mobile Internet users. Information on gender disparity across other digital platforms remains scarce, and patterns of usage across demographic segments require independent evaluation.

The same GSMA report highlights a significant divide in mobile ownership versus access. Approximately 35% of Pakistani women who use mobile Internet rely on borrowed devices, compared to only 6% of men.[38] Ownership itself reflects an even starker disparity: only 26% of women in Pakistan own smartphones, compared to 52% of men.[39] Beyond ownership, the digital gender gap extends to the quality of use. Even when women possess smartphones, they often face additional barriers, such as unreliable networks and limited digital literacy, both of which substantially diminish their user experience.[40] Thus, despite some progress, significant gaps persist.

Legal Backing for Right to Internet Access

In Pakistan, the right to Internet access has not yet been granted explicit constitutional protection, nor does any provincial legislation specifically guarantee this right or prescribe penalties for its infringement. Nonetheless, the right can be inferred from several constitutional provisions, including the right to access information, freedom of opinion and expression, peaceful assembly, and education.

---

35 Ibid., art.19.

36 Ibid., art. 37. See also: Tahir, R. (2020, June 30). *Access to Internet is a human right*. Daily Times. https://dailytimes.com.pk/633791/access-to-Internet-is-a-human-right/

37 Internet Society. (2020). *Impact of COVID-19 on the Internet Ecosystem in Bangladesh, Bhutan, and Pakistan*. https://www.Internetsociety.org/resources/doc/2022/impact-of-COVID-19-on-the-Internet-ecosystem-in-bangladesh-bhutan-and-pakistan/

38 Jeffrie, N. (Lead Author), Bahia, K. (Contributor), Gleek, A. (Contributor), Jena, S. (Contributor), Kapllani, B. (Contributor), Leary, R. (Contributor), Lindsey, D. (Contributor), Sibthorpe, C. (Contributor), & Zagdanski, J. (Contributor). (2025). *The Mobile Gender Gap Report 2025* (p. 9). GSMA. https://www.gsma.com/r/wp-content/uploads/2025/06/The-Mobile-Gender-Gap-Report-2025.pdf

39 Shaikh, H., & Chichaibelu, B. B. (2024). *Addressing the gender digital divide in Pakistan: Promoting equal access to mobile phones for economic empowerment*. Consortium for Development Policy Research. https://www.cdpr.org.pk/addressing-the-gender-digital-divide-in-pakistan-promoting-equal-access-to-mobile-phones-for-economic-empowerment/

40 Jefferie, N. (2025, April 9). *Mobile has the potential to empower rural women, but persistent gender gaps must be addressed*. GSMA. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/blog/mobile-has-the-potential-to-empower-rural-women-but-persistent-gender-gaps-must-be-addressed/

Beyond constitutional interpretation, certain legislative instruments indirectly support the right to Internet access. The *Prevention of Electronic Crimes Act (PECA) 2016* is the primary statute regulating unauthorized acts involving information systems.[41] However, the Act has been widely criticized for granting the government broad and vague powers that enable interference with citizens' Internet access and, more specifically, their ability to hold and express political opinions.[42] Under Section 37(2), read in conjunction with Section 51 of PECA 2016, the government introduced the *Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguard) Rules 2021*, which further expand executive control over online content.[43]

More recently, the *Personal Data Protection Bill 2023* has been introduced, which, once enacted, is expected to strengthen protections for users' digital rights, including the right to Internet access.[44]

Initiatives to Ensure the Right to Internet Access

The Government of Pakistan has recognized the challenges posed by the COVID-19 pandemic in the digital sphere and has undertaken certain measures in response. The following are some of the key initiatives introduced by the state:

Resource Management System (RMS)

The Federal Government launched the Resource Management System (RMS) through its pandemic control body, the National Command and Operation Center (NCOC). This initiative was designed to enhance citizens' ability to exercise their right to Internet access by improving digital connectivity within the healthcare system. The RMS facilitated reliable health resource mapping, covering more than 4,000 COVID and non-COVID hospitals nationwide. Leveraging military's health facilities and infrastructure, the system accelerated the testing and screening of COVID-19 patients, thereby strengthening the overall pace and efficiency of the public health response.[45]

Telehealth Platforms

Another significant government initiative was undertaken by the Ministry of National Health Services, Regulation and Coordination (MNHSRC), in collaboration with the World Health Organization (WHO) and the Commission on Science and Technology for Sustainable Development in the South (COMSATS). Together, they organized a short course to train doctors in providing online health services during the pandemic.[46]

---

41 Prevention of Electronic Crimes Act, No. XL of 2016 (Pak.).

42 IDRC-CRDI. (2017, February 13). *Protecting digital rights in Pakistan*. https://idrc-crdi.ca/en/stories/protecting-digital-rights-pakistan

43 Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules (2021), 1343 (1) S.R.O 1753 (Pak.).

44 Draft of The Personal Data Protection Bill (2023). (Pak.). https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf

45 Ministry of National Health Services, Regulation and Coordination. (2020). *National Action Plan for Coronavirus Disease (COVID-19) Pakistan* (p. 27). Government of Pakistan. https://www.nih.org.pk/wp-content/uploads/2020/03/COVID-19-NAP-V2-13-March-2020.pdf

46 Agha, R. J., Qaisrani, A. A., Mughal, M. L., & Asif, S. (2020). *COVID-19 and disaster vulnerability in Pakistan: A human rights based analysis*. Ministry of Human Rights, Government of Pakistan; United Nations Development Programme. https://files.acquia.undp.org/public/migration/pk/COVID-19-and-Disaster-Vulnerability-in-Pakistan---Revised-28_01_2021.pdf

This initiative proved particularly beneficial for women in rural areas, who already faced limited access to hospitals and whose mobility was further restricted by COVID-19. Participants in the telehealth courses received training in prenatal care, delivery, and postnatal care, with special emphasis on emergency situations requiring referrals, including cases of postpartum depression and other gender-specific health concerns.[47]

National Socio-Economic Registry (NSER)

The National Socio-Economic Registry (NSER) created comprehensive databases aimed at regulating and safeguarding the rights of laborers employed in the informal sector. The project was distinctive for its explicit emphasis on gender equality and played a critical role during COVID-19 by enrolling beneficiaries in various poverty-reduction schemes. Importantly, it ensured women's representation within these programs, thereby addressing structural inequalities.

However, significant challenges persisted. Only 25% of women living in poverty had access to mobile phones and computerized national identification cards (CNICs), compared with 68% of men. This disparity limited women's ability to fully benefit from the Registry's initiatives, which highlights the structural barriers that continue to reinforce the digital gender divide.[48]

The National Education Response and Resilience Plan

The National Education Response and Resilience Plan was developed to address educational challenges during the pandemic in all four of Pakistan's provinces. It categorized regions into three distinct groups. The first included areas where educational institutions operated without any access to technology. The second comprised areas with only basic technological access—in these regions, the government introduced broadcast-based learning initiatives, such as educational TV programs. The third category encompassed areas where educational institutions had access to advanced technological resources, allowing for higher levels of digital learning.[49]

Higher Education Commission (HEC) Policy Guidance

The Higher Education Commission (HEC) of Pakistan responded to the pandemic by formulating policies that distinguished between *advanced universities*—those prepared to conduct online classes with operational Learning Management Systems (LMS)—and *lagging universities*, which lacked such systems. To address these disparities, HEC established three specialized committees. The Technology Support Committee was tasked with developing LMS platforms for universities that lacked them, as well as ensuring student access to digital library resources.[50] The Content Identification Committee was responsible for cataloguing lectures, reading materials, and evaluation

---

47 Qaiser, N. (2023, April 6). COMSATS telehealth: Revolutionizing healthcare in rural Pakistan through ICT. *Daily Parliament Times*. https://www.dailyparliamenttimes.com/2023/04/06/comsats-telehealth-revolutionizing-healthcare-in-rural-pakistan-through-ict/

48 Ministry of Poverty Alleviation and Social Safety. (n.d.). *National Socio-Economic Registry (NSER)* (pp. 11–24). Government of Pakistan. Retrieved April, 12, 2025 from https://www.pass.gov.pk/Detail/NzAwYTI3NjAtOTNjYS00ZmU0LTk5OGEtYzBkYjA1NTdlZGQ1

49 Ministry of Federal Education and Professional Training. (2020). *Pakistan national education response and resilience plan (K-12) for COVID-19* (pp. 11–24). Government of Pakistan. https://planipolis.iiep.unesco.org/sites/default/files/ressources/pakistan_national_education_response_resilience_plan_COVID-19.pdf

50 Higher Education Commission of Pakistan. (2020). *COVID 19 — Technology Support Committee* (pp. 7–10) [Working paper]. https://www.hec.gov.pk/english/HECAnnouncements/Documents/nCoVirus/Approved-Working-Paper.pdf

tools, while the Preventive Measures Committee was established to implement standard operating procedures to prevent the spread of COVID-19 on campuses.[51]

In addition to these measures, HEC launched several broader initiatives, including the creation of the National Knowledge Bank (NKB), the establishment of the National Academy for Higher Education (NAHE), and the Radio School Program, which broadcast educational content daily from 10am to noon, with repeat sessions in the evening. HEC also launched televised lectures on HEC Web TV.[52]

At the regional level, HEC coordinated with other SAARC member states to design capacity-building programs during COVID-19. Furthermore, it established a transition body to regulate medical and dental education under the *Pakistan Medical Commission (PMC) Act 2020*.[53]

Digital Gender Inclusion Strategy 2024

The Pakistan Telecommunication Authority (PTA), in collaboration with UNESCO, the National Commission on the Status of Women (NCSW) and the Global System for Mobile Communications Association (GSMA), has launched a major initiative to address the digital gender divide in Pakistan. This program is part of Prime Minister Shehbaz Sharif's *Digital Nation Pakistan Vision*.[54] While the initiative represents an important step toward digital inclusivity, its effectiveness has yet to be systematically evaluated.

Results

Based on the comprehensive analysis presented above concerning the digital gender divide during and after the COVID-19 pandemic, both in South Asia broadly and in Pakistan specifically, the following recommendations are proposed:

1. **Regional Cooperation through SAARC**

   At the regional level, the South Asian Association for Regional Cooperation (SAARC) should play a more active role.[55]

   Therefore, ensuring equitable digital connectivity must be part of this agenda, enabling individuals to realize their potential through access to technology. Practical initiatives could include regional coding camps for women, modeled on successful programs like the *African Girls Can*

[51] Higher Education Commission of Pakistan. (2020). *HEC COVID-19 Policy Guidance No.5: Online Readiness* (pp. 4–6). https://www.hec.gov.pk/english/HECAnnouncements/Documents/nCoVirus/COVID-19-Policy-Guidance-No.5-Online%20Readiness.pdf

[52] Jamal, S. (2020, November 21). *COVID-19: Pakistan launches Radio Schools project to engage students during pandemic*. Gulf News. https://gulfnews.com/world/asia/pakistan/COVID-19-pakistan-launches-radio-schools-project-to-engage-students-during-pandemic-1.75414211

[53] Higher Education Commission of Pakistan. (2020). *COVID 19 — Technology Support Committee* (pp. 5–11) [Working paper]. https://www.hec.gov.pk/english/HECAnnouncements/Documents/nCoVirus/Approved-Working-Paper.pdf

[54] Pakistan Telecommunication Authority. (2024, February 28). *Digital Gender Inclusion Strategy*, https://www.pta.gov.pk/assets/media/digital_gender_inclusion_strategy_28-02-2024.pdf

[55] The eight founding members of SAARC, comprising Afghanistan, Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan, and Sri Lanka, signed its charter at Dhaka on Dec 08, 1985, with the main objective of promoting the welfare of people of South Asia through mutual assistance in the economic, social, cultural, technical, and scientific fields. *See*, Charter of the South Asian Association for Regional Cooperation, Dec. 8, 1985, Dhaka, Bangladesh, https://www.saarc-sec.org/index.php/resources/agreements-conventions/46-saarc-charter-provisional-rules-of-procedure/file

Code Initiative (AGCCI)[56] and the *Americas Girls Can Code (AGCC)*,[57] which provide training in programming and other digital skills.

2. **Constitutional Recognition of Internet Access**
   Pakistan should explicitly recognize the right to Internet access as a fundamental human right. Such recognition would establish a stronger legal framework against frequent Internet shutdowns, requiring that any restrictions meet strict proportionality standards in line with international human rights law. In parallel, strengthening existing government measures, such as right-of-way (ROW) charges for IT and fiber installations, would reinforce accessibility.
3. **Gender-Inclusive State Initiatives**
   All state-led initiatives must incorporate a gender-inclusive approach from the outset, ensuring that women's needs are addressed at the most basic level of policy and implementation.
4. **Public-Private Partnerships**
   Partnerships between the public and private sectors should be encouraged and incentivized. Investment in infrastructure, particularly in projects focused on women, should be guided by measurable Key Performance Indicators (KPIs). Telecom operators, including Jazz, Telenor, and Ufone, are already contributing to expanding Internet access and should be further supported. For instance, Jazz took the initiative of Mera *Goan Live* ("*My Village is Digitally Enabled*") in which Jazz outreached women at their door-steps leveraging GSMA mobile Internet skills training toolkits while respecting cultural norms.[58] Telenor worked on bridging gender digital divide by onboarding PTA on Disability Job Portal in 2022 as lead partner and job placement of 1 female person with disability at PTA. Further, it launched the program "Taleemabad" under which it established 6 virtual schools for girls at federal territory and digital birth registration system. Moreover, it also took the initiative of "Khushal Aangan" to empower women from rural and agri-focused regions of Pakistan.[59] Likewise, Ufone has also taken remarkable steps including the introduction of an industry-first Smart code (*765#) allowing women to receive mobile top-ups without having to share their phone numbers with retailers, addressing a key privacy need.[60]
5. **Affordable Devices and Data Plans**
   Programs to improve the affordability and accessibility of devices are essential. Mobile phones should be made available at subsidized rates, and telecom operators should be encouraged to offer discounted data packages or bundles tailored to rural areas and SIM cards registered to women.

---

56 UN Women Africa. (n.d.). *African Girls Can Code Initiative (AGCCI).* UN Women. Retrieved April 11, 2025, from https://africa.unwomen.org/en/where-we-are/eastern-and-southern-africa/liaison-office-to-au-and-uneca/african-girls-can-code-initiative-agcci

57 ITU Regional Office for the Americas. (2020, December 14). *Americas Girls Can Code: Leveling the tech playing field for girls and women*. The UN Agency for Digital Technologies. https://www.itu.int/hub/2020/12/americas-girls-can-code-leveling-the-tech-playing-field-for-girls-and-women/

58 Viljoen, K., & Manchanda, G. S. (2025). *Jazz Pakistan educates rural women and men about the transformational benefits and uses of mobile*. GSMA. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/blog/jazz-pakistan-educates-rural-women-and-men-about-the-transformational-benefits-and-uses-of-mobile/#:~:text=To%20ensure%20comfort%20and%20social,to%20reflect%20this%20inclusive%20approach

59 Telenor Group, & Pakistan Telecommunication Authority. (2022, February). *#HerDigitalPakistan accelerating gender inclusion in ICTs*. https://www.pta.gov.pk/assets/media/telenor_10-05-2024.pdf

60 Business Recorder. (2022, May 28). *Ufone 4G expands female customer base*. https://www.brecorder.com/news/40176230#:~:text=Also%20delivering%20on%20women's%20safety,GSMA%20Ufone%204G

6. **Promoting the Gig Economy for Women**
   The term gig economy is characterized by freelance, part-time, and project-based jobs facilitated through digital platforms, this model allows workers to offer services directly to customers or to businesses on a temporary basis (Dawid, 2024). Awareness campaigns should inform unemployed women, women in small-scale industries, and women with limited education and skills about the opportunities provided by the gig economy. Short-term online work offers flexible solutions that can help overcome cultural barriers and economic constraints, while reducing the gendered digital divide.
7. **Gender-Responsive Digital Safe Spaces**
   Women-centric platforms should be developed to provide safe spaces where women can voice concerns about Internet access and usage. A dedicated women's task force should also be created to address digital rights violations. Such measures can form part of a broader rights-based digital protection approach to social protection through technology.
8. **Education and Digital Literacy**
   The government should allocate sufficient budgetary resources to establish free public Wi-Fi hotspots, particularly in densely populated areas and government institutions. At the same time, strict measures must be adopted to ensure privacy protections and gender-sensitive policies. Digital literacy curricula should incorporate gender perspectives, and mentorship programs such as *Women in Cybersecurity*[61] should be expanded.
9. **STEM Quotas for Women**
   Quotas should be reserved for women in Science, Technology, Engineering, and Mathematics (STEM)—related jobs. Such affirmative action can encourage women's participation, help dismantle stereotypes, and contribute to narrowing the gender gap in technology.
10. **Awareness and Advocacy**
    Greater public awareness of the digital gender divide is essential. Journalists, think tanks, and advocacy groups should be engaged to highlight the urgency of the issue, fostering wider social and political support for reforms.

Conclusion

This research has systematically examined the digital gender divide as a fundamental infringement of the right to Internet access, with a concentrated focus on South Asia and an in-depth case study of Pakistan. The COVID-19 pandemic acted as a stark magnifier of pre-existing inequities. It highlighted the specific vulnerability of South Asia due to its socio-economic profile and introduced the four indicators of meaningful connectivity—regular use, appropriate device, sufficient data, and fast connection—the absence of which defines the gendered gap. The pandemic's acceleration of digital dependence across sectors like health, education, and employment rendered this divide not just a matter of inequality, but of acute disenfranchisement. The authors believe that addressing the digital gender divide requires a holistic, multi-stakeholder strategy that targets its technological, economic, and sociological roots simultaneously. In essence, securing digital equity for women in Pakistan and South Asia is not a standalone technical goal but a prerequisite for inclusive development, democratic participation, and the fulfillment of fundamental human rights. The path forward demands unwavering commitment to translating these interconnected recommendations from paper into practice.

[61] National Cyber Emergency Response Team of Pakistan (PKCERT). (n.d.). *Security Awareness for Female Empowerment and Resilience (SAFER)*. Retrieved April 11, 2025, from https://pkcert.gov.pk/safer.asp

References

1. David, R., & Phillips, P. (2022). The gender digital gap: Shifting the theoretical focus to systems analysis and feedback loops. *Information, Communication & Society*, *26*(10), 2071–2087. https://doi.org/10.1080/1369118X.2022.2069507
2. Dixon, L. J., Correa, T. Straubhaar, J., Covarrubias, L., Graber, D., Spence, J. & Rojas, V. (2014). Gendered space: The digital divide between male and female users in Internet public access sites. *Journal of Computer-Mediated Communication*, *19*(4), 991–1009. https://doi.org/10.1111/jcc4.12088
3. Shaeen, S. K., Tharwani, Z. H., Bilal, W., Islam, Z., & Essar, M. Y. (2022). Maternal mortality in Pakistan: Challenges, efforts, and recommendations. *Annals of Medicine and Surgery*, 81, Article 104380. https://doi.org/10.1016/j.amsu.2022.104380
4. Dawid, T. (2024). The rise of the gig economy: Benefits, drawbacks, and future prospects. *Journal of Economics and Economic Education Research, 25*(6), 1–3.
5. Reglitz, M. (2020). The human right to free Internet access. *Journal of Applied Philosophy, 37*(2), 314–331. https://doi.org/10.1111/japp.12395
6. OECD. (2021). *Understanding the digital divide*. https://doi.org/10.1787/236405667766
7. Pollicino, O. (2020). Right to Internet access: Quid iuris? In A. von Arnauld, K. von der Decken, M. Susi (Eds.), *The Cambridge handbook of new human rights: Recognition, novelty, rhetoric* (pp. 263–275). Cambridge University Press. https://doi.org/10.1017/9781108676106.021
8. Srinuan, C., & Bohlin, E. (2011). *Understanding the digital divide: A literature survey and ways forward*. EconStor. http://hdl.handle.net/10419/52191

Information about the authors:

Sadaf Qadir — LL.B., Law Faculty, Fatima Jinnah Women University, Rawalpindi, Pakistan.
sadafqadir13@gmail.com
ORCID: https://orcid.org/0009-0005-2608-434X

Zainab Iqbal — Assistant Director, National Counter Terrorism Authority (NACTA), Islamabad, Pakistan.
zainab.iqbal412@gmail.com
ORCID: https://orcid.org/0000-0001-8631-9503

Сведения об авторах:

Кадир С. — бакалавр права, юридический факультет, Женский университет имени Фатимы Джинны, Равалпинди, Пакистан.
sadafqadir13@gmail.com
ORCID: https://orcid.org/0000-0003-4962-2823

Икбал З. — заместитель директора Национального управления по борьбе с терроризмом, Исламабад, Пакистан.
zainab.iqbal412@gmail.com
ORCID: https://orcid.org/0000-0001-8631-9503

https://doi.org/10.38044/2686-9136-2025-6-9

СТАТЬИ

ДОМЕННЫЕ СПОРЫ И АРБИТРАЖ ПО UDRP: ПРАВОВЫЕ ПРОБЛЕМЫ И НОВЫЕ (СТАРЫЕ) ВЫЗОВЫ

М. А. Рожкова[1,2,*], **Е. В. Алымова**[1]

[1]Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации
117218, Россия, Москва, ул. Б. Черемушкинская, 34

[2]Российская государственная академия интеллектуальной собственности
117279, Россия, Москва, ул. Миклухо-Маклая, 55а

Аннотация

Настоящая статья посвящена комплексному исследованию правовой природы разбирательства по правилам процедуры, предусмотренной Единой политикой разрешения споров о доменных именах (UDRP). Целью работы является выявление особенностей правового регулирования UDRP, анализ ее арбитражной природы и существующих правовых проблем, возникающих в процессе применения данной процедуры. В качестве материалов использованы тексты UDRP и Правил UDRP, документы ICANN, аналитические исследования, судебная и арбитражная практика. Методологическую основу составили формально-юридический и сравнительно-правовой методы. В статье раскрываются аргументы в пользу квалификации разбирательства в рамках UDRP как вида арбитража (третейского разбирательства), несмотря на отсутствие классической арбитражной оговорки. Анализируется механизм согласования воли сторон на передачу спора в аккредитованный ICANN арбитражный центр через договор с регистратором и подачу жалобы. Авторами также рассматриваются проблемы арбитрабельности доменных споров и соотношения UDRP с национальными судами, а также структура системы DNS и полномочия ICANN. Отдельное внимание уделено критике UDRP: предвзятости аккредитованных арбитражных центров в пользу правообладателей товарных знаков, отсутствию апелляционного пересмотра, процессуальным ограничениям, вопросам языка разбирательства и невозможности санкционирования недобросовестных заявителей. Авторы делают вывод о том, что несмотря на процедурные особенности, отличающие UDRP от классического третейского разбирательства, данная модель разрешения споров обладает всеми признаками внесудебного частноправового (альтернативного) разбирательства. Результаты исследования позволяют отнести процедуру UDRP к арбитражу и рассматривать ее как значимый пример эффективного и адаптированного к цифровой среде механизма альтернативного разрешения споров.

Ключевые слова

доменные споры, доменное имя, товарный знак, *ICANN, UDRP,* альтернативное разрешение споров, арбитрабельность, арбитражное разбирательство, компетенция арбитражного учреждения, арбитражное соглашение

Конфликт интересов Авторы сообщают об отсутствии конфликта интересов.

Финансирование В рамках НИР «Совершенствование судебной защиты интеллектуальных прав в Российской Федерации и ее гармонизация с аналогичными системами стран — участниц ЕАЭС» (3-ГЗ-2023).

Для цитирования Рожкова, М. А., Алымова, Е. В. (2025). Доменные споры и арбитраж UDPR: правовые проблемы и новые (старые) вызовы. *Цифровое право, 6*(2), 44–71. https://doi.org/10.38044/2686-9136-2025-6-9

* Автор, ответственный за переписку

Поступила: 15.04.2025; принята в печать: 09.05.2025, опубликована: 30.06.2025

ARTICLES

DOMAIN DISPUTES AND ARBITRATION UNDER THE UDRP: LEGAL ISSUES AND NEW (OLD) CHALLENGES

Marina A. Rozhkova[1,2,*], Ekaterina V. Alymova[1]

[1]The Institute of Legislation and Comparative Law
under the Government of the Russian Federation
34, Bolshaya Cheremushkinskaya St., Moscow, Russia, 117218

[2]Russian State Academy of Intellectual Property
55a Miklukho-Maklaya St., Moscow, Russia, 117279

Abstract

In this article, we delve into a comprehensive study of the legal nature of proceedings regulated by the Uniform Domain Name Dispute Resolution Policy (UDRP). Our aim was to examine specific features of the UDRP legal regulation and to analyze its arbitration nature and legal problems arising in the process of its application. The pool of research materials included the texts of the UDRP and UDRP Rules, ICANN documents, analytical studies, as well as judicial and arbitration practice. Formal legal and comparative legal methods were used. Arguments in favor of qualifying proceedings under the UDRP as a type of arbitration (arbitration proceedings), despite the absence of a classic arbitration clause, are presented. The mechanism for agreeing the parties' intention to refer the dispute to an ICANN-accredited arbitration center through an agreement with the registrar and the filing of a respective complaint is examined. In addition, the issues involved with the arbitrability of domain disputes and the relationship between the UDRP and national courts are discussed, as well as the structure of the DNS system and the powers of ICANN. Particular attention is paid to criticism of the UDRP, including such aspects as the bias of accredited arbitration centers in favor of trademark owners, the lack of appeal review, procedural restrictions, issues of the language of proceedings, and the inability to sanction unscrupulous applicants. The conclusion is made that despite the procedural

features that distinguish UDRP from classical arbitration, this dispute resolution model has all the characteristics of extrajudicial private law (alternative) proceedings. The results obtained allow us to classify the UDRP procedure as arbitration and consider this procedure a significant example of an effective alternative dispute resolution mechanism adapted to the digital environment.

Keywords

domain disputes, domain name, trademark, ICANN, UDRP, alternative dispute resolution, arbitrability, arbitration proceedings, jurisdiction of arbitration, arbitration agreement

Conflict of interest	The authors declare no conflict of interest.
Financial disclosure	This research is part of the research project entitled "Improving the judicial protection of intellectual property rights in the Russian Federation and harmonising it with similar systems in EAEU member states" (3-GZ-2023).
For citation	Rozhkova, M. A., & Alymova, E. V. (2025). Domain disputes and arbitration under the UDRP: Legal issues and new (old) challenges. *Digital Law Journal, 6*(2), 44–71. https://doi.org/10.38044/2686-9136-2025-6-9

* Corresponding author

Submitted: 15 Apr. 2025, accepted: 9 May 2025, published: 30 June 2025

Введение

Сегодня под доменными спорами обычно понимают дела, связанные с регистрацией и/или использованием доменных имен, тождественных или сходных с зарегистрированными товарными знаками (знаками обслуживания). В более широком толковании сюда включают споры, касающиеся любых средств индивидуализации — не только товарных знаков, но и фирменных наименований, коммерческих обозначений и пр.[1] Существует и более обширная трактовка доменных споров, опирающаяся на обоснованные выводы о многообразии правовых конфликтов, возникающих по поводу доменных имен (Yakushev et al., 2017, p. 174; Sergo, 2023, p. 140).

Несмотря на наличие разных подходов, следует признать, что преобладающим остается *узкое понимание* доменного спора — как *спора о правомерности использования в доменном имени чужого товарного знака*. Именно в таком значении будет использоваться термин «доменный спор» в настоящей статье.

Чаще всего поводом для доменного спора становится обнаружение правообладателями в сети Интернет веб-сайтов, доменное имя которых полностью или частично воспроизводит охраняемое средство индивидуализации[2]. При этом наличие активного веб-сайта не является

[1] На это обращалось внимание в преамбуле одной из первых справок Суда по интеллектуальным правам: «Под доменным спором в настоящей справке понимаются дела о правомерности использования доменного имени, сходного с результатом интеллектуальной деятельности или средством индивидуализации, принадлежащим заявителю, в которых заявлено требование о понуждении к совершению либо о воспрещении каких-либо действий, подлежащее принудительному исполнению» (см.: Справка о некоторых вопросах, связанных с процессуальным порядком применения обеспечительных мер по доменному спору, утв. постановлением Президиума Суда по интеллектуальным правам от 15 октября 2013 г. № СП-23/3).

[2] Как указывалось выше, обычно, когда говорят о доменных именах, речь идет о товарных знаках, поэтому в дальнейшем отсылка к иным средствам индивидуализации делаться не будет.

обязательным условием для инициирования доменного спора как в национальных судах, так и в арбитражных центрах, рассматривающих споры по правилам *Единой политики разрешения споров о доменных именах* (*Uniform Domain Name Dispute Resolution Policy, UDRP*)[3]. Так, при рассмотрении доменного спора Суд по интеллектуальным правам, разбирая вопрос недобросовестного поведения ответчика при регистрации домена, прямо указал, что «исходя из целей регистрации доменного имени нарушением исключительного права на товарный знак может быть признана сама по себе такая регистрация»[4].

К аналогичному выводу пришел арбитражный центр, являющийся частью Международного бюро Всемирной организации интеллектуальной собственности (*World Intellectual Property Organization, WIPO;* далее — ВОИС), — Центр ВОИС по арбитражу и посредничеству (*WIPO Arbitration and Mediation Center*) — в деле № D2024-3829, где рассматривался спор об использовании доменного имени *sluk-clients.com* не для размещения сайта, а в мошеннических целях, для рассылки электронных сообщений якобы от имени сотрудника правообладателя[5].

Правообладатель, выявивший присутствие принадлежащего ему товарного знака в доменном имени, зарегистрированном на иное лицо, вправе предъявить иск, в котором может требовать запретить указанному лицу использовать данный товарный знак в упомянутом доменном имени. Как подчеркивает И. Е. Титов, основной экономической целью доменного спора является получение правообладателем права администрирования спорного доменного имени (Titov, 2025, p. 163).

Важно, что по общему правилу доменные споры могут рассматриваться как различными внесудебными органами, так и государственными судами, что актуализирует проблему определения компетентного суда. В свою очередь, возможность рассмотрения доменных споров разными органами предопределяет применение различных процедур, одной из которых является широко известная Единая политика разрешения споров о доменных именах.

В рамках настоящей статьи, как следует из ее названия, освещается комплекс правовых проблем, возникающих при рассмотрении доменных споров в соответствии с Единой политикой разрешения споров о доменных именах. Особое внимание уделяется вопросам правовой природы рассматриваемой процедуры, оценке направлений ее критики, определению арбитрабельности доменных споров как условия для установления компетенции соответствующих арбитражных учреждений[6]. Кроме того, анализируются механизмы формирования согласия сторон на участие в разбирательстве, специфика выбора компетентного арбитражного центра, а также особенности взаимодействия указанной процедуры с юрисдикцией национальных судебных органов.

---

[3] Все редакции полиса доступны для ознакомления на сайте Корпорации по присвоению имен и номеров (*Internet Corporation for Assigned Names and Numbers, ICANN*): ICANN. *Uniform Domain-Name Dispute-Resolution Policy*. https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/uniform-domain-name-dispute-resolution-policy-01-01-2020-en. Подробно про UDRP см. раздел «Общая характеристика UDRP и специфика доменных споров» настоящей статьи.

[4] Постановление Суда по интеллектуальным правам от 16 июля 2021 г. № С01-1060/2021 по делу № А40-70060/2020/.

[5] Phoenix Group Management Services Ltd. v. Name Redacted, WIPO Case No. D2024-3829 (WIPO Arb. & Mediation Ctr., Nov. 11, 2024).

[6] В. В. Еремин подчеркивает, что данный термин был впервые употреблен С. Н. Лебедевым в работе «Международный коммерческий арбитраж: компетенция арбитров и соглашение сторон» (1988), причем он использовал вариант написания через «и», т. е. «арбитрабильность». Указывая, что слова, скалькированные из иностранных языков, должны писаться с суффиксом «абель», В. В. Еремин предлагает использовать вариант написания через «е» — «арбитрабельность» (Eremin, 2019, pp. 96–97).

Устройство системы доменных имен, компетенция *ICANN* и полномочия администраторов доменов верхнего уровня

Рассмотрение обозначенных в заголовке статьи вопросов необходимо предварить кратким обзором построения системы доменных имен (*Domain Name System, DNS*).

DNS, разработанная Корпорацией по присвоению имен и номеров (*Internet Corporation for Assigned Names and Numbers, ICANN*)[7], имеет иерархическую структуру, предусматривая подразделение доменных имен на ряд уровней, которые записываются справа налево. Технические специалисты говорят о теоретической возможности включения в полное доменное имя до 128 уровней[8]. Однако для целей права, как показывает практика, интерес представляют домены первого (верхнего) и второго уровня, крайне редко — доменные имена третьего уровня (поддомены), которые практически не выступают предметом судебных или арбитражных споров. С поддоменами четвертого и последующих уровней юристы фактически не сталкиваются.

К компетенции *ICANN* отнесено осуществление всех ключевых административных функций, связанных с управлением и регулированием глобальной системы адресации сети Интернет, в том числе решение вопросов, касающихся с обеспечения работы **доменов первого (верхнего) уровня** (*Top-Level Domain, TLD*):

1) национальных (страновых, территориальных) доменов (*Country-Code Top-Level Domain, ccTLD*), созданных специально для стран или отдельных территорий: *.ru* (Россия); *.su* (СССР); *.de (*Германия); *.fr* (Франция); *.it* (Италия); *.jp* (Япония); *.uk* (Соединенное Королевство); *.eu* (Европейский союз); *.us* (США) и т. д.;
2) доменов общего назначения (*Generic Top-Level Domain, gTLD*) — изначально совсем небольшой[9] группы доменных имен, предназначенных для использования различными сообществами или определенного класса организациями: *.com* (от *commercial* — для коммерческих сайтов); *.org* (от *organization* — для некоммерческих организаций); *.biz* (от *business* — для бизнеса); *.edu* (от *education* — для образовательных сайтов); *.name* (для частных лиц) и т. п.;
3) новых доменов общего назначения (*New Generic Top-Level Domain, new gTLD*), создаваемых сегодня: *.club, .photography, .dance, .today, .moscow, .tatar,* .рус, .москва и т. д.

Обеспечение стабильной работы в Интернете каждого из названных *TLD* требует прежде всего создания и поддержания в актуальном состоянии баз данных, содержащих сведения о доменных именах. Такие базы данных (*registry*) на официальном сайте *ICANN* в глоссарии терминов на русском языке именуются «регистратурами»[10], но чаще переводятся

[7] Разработчиком-исполнителем *DNS* выступил Пол Мокапетрис в 1983 г. До этого сетевые адреса присваивались вручную. См. вебсайт системы (https://www.icann.org/ru).

[8] В технических стандартах *DNS* не содержится прямого ограничения числа уровней в полном доменном имени (*FQDN*) (см. к примеру, стандарт *RFC 1035*: Mockapetris, P. (1987). *Domain names — Implementation and specification*. RFC Editor. https://doi.org/10.17487/RFC1035). Но такие ограничения появляются автоматически из-за технических требований: максимальная длина полного доменного имени не может превышать 255 октетов (символов в двоичном представлении), каждой отдельной части (*label*) — 63 октета. С учетом этих технических параметров предельное количество уровней в одном полном доменном имени составляет 127–128 уровня (в зависимости от того, считается ли нулевой, корневой уровень). При этом обозначение 127–128 уровней выступает только расчетной (теоретической) величиной и не встречается на практике.

[9] Изначально было создано восемь *gTLD*: *.com, .net, .org, .int, .edu, .gov, .mil* и *.arpa*, а затем (в 2001 г.) было принято решение о введении еще семи: *.info, .biz, .name, .coop, .museum, .aero* и *.pro.*

[10] ICANN. (б.д.). Аббревиатуры и терминология ICANN. https://www.icann.org/ru/icann-acronyms-and-terms

как «реестры»[11], поэтому далее будет использоваться именно этот термин. Каждый *TLD* имеет собственный реестр, который содержит регистрационные записи всех доменных имен, зарегистрированных в этой доменной зоне.

В качестве примеров **доменных имен второго уровня** (часть полного доменного имени слева от *TLD*) можно указать, в частности, *yandex.ru, google.com, mail.ru, vk.com*. К примерам **доменных имен третьего уровня** (поддомены, которые располагаются слева от домена второго уровня) относятся *digital.gov.ru, ru.wikipedia.org.*

ICANN в целях обеспечения бесперебойной работы *DNS* делегирует функции администрирования и технического обеспечения работы *TLD* тем организациям, которые могут обеспечить стабильное функционирование *DNS*-инфраструктуры, а также обслуживать и поддерживать в актуальном состоянии реестр доменных имен второго уровня, зарегистрированных в зоне соответствующего *TLD*. Такие организации становятся администраторами *TLD,* заключая с *ICANN* соответствующее соглашение (Rozhkova & Kopylov, 2022, p. 100).

Примечательно, что полномочия администраторов *gTLD* и администраторов *new gTLD*, которые определяются по результатам частного аукциона, принципиально отличаются от полномочий администраторов *ccTLD*. Эта разница обусловлена различной степенью институционального контроля со стороны *ICANN.* Так, домены *gTLD* и *new gTLD* находятся под прямым управлением *ICANN,* которая осуществляет как их техническое сопровождение, так и нормативное регулирование. В отличие от этого *ccTLD* делегируются национальным администраторам, получающим полномочия из соглашений с *ICANN* и действующим в пределах конкретных государств.

Вследствие сказанного администраторы *gTLD* и администраторы *new gTLD* принимают на себя обязанность соблюдать все специальные процедуры и политики, разработанные *ICANN,* что существенным образом сказывается на содержании регламентирующих документов этих администраторов. В свою очередь администраторы *ccTLD* гораздо свободнее в части содержания собственных регламентирующих документов (например, о порядке регистрации в национальной доменной зоне доменов второго уровня и аккредитации регистраторов, об альтернативных способах урегулирования возникающих доменных споров и пр.) и обычно разрабатывают такие документы с опорой на национальное законодательство, хотя и с учетом политик, утвержденных *ICANN* применительно к *ccTLD.*

Например, управление национальными доменами верхнего уровня *.ru* и .рф осуществляет автономная некоммерческая организация «Координационный центр национального домена сети Интернет» (далее — Координационный центр доменов *.RU*/.РФ), на которую возложены публично значимые функции по обеспечению устойчивого функционирования инфраструктуры российского сегмента Интернета[12]. В рамках своей компетенции Координационный центр

[11] Например, пункт 1.1 Правил регистрации доменных имен в доменах *.RU* и .РФ гласит: «Реестр — база данных Координатора, содержащая сведения о зарегистрированных доменных именах второго уровня, их администраторах и другие необходимые сведения» (https://cctld.ru/files/pdf/docs/rules_ru-rf.pdf).

[12] Так, в ч. 4 ст. 14.2 закона «Об информации, информационных технологиях и о защите информации» было закреплено следующее: «Координацию деятельности по формированию доменных имен, входящих в группы доменных имен, составляющих российскую национальную доменную зону, осуществляет некоммерческая организация, одним из учредителей которой является Российская Федерация и которая является зарегистрированным владельцем баз данных этой зоны в международных организациях распределения сетевых адресов и доменных имен. От имени Российской Федерации функции и полномочия учредителя осуществляет федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи» (см.: Федеральный закон «Об информации,

доменов *.RU*/.РФ разрабатывает и утверждает необходимые регламентирующие документы[13], обеспечивает поддержание в актуальном состоянии реестров доменных имен в зонах *.ru* и .рф. Одной из ключевых функций Координационного центра доменов *.RU*/.РФ является аккредитация регистраторов, уполномоченных вносить сведения о доменных именах второго уровня в реестры доменных зон *.ru* и .рф. В то же время исполнение технических функций делегировано Техническому центру Интернет, который в настоящее время выступает в качестве технического оператора доменов *.ru* и .рф.

Управление национальным доменом Германии *.de* осуществляет товарищество *DENIC eG,* которое приняло на себя как административные, так и технические функции по обеспечению устойчивой работы указанной доменной зоны[14]. В рамках своей компетенции *DENIC eG* разрабатывает и утверждает нормативные документы, регулирующие регистрацию и использование доменных имен в зоне *.de,* а также осуществляет ведение и техническое сопровождение реестра этого *ccTLD*. Особенность немецкой модели заключается в том, что регистрация доменных имен может производиться посредством заключения договора присоединения как непосредственно с *DENIC eG*, так и через уполномоченные организации — члены товарищества (*DENIC-Mitglieder*)[15].

Общая характеристика *UDRP* и специфика доменных споров

ICANN обладает полномочиями по вопросам, связанным с обеспечением стабильного функционирования *TLD,* включая разработку и утверждение как общих политик, так и специальных положений, регламентирующих отдельные доменные зоны.

К числу таких общих политик относится упоминавшаяся *Единая политика разрешения споров о доменных именах*, принятая *ICANN* в 1999 г.[16] Одновременно на ее основе были разработаны Правила *UDRP* (*Rules for Uniform Domain Name Dispute Resolution Policy*), которые неоднократно обновлялись[17].

информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. 24.06.2025). Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448). В связи с указанным положением в 2020 г. в состав учредителей Координационного центра доменов *.RU*/.РФ вошла Российская Федерация, функции и полномочия от имени которой реализует Роскомнадзор.

13 К числу регламентирующих документов Координационного центра доменов *.RU*/.РФ относятся, в частности, Правила регистрации доменных имен в доменах .RU и .РФ, Положение «О процедурах, подлежащих применению при возникновении споров о доменных именах» и др.

14 Согласно мировой доменной статистике за второй квартал 2025 г., домен .de является крупнейшим национальным доменом *ccTLD* (более 17 млн регистраций), на втором месте китайский домен *.cn* (более 11 млн регистраций). Домен *.ru* занимает пятое место (более 5 млн регистраций) (Координационный центр доменов .RU/.РФ. (2025). Мировая доменная статистика: 2 квартал 2025 года. https://cctld.ru/upload/iblock/d21/ja60x82zbp1boryqoojy0ksujo1zx39i/World_stat_2025_2kv_.pdf).

15 Denic. (n.d.). *DENIC-Domainrichtlinien und Datenschutzhinweise*. Retrieved April 14, 2025, from https://www.denic.de/domainrichtlinien/

16 В Справке по вопросам, возникающим при рассмотрении доменных споров, *UDRP* обозначена как «Единообразная политика по разрешению споров в связи с доменными именами, одобренная Интернет-корпорацией по присвоению названий и номеров (*ICANN*)» (см.: Постановление Президиума Суда по интеллектуальным правам «Об утверждении справки по вопросам, возникающим при рассмотрении доменных споров» от 28 марта 2014 г. № СП-21/4). Под таким наименованием *UDRP* упоминается и во многих судебных актах.

17 ICANN. (n.d.). Rules for Uniform Domain Name Dispute Resolution Policy. https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/rules-for-uniform-domain-name-dispute-resolution-policy-the-rules-11-03-2015-en

Как отмечается в зарубежной научной литературе, введение *UDRP* преследовало двойную цель. С одной стороны, ее задача заключалась в оперативном и эффективном реагировании на наиболее очевидные и массовые нарушения в области товарных знаков (в частности, случаи киберсквоттинга[18]). С другой стороны, *UDRP* была призвана снизить риски судебного преследования реестра и регистраторов со стороны правообладателей товарных знаков (Cortés Diéguez, 2008, p. 350).

Первоначально *UDRP* применялась только к доменам зоны *gTLD,* таким как *.com, .net, .org, .biz* и др. Однако уже на начальном этапе действия *UDRP* ее влияние на разрешение споров в интернете оказалось столь масштабным, что в научной литературе появилась оценка *UDRP* как основы для формирования «всемирного права по изъятию доменного имени» (Froomkin, 2002, p. 632). Позднее (в результате решений *ICANN* и соответствующих изменений в соглашениях с администраторами) действие *UDRP* было распространено на все *new gTLD*, включая *.app, .site, .moscow, .tatar,* .рус, .москва и др.

Применение *UDRP* в отношении национальных доменных имен возможно только при условии, что администраторы соответствующих *ccTLD* официально признали допустимость использования такой процедуры при разрешении доменных споров. На сегодняшний день *UDRP* в полном объеме применяется, например, к доменам верхнего уровня: *.ai* (Ангилья), *.me* (Черногория), *.tv* (Тувалу) и *.pk* (Пакистан).

Наряду с этим некоторые администраторы *ccTLD,* пользуясь предоставленными полномочиями, внедрили собственные, адаптированные под национальное право механизмы — модифицированные версии *UDRP* (*modified UDRP*). Такого рода процедуры формально не являются *UDRP,* хотя и основаны на аналогичных принципах. В таких случаях разбирательство осуществляется не по стандартной процедуре, установленной *ICANN*, а в соответствии со специальными политиками, основанными на *UDRP* и принятыми для конкретного национального домена. Подобные правила в отношении *ccTLD* предусмотрены для доменных зон: *.au* (Австралия), *.cn* (Китай), *.fr* (Франция), *.mx* (Мексика) и др.[19]

Примечательно, что ни в *UDRP,* ни в Правилах *UDRP* не закреплено определение понятия «доменный спор». Вместе с тем согласно п. 4(a)(i) *UDRP* обязательные административные слушания проводятся в случае, если доменное имя идентично или сходно с товарным знаком или знаком обслуживания, права на которые принадлежат заявителю[20]. Изложенное дает основание сделать несколько важных в целях настоящей статьи выводов. Так, со всей определенностью усматривается, что процедура *UDRP* допустима в случае противостояния «доменное имя — товарный знак» и не предполагает использование в тех случаях, когда доменному имени противопоставляется какое-либо иное средство индивидуализации. Тем не менее в научной литературе и на практике признается допустимость рассмотрения споров по правилам *UDRP* в отношении доменных имен, воспроизводящих незарегистрированные товарные знаки, несмотря на то что возможность правовой охраны зависит от национального законодательства в каждом конкретном случае. Вместе с тем воспроизведение в доменном

[18] Под киберсквоттингом традиционно понимается недобросовестное приобретение доменных имен, созвучных с названиями известных организаций, товарных знаков, брендов, сообществ и стран, с целью их дальнейшей перепродажи.

[19] Полный перечень стран, которые применяют *UDRP* или собственные политики, основанные на *UDRP*, доступен на сайте Всемирной организации интеллектуальной собственности: WIPO.ADR. (n.d.). *Domain name dispute resolution*. Retrieved April 14, 2025, from https://www.wipo.int/amc/en/domains/

[20] Internet Corporation for Assigned Names and Numbers [ICANN]. *Uniform Domain Name Dispute Resolution Policy* (Aug. 26, 1999, as amended Feb. 21, 2024). https://www.icann.org/resources/pages/policy-2024-02-21-en

имени географических указаний, фирменных наименований и иных обозначений, не признаваемых товарными знаками, хотя формально и относящихся к средствам индивидуализации, не может служить основанием для инициирования разбирательства в порядке *UDRP* (Cortés Diéguez, 2008, p. 351).

Тем не менее, как отмечает Милтон Мюллер (*Milton Mueller*) *на* основе анализа практики, отдельные попытки инициировать разбирательства по правилам *UDRP* в отношении доменных имен, содержащих географические указания, предпринимались[21]. При этом такие иски, как правило, не увенчивались успехом, а исключения носили единичный характер. Наиболее примечательным примером такого спора является дело ВОИС № D2000-0505 в отношении домена *barcelona.com*[22]. Как подчеркивает М. Мюллер, решение ВОИС по данному делу критикуется за отход от основополагающего требования *UDRP* о наличии прав на товарный знак у заявителя; подчеркивается, что жалобы, основанные исключительно на географических указаниях, не должны удовлетворяться, за исключением случаев, когда заявитель обладает законодательно закрепленными правами, например, как это имело место в делах, инициированных Городским советом Глазго или Правительством Канады[23].

Другой особенностью процедуры рассмотрения доменных споров по правилам *UDRP* являются документальный характер и предусмотренная возможность вынесения решения при отсутствии явно выраженной позиции ответчика. В соответствии с п. 13 Правил *UDRP* проведение устных слушаний (*in-person hearings*), включая телеконференции, видеоконференции или онлайн-заседания, не допускается, за исключением случаев, когда административная комиссия по собственному усмотрению признает такое слушание необходимым для вынесения решения[24].

Кроме того, согласно 5(a) Правил *UDRP* ответчик обязан представить письменный ответ на жалобу в течение 20 дней с момента начала разбирательства. Если ответ в установленный срок не представлен и отсутствуют исключительные обстоятельства, свидетельствующие о необходимости продления установленного срока (в частности, если ответчик не ходатайствовал о продлении срока или между сторонами не было заключено письменное соглашение), административная комиссия вправе разрешить спор на основе материалов, представленных заявителем, что прямо вытекает из п. 5(e) Правил *UDRP*[25].

Несмотря на то что в п. 4(a)(i) *UDRP* упоминается проведение обязательных административных слушаний (*mandatory administrative proceeding*), термин «слушание» в данном контексте не следует интерпретировать в традиционном для русского языка значении как «устное разбирательство». В оригинале *UDRP* четко различает понятия *proceeding* («процедура») и *hearing*

---

21 Mueller, M. (2002). *Success by default: A new profile of domain name trademark disputes under ICANN's UDRP* (p. 14). Syracuse University School of Information Studies. https://cent.ischool.syr.edu/wp-content/uploads/2014/05/markle-report-final.pdf

22 Barcelona.com, Inc. v. Excelentisimo Ayuntamiento de Barcelona, WIPO Case No. D2000-0505 (2000), https://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0505.html

23 Mueller, M. (2002). *Success by default: A new profile of domain name trademark disputes under ICANN's UDRP* (p. 14). Syracuse University School of Information Studies. https://cent.ischool.syr.edu/wp-content/uploads/2014/05/markle-report-final.pdf

24 ICANN. (n.d.). Rules for Uniform Domain Name Dispute Resolution Policy. https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/rules-for-uniform-domain-name-dispute-resolution-policy-the-rules-11-03-2015-en

25 Ibid.

(«слушание»)[26]. В пункте 4(a)(i) *UDRP* речь идет именно о начале письменной процедуры рассмотрения спора.

Документальное производство, отсутствие обязательных устных слушаний и возможность вынесения заочного решения в достаточно короткий срок представляют собой практическое воплощение модели упрощенного разбирательства, заложенной в основу процедуры *UDRP.* Такая модель соответствует целям *UDRP* как ускоренного и формализованного механизма разрешения доменных споров и передачи доменных имен правообладателям товарных знаков, обусловленного в первую очередь спецификой доменных имен как технических и экономически значимых объектов, доступ к которым регулируется в условиях ограниченного ресурса и высокой степени автоматизации.

Правовая природа разбирательства по *UDRP*

Период наибольшего исследовательского внимания к разбирательству по правилам *UDRP* пришелся на первые годы после ее принятия. Именно в начале 2000-х гг. в зарубежной литературе была заложена теоретическая основа проблематики применения *UDRP:* ряд авторов, включая *Мильтона Мюллера*[27]*, Майкла Гейста* (Geist, 2002) и др., детально анализировали появлявшуюся практику арбитражных центров, оценивая содержание и эффективность применяемого механизма разрешения доменных споров.

В зарубежной литературе преобладает мнение о том, что *UDRP* представляет собой особую форму альтернативного разрешения споров (*Alternative Dispute Resolution, ADR*), обладающую рядом черт арбитражного разбирательства. Как справедливо отмечает Елизабет Вудард (*Elizabeth Woodard*), категория *ADR* охватывает широкий спектр механизмов, в рамках которых стороны сознательно выбирают процедуру, отличающуюся от традиционного судебного процесса. При этом среди всех форм *ADR* процедура по правилам *UDRP* наиболее близка по своей природе к арбитражу. Однако, как подчеркивает автор, *UDRP* имеет гибридное происхождение, что обусловило ряд отличий от классической арбитражной модели (Woodard, 2009, pp. 1183–1184). Разбирательство по правилам *UDRP* квалифицируется в качестве формы *ADR* либо особой разновидности арбитражного разбирательства и в других авторитетных зарубежных исследованиях (Geist, 2002; Cortés Diéguez, 2008; Ware, 2002).

Как уже указывалось (Yakushev et al., 2017, p. 174), обращает на себя внимание то, что и в *UDRP,* и в Правилах *UDRP* процедура рассмотрения доменного спора поименована как «административная процедура», а лица, ее осуществляющие, — как «административная комиссия» («административная группа»). В русскоязычной литературе это стало обоснованием позиции, согласно которой арбитражные учреждения, аккредитованные на рассмотрение доменных споров, не являются полноценными арбитражными учреждениями (третейским судом), в подтверждение чего приводятся ссылки на «невозможность применения законов, регулирующих

[26] Ср. соответствующие положения английской и русской версий *UDPR*: ICANN. *Uniform Domain Name Dispute Resolution Policy* (Aug. 26, 1999, as amended Feb. 21, 2024). https://www.icann.org/resources/pages/policy-2024-02-21-en и ICANN. *Единая политика разрешения споров о доменных именах* (UDRP) (утв. 26.08.1999, в ред. 24.02.2024). https://www.icann.org/resources/pages/policy-2024-07-01-ru

[27] Mueller, M. (2002). *Success by default: A new profile of domain name trademark disputes under ICANN's UDRP* (p. 14). Syracuse University School of Information Studies. https://cent.ischool.syr.edu/wp-content/uploads/2014/05/markle-report-final.pdf

обязанности арбитров; неокончательность вынесенного решения; ограниченный характер средств правовой защиты и т. п.» (Terent'eva, 2020b, p. 135).

С учетом указанного в российской юриспруденции превалирует мнение, что разбирательство доменных споров в таких учреждениях представляет собой иную, новую процедуру, неизвестную ранее российскому законодательству и юридической науке. В обсуждениях разбирательство доменных споров в соответствии с *UDRP* и Правилами *UDRP* нередко характеризовалось как *некая административная процедура, выполняемая непубличным, частным органом,* и т. д.

Между тем оставалось без внимания то, что по сути доменный спор представляет собой частноправовой спор об имущественных правах. А указание в документах *ICANN* на «административность» процедуры и состава лиц, разрешающих доменный спор, проистекает из особенности доменных споров, касающейся прежде всего исполнения вынесенных по этим делам арбитражных решений, т. е. из возможности исполнения решения без обращения за содействием к государственным институтам, включая судебные органы. Иными словами, процедура *UDRP* представляет собой форму саморегулирования, в рамках которой решение арбитража подлежит прямому исполнению регистратором.

Как известно, при отсутствии добровольного исполнения обычного арбитражного решения заинтересованной стороне нужно обратиться в государственный суд за исполнительным листом на принудительное исполнение этого решения. Применительно к доменным спорам в этом нет необходимости: при удовлетворении требования заявителя (правообладателя товарного знака) об отмене регистрации доменного имени, передаче домена другому лицу и т. д. вынесенное арбитражным учреждением решение приводится в исполнение регистратором посредством внесения соответствующий записи в реестр доменных имен. Подобное исполнение решения, нехарактерное для исполнения арбитражных решений, имеет отчетливый административно-властный оттенок, что и оказало серьезное влияние на используемую в *UDRP* и Правилах *UDRP* терминологию.

Вместе с тем специфика исполнения вынесенного по доменному спору решения не должна рассматриваться в качестве основания для исключения данной процедуры из числа разновидностей арбитражных разбирательств. С такой позицией соглашается и Л. В. Терентьева, подчеркивающая: «Наличие принудительного механизма исполнения решений арбитражных центров не является принципиальным отличием от процедуры арбитражного разбирательства. Решения, вынесенные коммерческими арбитражными судами, должны исполняться добровольно, и отсутствие необходимости обращения за исполнением соответствующих решений к государственным судам не должно являться критическим доводом в пользу позиции, в рамках которой ученые отказывают арбитражным центрам, рассматривающим споры по процедуре *UDRP*, в праве признаваться арбитражными судами» (Terent'eva, 2020b, pp. 134–135). Кроме того, немаловажно, что механизм принудительного исполнения по *UDRP* не является безусловным: в соответствии с п. 4(k) *UDRP* в течение 10 дней проигравшая сторона вправе обратиться в национальный (государственный) суд, заявив ходатайство о приостановлении исполнения решения арбитражного центра[28].

В пользу арбитражно-правовой природы процедуры *UDRP* свидетельствует и тот факт, что в случае рассмотрения спора коллегиальным составом административной комиссии сторонам предоставляется возможность участвовать в формировании состава комиссии путем выдвижения кандидатур арбитров. Согласно п. 6(c)–(e) Правил *UDRP* каждая из сторон может

[28] Подробно об этой особенности процедуры *UDRP* см. раздел «Особенности определения компетентного арбитражного центра и взаимодействия с национальными судами» настоящей статьи.

назначить по одному арбитру из утвержденного перечня, после чего третий арбитр назначается соответствующим арбитражным центром из числа оставшихся кандидатов[29]. Такая конструкция отвечает принципам арбитражного разбирательства, предполагающим участие сторон в формировании состава третейского суда, и опровергает утверждения об административной природе данной процедуры.

В свою очередь, отсутствие у сторон возможности повлиять на назначение арбитра в случае единоличного разбирательства (п. 6(b) Правил *UDRP*)[30] также не противоречит арбитражной природе процедуры, а лишь отражает специфику упрощенного механизма разрешения доменного спора. В этой ситуации, как и в ряде других форм арбитража, стороны заранее соглашаются с правилами формирования состава суда, включая возможность назначения арбитра администратором спора (например, Центром ВОИС по арбитражу и посредничеству) без их непосредственного участия. Такая модель широко применяется в практике коммерческого арбитража при рассмотрении споров с незначительной сложностью или в целях сокращения временны́х и финансовых затрат. Соответственно, даже в случае единоличного рассмотрения доменного спора и, как следствие, отсутствия у сторон возможности участвовать в выборе арбитра сохраняются черты, сближающие *UDRP* с арбитражем. При этом процедура *UDRP* действительно предусматривает ряд отличий от традиционного арбитражного разбирательства:

1) *публичная доступность вынесенного решения* (его текст публикуется в открытом доступе), что обусловлено целью сформировать единообразную практику, обеспечить предвидимость (предсказуемость) арбитражных решений по данным спорам;
2) *возможность обращения в национальный суд для повторного рассмотрения жалобы* (а не ее пересмотра);
3) *отсутствие между сторонами предшествующих договорных отношений и традиционной арбитражной оговорки*[31];
4) *ограниченное раскрытие информации и доказательств в рамках разбирательства.*

Указанные особенности хотя и отличают процедуру *UDRP* от классических моделей коммерческого арбитража, но не затрагивают ее частноправовую сущность и не влияют на ее правовую природу.

Тем не менее в деле *Dluhos v. Strasberg* (2003) был сделан иной вывод относительно правовой природы разбирательства по правилам *UDRP*[32]. Истец, зарегистрировавший доменное имя *leestrasberg.com,* отсылавшее к имени известного педагога по актерскому мастерству Ли Страсберга, столкнулся с жалобой, поданной наследниками Страсберга в один из арбитражных центров в порядке *UDRP.* В соответствии с процедурой было вынесено решение о передаче доменного имени наследникам в связи с недобросовестностью действий по регистрации доменного имени. *Dluhos* попытался оспорить решение в федеральном суде США, заявляя о неконституционности процедуры и отсутствии у *UDRP* признаков арбитража.

---

29 ICANN. (n.d.). Rules for Uniform Domain Name Dispute Resolution Policy. https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/rules-for-uniform-domain-name-dispute-resolution-policy-the-rules-11-03-2015-en

30 Ibid.

31 Подробнее про арбитражную оговорку см. разд. «Механизм формирования согласия сторон на рассмотрение спора в аккредитованном ICANN арбитражном учреждении» настоящей статьи.

32 Dluhos v. Strasberg, 321 F.3d 365 (3d Cir. 2003).

Окружной суд первой инстанции отклонил его иск, применив к решению арбитражного центра стандарт «крайнего судебного уважения» (*extremely deferential judicial review*) в соответствии с Федеральным законом об арбитраже (*Federal Arbitration Act, FAA*)[33].

Впрочем, апелляционный суд отменил данное решение, сделав вывод, что *UDRP* не подпадает под понятие арбитража в смысле *FAA.* Суд подчеркнул, что *UDRP* не является обязательным этапом до обращения в суд, не заменяет судебного разбирательства и не требует согласия сторон на арбитраж в традиционном понимании[34]. Тем самым процедура *UDRP* была охарактеризована как механизм быстрой и независимой квазисудебной оценки, но не как арбитраж в смысле федерального законодательства США.

Правильность подобных выводов вызывает обоснованные сомнения. Аргументация апелляционного суда основывалась преимущественно на формальном отсутствии арбитражного соглашения между сторонами в его классическом выражении. Однако специфика доменных споров, как это будет подробно проанализировано далее, изначально исключает возможность существования прямых договорных отношений между владельцем доменного имени и правообладателем товарного знака. С учетом этого традиционная модель арбитражной оговорки, зафиксированной в договоре между сторонами, в этих условиях нереализуема.

Вместе с тем нельзя игнорировать поддерживаемую в научной литературе допустимость альтернативных форм выражения согласия на арбитраж, к числу которых относят молчаливое или одностороннее волеизъявление. Иными словами, формальная ссылка на отсутствие классической арбитражной оговорки не может служить достаточным основанием для отказа в признании *UDRP* формой арбитража.

Исходя из сказанного, нет никаких серьезных оснований для характеристики разбирательства доменных споров в соответствии с *UDRP* и Правилами *UDRP* как имеющего неясную правовую природу. Взвешенной представляется позиция тех авторов, которые относят рассматриваемую процедуру к третейскому (арбитражному) разбирательству (Terent'eva, 2020b, p. 135).

Критика *UDRP* и ее обоснованность

В зарубежной литературе процедура *UDRP* неоднократно подвергалась серьезной критике. Наиболее часто встречаются обвинения в предвзятости процедуры в пользу правообладателей товарных знаков (Cortés Diéguez, 2008, pp. 353–355; Woodard, 2009, pp. 1187–1189; Geist, 2002, p. 905); ссылка на языковые трудности, возникающие в связи с необходимостью ведения разбирательства на языке регистрации доменного имени (Cortés Diéguez, 2008, p. 355); упор на высокую стоимость процедуры (Cortés Diéguez, 2008, pp. 355–356); указания на ограниченный срок представления возражений (Cortés Diéguez, 2008, p. 356), а также практику вынесения решения без участия ответчика (Woodard, 2009, pp. 1191–1192). Серьезное внимание уделяется также отсутствию механизма апелляционного пересмотра решений в рамках самой системы *UDRP* (Kelley, 2002, pp. 194–203; Woodard, 2009, pp. 1200–1202).

Тщательный анализ поименованных критических замечаний позволил сделать следующие выводы.

Предвзятость процедуры UDRP в пользу правообладателей товарных знаков является одним из наиболее часто озвучиваемых упреков. Аргументация критиков строится преимущественно на доводах, касающихся высокой доли удовлетворенных жалоб (до 93% за третий

[33] Federal Arbitration Act, 9 U.S.C. §§ 1–16 (1925).

[34] *Dluhos*, 321 F.3d.

квартал 2025 г.[35]), различия в процессуальных сроках, а также самостоятельного выбора заявителем арбитражного центра и оплаты всех сборов, что, по мнению критиков, потенциально стимулирует арбитров к принятию решений в пользу заявителей (Cortés Diéguez, 2008, pp. 353-355; Woodard, 2009, pp. 1187–1189; Geist, 2002, p. 905). На наш взгляд, подобная трактовка статистических и процедурных аспектов не всегда учитывает специфическую правовую природу *UDRP* как формы *ADR* с предельно узкой сферой применения — борьбой с киберсквоттингом.

Во-первых, как справедливо отмечает *E. Вудард,* сама по себе высокая доля решений в пользу заявителей не является убедительным доказательством предвзятости системы (Woodard, 2009, p. 1189). Статистика, на которую ссылаются критики, не учитывает отсутствие возражений со стороны ответчика, что обусловлено спецификой доменных споров: ответчиками, как правило, являются массовые киберсквоттеры, не заинтересованные в полноценной защите своей позиции или не обладающие серьезными правовыми аргументами, обосновывающими их добросовестность. При этом различия в процедурных сроках для заявителя и ответчика (20 дней с даты начала разбирательства для представления ответчиком возражений в соответствии с п. 5(a) Правил *UDRP* против формального отсутствия срока на подачу жалобы заявителем) отражают скорее необходимость процессуального баланса между скоростью разбирательства и доступностью защиты, чем институциональную предвзятость. Ответчик не лишен права ходатайствовать о продлении срока для подачи возражения: в соответствии с п. 5(b) Правил *UDRP* ему автоматически предоставляется четыре дополнительных календарных дня; согласно п. 5(e) Правил *UDRP* он вправе ходатайствовать о продлении на более длительный срок. Кроме того, ни одно исследование не подтвердило, что продление срока на представление возражений принципиально могло бы повлиять на результат дела для добросовестного ответчика (Woodard, 2009, p. 1191).

Во-вторых, модель, при которой заявитель самостоятельно выбирает аккредитованный арбитражный центр, действительно может создавать определенные риски восприятия зависимости арбитров от заявителя, несмотря на то что сам заявитель не назначает ни единоличного арбитра, ни всех членов комиссии в случае коллективного рассмотрения.

Майкл Гейст, описывая данную проблему, указывал, что изначально аккредитация всего лишь нескольких арбитражных центров («провайдеров *ICANN*» в терминологии автора) была направлена на создание конкурентной среды. Однако уже в начале 2000-х гг. предсказание об эффекте *forum shopping,* т. е. о выборе «провайдера» с наиболее предсказуемой позицией в пользу заявителей, сбылось (Geist, 2002, p. 905). Исследователь прямо называл возможность выбора «провайдера *ICANN*» заявителем «встроенным элементом механизма *UDRP*» (Geist, 2002, p. 910).

Вместе с тем необходимо учитывать, что данный вывод был сделан более двух десятилетий назад и, очевидно, нуждается в пересмотре. Сегодня выбор аккредитованного *ICANN* арбитражного центра, как правило, продиктован не столько предполагаемой «лояльностью», сколько репутацией арбитражного учреждения, эффективностью процедур, языковыми и региональными предпочтениями, а также размером сборов.

Тем не менее вопрос возможной предвзятости процедуры *UDRP* получает дополнительный оттенок в свете отсутствия эффективных механизмов, направленных на предотвращение злоупотреблений со стороны заявителей. Как справедливо отмечает М. Мюллер, даже если подобные истцы и проигрывают дело, их потери сводятся к оплате арбитражного разбирательства,

[35] См. статистические данные в отчете: GigaLaw. (2025). *GigaLaw's domain dispute digest.* https://static1.squarespace.com/static/58febdfcbf629aa913a85974/t/6904cb8b6d168173f3909363/1761921931694/2025-q3-domain-dispute-digest.pdf).

в то время как никакие дополнительные санкции за подачу недобросовестной жалобы не предусмотрены ни *UDRP,* ни Правилами *UDRP.* Поскольку *UDRP* не устанавливает компенсационных или карательных последствий для недобросовестного заявителя, то единственным предусмотренным способом реагирования на подобные действия является признание заявителя «обратным захватчиком доменных имен» (*reverse domain name hijacker*), что носит, скорее, декларативный характер и практически не влечет правовых последствий[36]. В этой части критику следует признать обоснованной, поскольку отсутствие действенных инструментов для сдерживания недобросовестных заявителей на самом деле может создавать дисбаланс и способствовать предъявлению необоснованных жалоб со стороны крупных правообладателей.

Высокая стоимость процедуры UDRP также является одним из объектов критики: по мнению некоторых исследователей, она может выступать сдерживающим фактором для добросовестных ответчиков, особенно если спор касается небольшого количества доменных имен и не предполагает значительного коммерческого интереса. Анализ тарифов различных аккредитованных *ICANN* арбитражных центров показывает определенную вариативность уровня сборов, при этом общая финансовая нагрузка действительно может быть ощутимой для частных лиц и малого бизнеса[37].

Важно, что расходы между сторонами распределяются ассиметрично: если заявитель выбирает одного арбитра, он полностью оплачивает стоимость процедуры. Однако если ответчик требует назначения коллегии из трех арбитров, он обязан разделить с заявителем расходы на арбитров пополам (п. 19 Правил *UDRP*)[38]. Следовательно, добросовестные ответчики, желающие обеспечить максимально возможно нейтральное рассмотрение дела, могут столкнуться с существенными издержками.

Это может быть особенно проблематичным на фоне ситуации, когда инициатором спора выступает крупная корпорация. Так, для транснациональных компаний расходы в несколько тысяч долларов представляют собой незначительную сумму. Это, в свою очередь, может создавать риск злоупотребления процедурой *UDRP* в целях «обратного захвата доменных имен» (*reverse domain name hijacking*), в частности в случаях, когда ответчиком выступает физическое лицо или малый бизнес, неспособный покрыть затраты на защиту своих прав в рамках *UDRP*.

---

[36] Mueller, M. (2002). *Success by default: A new profile of domain name trademark disputes under ICANN's UDRP* (p. 14). Syracuse University School of Information Studies. https://cent.ischool.syr.edu/wp-content/uploads/2014/05/markle-report-final.pdf

[37] Наиболее авторитетные арбитражные центры, такие как *WIPO, FORUM, ADNDRC* и *CIIDRC*, проводят сопоставимую ценовую политику. Например, базовая плата за рассмотрение спора одним арбитром по жалобе, включающей от одного до пяти доменов, колеблется от 1300 до 1500 долл. США. При выборе коллегиального состава стоимость возрастает до 2800–4000 долл. *ADNDRC* и *CIIDRC*, как правило, предлагают более доступные условия, особенно при рассмотрении дел с участием одного арбитра. В некоторых случаях также предусмотрены дополнительные сборы, например невозвратный регистрационный взнос (*CIIDRC*) или комиссии за оплату. Подробнее см. официальные сайты арбитражных центров: WIPO. (n.d.). *Schedule of fees in WIPO domain name dispute resolution proceedings.* Retrieved April 14, 2025, from https://www.wipo.int/amc/en/domains/fees/index.html; ADNDRC. (n.d.). *Uniform Domain Name Dispute Resolution Policy.* Retrieved April 14, 2025, from https://www.adndrc.org/udrp; CIIDRC. (n.d.). *UDRP fee schedule.* Retrieved April 14, 2025, from https://ciidrc.org/how-it-works/fee-schedule/; FORUM. (n.d.). *UDRP fees per FORUM's supplemental Rule 17.* Retrieved April 14, 2025, https://www.adrforum.com/assets/resources/domain/udrp/UDRP%20Fee%20Schedule%20Final.pdf

[38] ICANN. (n.d.). Rules for Uniform Domain Name Dispute Resolution Policy. https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/rules-for-uniform-domain-name-dispute-resolution-policy-the-rules-11-03-2015-en

Тем не менее в сравнении с судебным разбирательством в национальных судах стоимость процедуры *UDRP* остается относительно невысокой. Даже при участии трех арбитров общая сумма редко превышает 5000 долл., что зачастую существенно ниже расходов на оплату государственных пошлин, юридическое сопровождение и потенциальные убытки от затяжного процесса в рамках традиционного судебного разбирательства. Кроме того, *UDRP* предлагает оперативное рассмотрение спора и стандартизированные, понятные механизмы, что делает данную процедуру привлекательной альтернативой. В этом смысле затраченные суммы представляют собой плату за скорость, процедурную эффективность и возможность законным способом вернуть доменное имя без необходимости выкупать его у киберсквоттеров по спекулятивной цене.

Языковые трудности называют еще одним недостатком процедуры *UDRP:* критики, указывающие на языковой барьер, опираются на положение, согласно которому по умолчанию разбирательство ведется на языке соглашения о регистрации доменного имени (п. 11(a) Правил *UDRP*)[39]. Таким образом, если регистрация была осуществлена, например, через китайского регистратора, языком процедуры может быть китайский, даже если обе стороны не владеют этим языком. Это особенно актуально для ответчиков, которые могут не понимать содержание уведомлений и требований, что теоретически снижает уровень их процессуальной защиты.

Впрочем, остается без должного внимания то, что данное правило не является жестким: пункт 11(a) Правил *UDRP* прямо наделяет комиссию полномочием изменить язык разбирательства, «принимая во внимание обстоятельства дела». На практике комиссия нередко разрешает заявителю подавать документы на английском языке. Более того, она также вправе запрашивать частичный или полный перевод документов на язык процедуры (п. 11(b) Правил *UDRP*)[40].

Следовательно, хотя языковые затруднения и могут возникать во время разбирательства по правилам *UDRP,* существующий механизм позволяет обеспечить дополнительную защиту для недоминирующей стороны в случае возникновения языковых сложностей.

Отсутствие механизма апелляционного пересмотра решений считается одним из наиболее существенных недостатков процедуры *UDRP.* На данный пробел неоднократно указывалось уже в первые годы функционирования *UDRP,* и с тех пор вопрос остается нерешенным.

Критики подчеркивают, что отсутствие апелляционного органа внутри системы снижает предсказуемость и единообразие решений, особенно с учетом того, что решения выносятся различными арбитрами в разных арбитражных центрах. Среди возможных решений предлагается создание независимого внутреннего апелляционного органа, который мог бы не только рассматривать апелляции, но и формировать обязательные для нижестоящих составов стандарты и прецеденты, тем самым способствуя согласованности практики [Kelley, 2002, pp. 194–203].

Возражая подобным критическим замечаниям, надо отметить, что в контексте концепции *ADR* подобная система вовсе не обязательна.

В то же время введение апелляционного органа в процедуру *UDRP* усложнит и существенно удорожит эту процедуру. Кроме того, нельзя игнорировать и возможность последующего обращения в национальный суд, что, как будет показано далее, выступает своеобразным внешним механизмом нового рассмотрения спора. Иными словами, проигравшая сторона вовсе не лишена определенных правовых гарантий.

---

[39] ICANN. (n.d.). Rules for Uniform Domain Name Dispute Resolution Policy. https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/rules-for-uniform-domain-name-dispute-resolution-policy-the-rules-11-03-2015-en

[40] Ibid.

Подводя промежуточный итог, следует подчеркнуть, что, несмотря на обозначенные критические замечания, даже наиболее последовательные оппоненты признают, что процедура *UDRP* в целом демонстрирует высокую эффективность и справляется с поставленными задачами. Так, М. Гейст подчеркивал, что *UDRP* «является важной моделью для разрешения споров в других областях электронной коммерции» (Geist, 2002, pp. 903–904).

Кроме того, надо учитывать, что многие критики при изложении своей аргументации зачастую игнорируют природу *UDRP* как специализированной формы *ADR* в интернет-сфере. В связи со сказанным абсолютно справедливо замечание Е. Вудард о том, что многие критические замечания в адрес *UDRP* проистекают не столько из дефектов самой процедуры, сколько из недостаточного понимания природы *ADR* (Woodard, 2009, p. 1187). Ограничения в сфере применения *UDRP,* критикуемые в литературе, представляют собой не недостатки, а результат осознанного выбора в пользу максимально быстрой, недорогой и унифицированной процедуры, применимой к узкому классу вопиющих случаев нарушения исключительных прав на товарные знаки в интернет-среде.

Арбитрабельность доменных споров и компетенция аккредитованных *ICANN* арбитражных центров

На сегодняшний день широкое распространение получило понимание *арбитрабельности как свойства спора, которое позволяет ему быть предметом третейского разбирательства* (Skvortsov, 2017, p. 118). В связи с этим В. В. Еремин отмечает: «В широком смысле арбитрабельность включает в себя вопросы действительности и существования арбитражного соглашения. В узком смысле арбитрабельность — это категория споров, которые могут передаваться в арбитраж» (Eremin, 2019, p. 99). В свою очередь О. Ю. Скворцов подчеркивает, что «укоренение доктрины арбитрабельности является одним из эффективных способов определения круга спорных правоотношений, которые могут охватываться третейским (арбитражным) соглашением и, следовательно, подпадают под юрисдикцию третейских судов» (Rozhkova et al., 2019).

Несмотря на то что в *UDRP* разбирательство доменных споров обозначено как «административные слушания», оно проводится арбитражными учреждениями (провайдерами), которые получили специальную аккредитацию *ICANN* на разрешение доменных споров.

На сегодняшний день статус аккредитованного *ICANN* арбитражного центра имеют пять организаций[41]. В их числе Центр ВОИС по арбитражу и посредничеству, который занимает ведущее место среди аккредитованных *ICANN* арбитражных институтов как по числу рассматриваемых доменных споров (более 6000 дел в год[42]), так и по качеству вырабатываемой правоприменительной практики.

[41] Список аккредитованных арбитражных институтов доступен на сайте *ICANN*: ICANN. (б.д.). Список одобренных поставщиков услуг разрешения споров. https://www.icann.org/ru/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/list-of-approved-dispute-resolution-service-providers-25-02-2012-ru

[42] В 2024 г. в Центр ВОИС по арбитражу и посредничеству было подано 6168 обращений о рассмотрении доменного спора в порядке, предусмотренном *UDRP*. Данный показатель лишь незначительно уступает количеству обращений, поданных в 2023 г. (6192 жалобы), который, в свою очередь, остается рекордным с момента введения процедуры *UDRP* в 1999 г. Согласно ежегодному отчету ВОИС, с 2013 г. наблюдается устойчивая тенденция существенного роста числа доменных споров: так, за 10 лет (с 2013 по 2023 г.) данный показатель увеличился более чем в 2,3 раза, что свидетельствует о стабильном росте востребованности указанной процедуры (WIPO. (2025). *WIPO domain name report 2024: UDRP case filings remain strong*. https://www.wipo.int/amc/en/domains/news/2025/news_0001.html).

Важно отметить (и это признает в своей работе Л. В. Терентьева (Terent'eva, 2020b, p. 135)), что многие аккредитованные *ICANN* провайдеры одновременно уполномочены на разрешение и урегулирование иных (коммерческих) споров[43]. На наш взгляд, это подтверждает тезис о том, что доменные споры относятся к числу дел, обладающих свойством арбитрабельности, а процедура их рассмотрения подпадает под понятие «арбитражное разбирательство».

Вместе с тем в целях настоящей статьи особого внимания заслуживает тот момент, что компетенция аккредитованных *ICANN* арбитражных центров по рассмотрению доменных споров в соответствии с *UDRP* не основывается на традиционном двустороннем арбитражном соглашении, заключаемом спорящими сторонами, а вытекает из *специфики регистрации доменных имен*, что выражается в следующем.

ICANN, как уже было отмечено, аккредитует администраторов *TLD* для обеспечения бесперебойной работы *DNS.* При этом не все администраторы *TLD* сами оказывают услуги по регистрации доменных имен в реестре. Нередко администратор *TLD,* сам не являясь регистратором (прямая регистрация пользователем доменного имени через него невозможна), предоставляет право регистрации в реестре иным лицам – регистраторам, которые получают у этого администратора *TLD* соответствующую аккредитацию. Например, как уже отмечалось, Координационный центр доменов *.RU*/.РФ не выполняет функции регистратора, ограничиваясь аккредитацией уполномоченных организаций – регистраторов, которые непосредственно вносят соответствующие сведения в реестр доменов *.ru* и .рф. В то же время в доменной зоне *.de* допускается как опосредованная регистрация доменов второго уровня через аккредитованных членов товарищества *DENIC eG,* так и непосредственное заключение договора между заинтересованным в регистрации домена лицом и администратором *ccTLD.*

В доменах *new gTLD* также могут быть реализованы различные модели взаимодействия между администратором *new gTLD* и лицами, заинтересованными в регистрации на себя домена второго уровня. Например, в доменной зоне *.deti* регистрация доменных имен второго уровня возможна исключительно через аккредитованных регистраторов[44] без возможности прямого обращения к администратору *new gTLD.* В то же время для доменной зоны *.tatar* предусмотрена более гибкая модель: заинтересованное лицо может зарегистрировать доменное имя второго уровня как через аккредитованного регистратора, так и путем подачи заявки непосредственно на сайте администратора *new gTLD*[45]. Однако сто́ит признать, что в большинстве случаев администраторы *gTLD* и *new gTLD* осуществляют регистрацию доменов в соответствующих доменных зонах посредством аккредитованных регистраторов.

Важно отметить, что в модели *DNS* субъектами отношений по поводу регистрации доменного имени указаны следующие фигуры.

- *Registrar* — лицо, которое вносит сведения о доменном имени второго уровня в реестр соответствующего *TLD.* То есть это либо аккредитованный регистратор, либо аккредитованный *ICANN* администратор *TLD,* если он сам непосредственно осуществляет регистрацию доменных имен.

[43] См., например, процедуры альтернативного разрешения споров ВОИС: WIPO. (n.d.). *WIPO ADR procedures.* https://www.wipo.int/amc/en/center/wipo-adr.html

[44] Таких регистраторов в настоящее время четыре (Фонд «Разумный Интернет». (б.д.). *Зарегистрировать домен.* https://dotdeti.ru/foruser/regdomain/).

[45] См. подробнее: Координационный центр Регионального домена Республики Татарстан. (б.д.). *Зарегистрировать домен.* https://domain.tatar/users/how-to-register.php

- *Registrant* — лицо, на чье имя зарегистрировано данное доменное имя в реестре. В зарубежной литературе его иногда обозначают как *owner* (т. е. собственник, владелец домена) (Snow, 2005, p. 84; Nathenson, 1997, p. 963), однако с учетом положений отечественной доктрины, допускающей возникновение права собственности только на материальные вещи, следует говорить об обладателе прав на доменное имя или, иными словами, «*правообладателе доменного имени*» — именно это понятие и будет использоваться далее в настоящей статье. К сожалению, в отечественной практике исторически сложилась традиция обозначать это лицо термином «администратор доменного имени»[46], что в контексте модели *DNS* неверно ввиду использования нижеследующих обозначений.
- *Admin* (сокр. от *administrator*) — администратор (со стороны правообладателя доменного имени), т. е. контактное лицо по вопросам администрирования домена, а также размещения информации и материалов на информационном ресурсе, размещенном на данном домене. В качестве администратора, таким образом, могут выступать, например, веб-разработчик или команда копирайта, т. е. те, кто управляет контентом сайта, является лицом, ответственным перед правообладателем доменного имени, или с кем правообладатель заключил договор на использование доменного имени, и т. д.
- *Tech* (сокр. от *technical administrator*) — лицо, отвечающее за техподдержку (со стороны правообладателя доменного имени), т. е. контактное лицо по техническим вопросам. Это может быть, например, сотрудник (подразделение) правообладателя – юридического лица или самостоятельная компания, осуществляющая техподдержку доменного имени на основании соответствующего договора.

Таким образом, лицо, заинтересованное в регистрации на себя доменного имени второго уровня *в доменных зонах gTLD и new gTLD*, обращается к соответствующему *registrar,* вступает с ним в отношения, которые оформляются договором об оказании услуг по регистрации доменного имени, являющимся по правовой природе договором присоединения. Неотъемлемой частью договоренностей в этом случае становится согласие заинтересованного лица на соблюдение политик *ICANN,* регулирующих функционирование конкретной доменной зоны, включая *UDRP* и Правила *UDRP.* Присоединяясь к договору, заинтересованное лицо (впоследствии — *registrant*) тем самым соглашается с компетенцией аккредитованных *ICANN* арбитражных центров по рассмотрению споров, возникающих в отношении регистрируемого доменного имени. Отсюда можно заключить, что *registrar* и *registrant* связаны арбитражным соглашением, в силу которого все споры, касающиеся зарегистрированного доменного имени, подлежат рассмотрению в предусмотренном *UDRP* порядке в пределах компетенции соответствующего арбитражного института.

[46] Термин «администратор доменного имени» был использован в Справке по вопросам, возникающим при рассмотрении доменных споров № СП-21/4 (см.: Постановление Президиума Суда по интеллектуальным правам «Об утверждении справки по вопросам, возникающим при рассмотрении доменных споров» от 28 марта 2014 г. № СП-21/4). В настоящее время, данный термин также активно используется в судебной практике при рассмотрении как доменных споров (см.: постановление Суда по интеллектуальным правам от 24 сентября 2024 по делу № А40-188058/2023; постановление Суда по интеллектуальным правам от 26 мая 2025 по делу № А40-166754/2024), так и споров о нарушении авторских прав в Интернете, где поднимается вопрос об установлении владельца сайта (см.: постановление Суда по интеллектуальным правам от 26 сентября 2023 по делу № А40-243692/2022).
Тем не менее необходимо отметить, что наряду с термином «администратор доменного имени» в российской судебной практике также встречается синонимичный термин «владелец доменного имени» (см.: постановление Суда по интеллектуальным правам от 4 июня 2025 по делу № А20-3208/2024; постановление Суда по интеллектуальным правам от 23 июля 2025 по делу № А40-53482/2024).

В том случае, если лицо заинтересовано в регистрации доменного имени *в доменной зоне ccTLD*, применимость той или иной процедуры разрешения возможного спора будет напрямую зависеть от регламентирующих документов, утвержденных администратором соответствующего *ccTLD*. Здесь возможны три варианта, допустимость которых упоминалась ранее.

1. Некоторые администраторы *ccTLD* в соответствующих регламентирующих документах предусматривают возможность рассмотрения спора как в государственном, так и в третейском суде (в том числе по процедуре *UDRP* или по ее национальной модификации (*modified UDRP*)). Это правило закреплено для таких доменных зон как, например, *.br* (Бразилия), *.es* (Испания).
2. В ряде случаев регламентирующие документы администратора *ccTLD,* напротив, прямо закрепляют обязательность применения *UDRP,* что означает обязательность передачи возникшего доменного спора в аккредитованный *ICANN* арбитражный центр. Такое правило предусмотрено, например, для доменной зоны *.ai* (Ангилья). Применительно к этой ситуации будет правильным вывод А. Е. Голубева, согласно которому использование альтернативного механизма разрешения доменного спора (в данном случае по модели *UDRP*) возможно, лишь когда это прямо предусмотрено договором об оказании услуг по регистрации доменного имени (Golubev, 2022, p. 121).
3. Допустимо и полное отсутствие каких-либо упоминаний о специальных процедурах разрешения доменных споров в регламентирующих документах администратора *ccTLD.* Так, для доменных зон *.ru* и .рф регламентирующие документы не предусматривают отсылок к *UDRP* или иным альтернативным процедурам разбирательств, вследствие чего споры, связанные с доменами второго уровня, зарегистрированными в этих *ccTLD,* подлежат разрешению в порядке, установленном действующим законодательством Российской Федерации.

Механизм формирования согласия сторон на рассмотрение спора в аккредитованном *ICANN* арбитражном учреждении

Вышеизложенное со всей однозначностью свидетельствует о том, что правообладатель товарного знака, полагающий, что его права нарушены регистрацией и (или) использованием товарного знака в принадлежащем иному лицу доменном имени, *формально не связан арбитражным соглашением, связывающим registrar и registrant* (правообладателя доменного имени): применительно к этому соглашению правообладатель товарного знака является третьим лицом.

Отсутствие классического двустороннего арбитражного соглашения между правообладателем товарного знака и правообладателем доменного имени нередко называют причиной того, что решения, принятые по процедуре *UDRP,* не подчиняются Конвенции о признании и приведении в исполнение иностранных арбитражных решений (Нью-Йорк, 1958 г.) (далее — Нью-Йоркская конвенция)[47]. С учетом этого делается заключение: «Именно отсутствие арбитражной оговорки в должной форме согласно ст. 2 Нью-Йоркской конвенции дает основание называть процедуру *UDRP* квазиарбитражной» (Krobka, 2020, p. 340).

Между тем исполнение решений по доменным спорам предусматривает применение специального принудительного механизма (реализуемого посредством внесения регистратором соответствующих сведений в реестр доменных имен), что, как указывалось выше, вовсе не исключает процедуру *UDRP* из числа арбитражных процедур.

[47] Convention on the Recognition and Enforcement of Foreign Arbitral Awards, June 10, 1958, 330 U.N.T.S. 3 (entered into force June 7, 1959).

В то же время вопрос связанности арбитражной оговоркой правообладателя товарного знака и правообладателя доменного имени представляется крайне значимым.

В связи со вышеупомянутым надо подчеркнуть, что в юридической литературе высказываются различные позиции относительно допустимости распространения арбитражного соглашения на лиц, формально не участвовавших в его заключении.

С одной стороны, некоторыми исследователями подчеркивается, что неучастие одной из сторон в формировании арбитражной оговорки может свидетельствовать о несогласованности последней и, как следствие, о невозможности признания арбитражного соглашения действительным в отношении такого лица (Terent'eva, 2020a, p. 39). В развитие такого подхода можно сослаться на правовую позицию Конституционного Суда РФ, выраженную в постановлении от 26 мая 2011 г. № 10-П, согласно которой в случае, если решением третейского суда затрагиваются права и законные интересы лиц, не участвовавших в третейском разбирательстве и не выражавших согласия на передачу спора в арбитраж, наличие таких обстоятельств является основанием для отказа в выдаче исполнительного листа на принудительное исполнение соответствующего решения. Конституционный Суд подчеркнул, что в подобной ситуации решение третейского суда содержит постановления по вопросам, выходящим за пределы третейского соглашения, и, следовательно, не соответствует требованиям закона[48].

С другой стороны, в публикациях встречаются и противоположные суждения, включая указания на то, что во многих правопорядках допускается распространение действия арбитражного соглашения на третьих лиц (*non-signatories*) в исключительных случаях, когда это продиктовано принципами справедливости, добросовестности и эффективности арбитражного разбирательства (Rozeeva, 2016, p. 53), в частности в ситуациях, когда действие арбитражных соглашений распространяется на третьих лиц в результате реорганизации, уступки прав и перевода долга, заключения договоров в пользу третьих лиц и суброгации (Skvortsov et al., 2018).

Думается, что в исследуемой ситуации возникновения доменного спора речь не идет об автоматическом распространении арбитражного соглашения на третье лицо — правообладателя товарного знака. *Связанность спорящих сторон — правообладателя товарного знака и правообладателя доменного имени, — которая позволят признавать аккредитованное ICANN арбитражное учреждение компетентным по рассмотрению доменного спора, возникает вследствие других обстоятельств.*

Анализ этих обстоятельств необходимо предварить указанием на достаточную обширность перечня способов заключения арбитражного соглашения. В юридической литературе подчеркивается, что такое заключение допускается не только в традиционной форме подписанного обеими сторонами единого документа, но и посредством обмена письмами и иными документами (включая электронные), и путем включения в связывающий стороны договор ссылки на документ, содержащий арбитражную оговорку, и через включение в устав юридического лица арбитражного соглашения, и посредством обмена процессуальными документами (в том числе исковым заявлением и отзывом на исковое заявление), в которых одна из сторон заявляет о наличии арбитражного соглашения, а другая против этого не возражает, и другим образом (Aleshukina, 2017, p. 32).

[48] Постановление Конституционного Суда РФ «По делу о проверке конституционности положений пункта 1 статьи 11 Гражданского кодекса Российской Федерации, пункта 2 статьи 1 Федерального закона "О третейских судах в Российской Федерации", статьи 28 Федерального закона "О государственной регистрации прав на недвижимое имущество и сделок с ним", пункта 1 статьи 33 и статьи 51 Федерального закона "Об ипотеке (залоге недвижимости)" в связи с запросом Высшего Арбитражного Суда Российской Федерации» от 26.05.2011 № 10-П.

В свою очередь, связанность правообладателя товарного знака и правообладателя доменного имени (*registrant*) возникает вследствие двух обстоятельств.

Во-первых, обращаясь с жалобой в один из аккредитованных *ICANN* арбитражных судов в порядке, предусмотренном пунктом 3(a) Правил *UDRP,* правообладатель товарного знака тем самым выступает инициатором арбитражного разбирательства, фактически принимая условия *UDRP* и Правила *UDRP* об арбитражной процедуре и о компетенции аккредитованных арбитражных центров[49]. Иными словами, имеет место добровольное признание со стороны правообладателя товарного знака компетенции аккредитованного *ICANN* арбитражного учреждения, которое реализуется посредством совершения конкретного юридически значимого действия — подачи жалобы в рамках процедуры, предусмотренной *UDRP.*

Впрочем, для признания компетенции аккредитованного *ICANN* арбитражного учреждения недостаточно волеизъявления только одной спорящей стороны — правообладателя товарного знака. При этом волеизъявление другой стороны — правообладателя доменного имени — на рассмотрение доменного спора в аккредитованном арбитражном суде вытекает вовсе не из классического (упомянутого выше) варианта представления отзыва на жалобу.

Вторым обстоятельством, необходимым для признания компетенции аккредитованного *ICANN* арбитражного учреждения, выступает согласие правообладателя доменного имени, которое закреплено в договоре, связывающем *registrar* и *registrant.* Это согласие носит предварительно обязывающий характер: включение условий *UDRP* и Правил *UDRP* в договор, заключаемый *registrar* и *registrant*, подразумевает, что *registrant* принимает на себя обязанность участвовать в разбирательстве по доменному спору и в тех случаях, когда оно инициируется третьим лицом — правообладателем товарного знака.

Таким образом, компетенция аккредитованного арбитражного центра по рассмотрению такого доменного спора формируется не по классической модели, а через совокупность двух разобщенных юридических фактов: (1) принятия правообладателем доменного имени на себя обязанности исполнять условия *UDRP* и признавать обязательность процедуры *UDRP* в случае предъявления к нему любых претензий (соглашение, связывающее *registrar* и *registrant*) и (2) обращения в аккредитованное *ICANN* арбитражное учреждение правообладателя товарного знака.

Бесспорно, подобный способ связывания спорящих сторон арбитражной оговоркой выходит за пределы классического понимания арбитражного соглашения и способа его заключения. Однако этот способ давно стал общеупотребимым для признания аккредитованного *ICANN* арбитражного учреждения компетентным третейским судом по рассмотрению доменного спора. В условиях отказа от чрезмерной строгости и формалистичности правил толкования арбитражного соглашения в пользу выявления действительной воли сторон, что наблюдается в том числе и в отечественной правоприменительной практике (Loboda, 2020; Loboda, 2019), можно сделать следующий вывод. Арбитрабельность доменных споров в широком смысле основывается на функциональном подходе, при котором определяющим фактором является не форма арбитражного соглашения, а реальное (действительное) волеизъявление каждой из спорящих сторон на передачу спора в арбитраж.

[49] ICANN. (n.d.). Rules for Uniform Domain Name Dispute Resolution Policy. https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/rules-for-uniform-domain-name-dispute-resolution-policy-the-rules-11-03-2015-en

Особенности определения компетентного арбитражного центра и взаимодействия с национальными судами

В рамках настоящей статьи не может быть обойден вниманием и ряд иных моментов, связанных с определением компетентного суда по разрешению доменного спора.

Во-первых, правообладатель товарного знака — инициатор арбитражного разбирательства вправе самостоятельного выбрать аккредитованный *ICANN* арбитражный центр, в который будет направлена жалоба. Указанное дискреционное право закреплено за правообладателем товарного знака в силу специфики *UDRP* как процедуры, инициируемой исключительно по его инициативе: у правообладателя доменного имени как ответчика отсутствует возможность влиять на выбор заявителем арбитражного суда.

В то же время обозначенное право выбора арбитражного центра не является безусловным и подлежит ограничению в случае, предусмотренном пунктом 4(f) *UDRP:* этот пункт регламентирует вопрос объединения дел, возникших между одними и теми же сторонами[50]. В соответствии с данным пунктом *UDRP* при наличии нескольких споров между заявителем и ответчиком любая из сторон вправе ходатайствовать о передаче дел на рассмотрение одного и того же провайдера. Соответствующее ходатайство подается в первый по времени арбитражный центр. Вопрос о допустимости объединения дел разрешается по усмотрению арбитражного учреждения при условии, что все подлежащие консолидации споры регулируются действующей редакцией *UDRP* или более поздней ее версией, утвержденной *ICANN*. Таким образом, в случае объединения разбирательств право заявителя на выбор арбитражного института фактически утрачивает самостоятельное значение, уступая приоритет принципу процессуальной экономии и согласованности разрешения взаимосвязанных споров.

Здесь же следует подчеркнуть, что все аккредитованные *ICANN* арбитражные центры для разрешения спора обязаны руководствоваться *UDRP,* включая пункт 4(a), закрепляющий основные обстоятельства, которые арбитражу необходимо установить для удовлетворения жалобы заявителя[51]. Таким образом, положения *UDRP* имеют универсальный характер и подлежат применению независимо от выбранного арбитражного института, что обеспечивает единообразие подходов к разрешению соответствующей категории дел[52].

Вместе с тем, несмотря на формальную универсальность процедуры, выбор конкретного арбитражного учреждения может определяться рядом практических соображений, в частности территориальным расположением арбитражного центра, размером арбитражного сбора, языком производства, репутацией и сложившейся практикой соответствующего арбитражного суда и иными факторами.

[50] ICANN. *Uniform Domain Name Dispute Resolution Policy* (Aug. 26, 1999, as amended Feb. 21, 2024). https://www.icann.org/resources/pages/policy-2024-02-21-en

[51] Ibid.

[52] Более того, на *UDRP* ориентируются и государственные суды при разрешении доменных дел. Так, согласно п. 3 Справки по вопросам, возникающим при рассмотрении доменных споров, по доменным спорам при рассмотрении вопросов о недобросовестности лица, участвующего в деле, «для установления содержания честных обычаев при регистрации и использовании (администрировании, делегировании и других действиях) доменных имен могут использоваться положения, сформулированные в Единообразной политике по разрешению споров в связи с доменным именами, одобренной Интернет-корпорацией по присвоению названий и номеров (*ICANN*), в том числе в ее параграфах 4(a), 4(b) и 4(c)» (см.: Постановление Президиума Суда по интеллектуальным правам «Об утверждении справки по вопросам, возникающим при рассмотрении доменных споров» от 28 марта 2014 г. № СП-21/4).

Во-вторых, значим и тот факт, что правообладатель товарного знака не лишен возможности, отказавшись от инициирования разбирательства в порядке *UDRP* или не согласившись с решением административной комиссии, обратиться с аналогичным требованием в государственный суд при соблюдении установленных национальным законодательством правил юрисдикции и подсудности.

Это положение находит отражение в пункте 4(k) *UDRP,* согласно которому обращение к административной процедуре не препятствует ни заявителю, ни ответчику передать спор на рассмотрение государственного суда как до начала административного слушания, так и после его завершения. Более того, в случае вынесения решения о передаче или аннулировании доменного имени его исполнение приостанавливается на срок 10 рабочих дней с момента уведомления регистратора. Если в течение этого срока от ответчика поступает надлежащее подтверждение подачи иска в государственный суд, арбитражное решение не подлежит исполнению до разрешения спора в государственном суде либо до представления доказательств прекращения соответствующего производства[53].

Важно, что обращение в государственный суд с требованием, аналогичным предмету спора, ранее рассмотренного в порядке *UDRP,* не является формой пересмотра или обжалования арбитражного решения. На это указывает Л. В. Терентьева, обоснованно отмечая, что при обращении в государственный суд спор подлежит рассмотрению по существу с самого начала (*de novo*) в рамках самостоятельного судебного производства, не связанного с оценкой правомерности или обоснованности решения, принятого в соответствии с *UDRP* (Terent'eva, 2020b, p. 134).

На эту особенность обращает внимание и Стивен Дж. Уэр (*Stephen J. Ware*), называя возможность повторного рассмотрения дела в национальном суде *de novo* важным отличием *UDRP* от традиционного арбитража (Ware, 2002, p. 162), где решение третейского суда, как правило, может быть оспорено лишь по ограниченным основаниям, связанным с процедурными нарушениями. Тем не менее изначально включение возможности обращения в национальный суд рассматривалось *ICANN* как способ нивелирования критики относительно создания *ICANN* формы частного законотворчества, узурпирующей полномочия национальных судов[54].

Возможность обращения в государственный суд после вынесения решения аккредитованным *ICANN* арбитражным учреждением ставит вопрос о допустимости и реальных перспективах принятия иного решения в судебном порядке. Согласно общепринятой позиции, изложенной в Обзоре ВОИС по отдельным вопросам *UDRP,* национальные суды не связаны арбитражными решениями, принятыми в рамках *UDRP*[55].

Анализируя указанную проблему на примере правоприменительной практики швейцарских государственных судов, Н. Руйе приходит к выводу об ограниченном характере судебного вмешательства в результаты арбитражного разбирательства доменных споров. В частности,

[53] ICANN. *Uniform Domain Name Dispute Resolution Policy* (Aug. 26, 1999, as amended Feb. 21, 2024). https://www.icann.org/resources/pages/policy-2024-02-21-en

[54] "It is recommended that any dispute-resolution system, which is alternative to litigation and to which domain name applicants are required to submit, should not deny the parties to the dispute access to court litigation" (See: WIPO. *The management of Internet names and addresses: Intellectual property issues (final report of the WIPO Internet domain process),* ¶ 140 (Apr. 30, 1999), https://www.wipo.int/export/sites/www/amc/en/docs/report-final1.pdf
Текст доклада также доступен на русском языке: WIPO. *Управление именами и адресами в Интернете: Вопросы интеллектуальной собственности (Заключительный доклад Первого процесса в рамках ВОИС по названиям доменов в Интернете).* https://www.wipo.int/export/sites/www/amc/ru/docs/report.pdf

[55] WIPO. *WIPO Overview of WIPO Panel Views on Selected UDRP Questions* (3d ed. 2017), 14.4.4 at 101, https://www.wipo.int/export/sites/www/amc/en/docs/overview3.pdf

автор подчеркивает, что в случае, если аккредитованный арбитражный центр пришел к выводу об отсутствии у ответчика законного интереса в отношении спорного доменного имени и принял решение о его передаче заявителю, убедить государственный суд в обратном крайне затруднительно. При этом, по мнению Н. Руйе, единственным действенным основанием для отказа в признании и исполнении такого решения может выступать доказанный факт того, что ответчик был лишен возможности участвовать в арбитражном разбирательстве и, соответственно, не мог реализовать право на защиту (Ruje, 2018, p. 500).

В рамках своего анализа Н. Руйе обращает внимание на встречающиеся на практике ситуации, отличающиеся повышенной сложностью, когда заявители предпочитают обращаться непосредственно в государственный суд, минуя процедуру, предусмотренную *UDRP* (Ruje, 2018, p. 502). В российской практике, которую, впрочем, сложно назвать единообразной (Evteeva, 2024, pp. 139–141), яркой иллюстрацией такой ситуации служит дело о доменном имени *besogon.tv*. Доменное имя *.tv* является *ccTLD* государства Тувалу, администратор которого признал применимость *UDRP* к возникающим в данной доменной зоне спорам, вследствие чего аккредитованные *ICANN* арбитражные центры могут быть признаны компетентными судами по рассмотрению доменного спора. Между тем в рамках данного дела правообладатель серии товарных знаков — российское юридическое лицо ООО «Бесогон» — принял решение инициировать судебное разбирательство в российском государственном суде. Юрисдикция российского государственного суда обосновывалась наличием личной и территориальной связи спора с Российской Федерацией: на начальном этапе в качестве *registrar* и *registrant* спорного доменного имени выступали российские лица. Несмотря на последующую передачу прав на спорное доменное имя новому правообладателю — гражданину США (*registrant*), а также смену *registrar* на американскую компанию, российские суды тем не менее признали за правообладателем товарных знаков не только право на иск, но и право на спорное доменное имя, удовлетворив заявленные требования[56].

Изложенное дело наглядно иллюстрирует то, что наличие действующего альтернативного механизма разрешения доменных споров в рамках *UDRP* не исключает возможности обращения заинтересованного лица в государственный суд, что может быть обусловлено не только сложностью дела, но и стремлением обеспечить рассмотрение спора в юрисдикции, которая, по мнению правообладателя товарного знака, может гарантировать для него более благоприятный исход дела. Вследствие этого выбор между арбитражем и государственным судом нередко носит стратегический характер и определяется совокупностью различных обстоятельств.

Заключение

Процедура *UDRP* регулирует специфический тип нарушений прав на товарные знаки, связанный с недобросовестной регистрацией и использованием доменных имен — киберсквоттингом. Такие случаи предполагается доказывать в рамках ускоренного разбирательства, в котором сознательно в угоду эффективности было ограничено использование определенных процессуальных механизмов.

Проведенное исследование позволяет утверждать, что, несмотря на терминологические особенности *UDRP,* отсылающие к административной процедуре, по правовой природе данная модель разрешения споров функционально сопоставима со специфическим видом

[56] Решение Арбитражного суда Московской области от 9 апреля 2025 г. по делу № А41-68198/2021; см. также решение Арбитражного суда Московской области от 11 июня 2025 г. по делу № А41-68198/2021.

арбитража и альтернативного разрешения споров. Споры, возникающие в связи с регистрацией и использованием доменных имен, полностью или частично воспроизводящих товарные знаки, обладают всеми признаками частноправового конфликта имущественного характера и, следовательно, могут быть предметом арбитражного разбирательства, т. е. обладают свойством арбитрабельности.

Несмотря на наличие критики, в частности в отношении ограниченности процедурных гарантий, отсутствия внутреннего апелляционного механизма, языковых трудностей и возможной предвзятости в пользу заявителей, ни одно из этих замечаний не ставит под сомнение ни правовую природу разбирательства по правилам *UDRP,* ни эффективность заложенных в него механизмов.

Особое значение для признания аккредитованного *ICANN* арбитражного центра компетентным судом имеет двухэтапная конструкция согласия сторон, сочетающая предварительное согласие правообладателя доменного имени на применение *UDRP* и последующее одностороннее волеизъявление правообладателя товарного знака, реализуемое в форме подачи жалобы. Данный механизм демонстрирует гибкость арбитражных процедур в условиях глобализированного цифрового пространства и подтверждает применимость функционального подхода при определении арбитрабельности споров.

Анализ различных моделей применения *UDRP* в *gTLD, new gTLD* и *ccTLD* показал, что вариативность национальных подходов не препятствует формированию единообразной правоприменительной практики в международном масштабе. В то же время сохранение возможности обращения в государственные суды обеспечивает баланс интересов сторон и повышает уровень гарантий судебной защиты.

UDRP продолжает оставаться устойчивой и признанной моделью глобального реагирования на киберсквоттинг. Полученные результаты позволяют рассматривать *UDRP* не только как эффективный инструмент разрешения доменных споров, но и как пример развития негосударственных форм разбирательства частноправовых споров, которые адаптированы к особенностям цифровой экономики.

Список литературы / References

1. Aleshukina, S. A. (2017). Pryamye soglasheniya — novella zakonodatel'stva ob arbitrazhe (treteyskom razbiratel'stve) [Direct agreements — novella of the legislation on arbitration]. *Vestnik Tverskogo Gosudarstvennogo Universiteta. Seriya: Pravo,* (2), 31–35.
2. Cortés Diéguez, J. P. (2008). An analysis of the UDRP experience — Is it time for reform? *Computer Law and Security Report, 24*(4), 2008, 349–359. https://doi.org/10.1016/j.clsr.2008.05.002
3. Eremin, V. V. (2019). Podkhody k opredeleniyu arbitrabel'nosti: sootnosheniye arbitrabel'nosti, podvedomstvennosti i kompetentsii [Approaches to arbitrability determination: Arbitrability, jurisdiction and competence correlation]. *Aktual'nyye Problemy Rossiyskogo Prava,* (8), 95–107. https://doi.org/10.58741/23134852_2024_4_13
4. Evteeva, E. V. (2024). Obzor sudebnoy praktiki v sfere domennykh imen: tendentsii i problemy [Review of judicial practice in the field of domain names: trends and problems]. *Zhurnal Suda po Intellektual'nym Pravam,* (4), 134–146. https://doi.org/10.58741/23134852_2024_4_13
5. Froomkin, M. A. (2002). ICANN's "Uniform Dispute Resolution Policy" — Causes and (partial) cures. *Brooklyn Law Review, 67*(3), 605–718.

6. Geist, M. (2002). Fair.com? An examination of the allegations of systemic unfairness in the ICANN UDRP. *Brooklyn Journal of International Law, 27*(3), 903–938.
7. Golubev A. E. (2022). Sushchestvuyushchiye mekhanizmy rassmotreniya i razresheniya domennykh sporov [Existing mechanisms for consideration and resolution of domain disputes]. *Zhurnal Suda po Intellektual'nym Pravam,* (1), 118–125.
8. Kazachenok, S. Yu. (2013). Arbitrazhnye ogovorki na strazhe realizatsii printsipa gibkogo razresheniya vneshneekonomicheskogo spora [Arbitration clauses to guard the principle of flexible foreign trade dispute resolution]. *Vestnik Volgogradskogo Gosudarstvennogo Universiteta. Seriya 5: Yurisprudentsiya,* (1), 72–75.
9. Kelley, P. D. (2002). Emerging patterns in arbitration under the Uniform Domain-Name Dispute-Resolution Policy. *Berkeley Technology Law Journal, 17*(1), 181–204. https://doi.org/10.15779/Z38K39R
10. Krobka, N. N. (2020). Deyatel'nost' VOIS po razresheniyu sporov v sfere intellektual'noy sobstvennosti [WIPO intellectual property dispute resolution activities]. *Uchenye zapiski Krymskogo federal'nogo universiteta imeni V. I. Vernadskogo. Yuridicheskie Nauki, 6*(1), 334–349.
11. Loboda, A. I. (2019). Tolkovaniye arbitrazhnogo soglasheniya v prave Rossii [Interpretation of arbitration agreement in Russian law]. *Treteyskiy Sud,* (1/2), 179–201.
12. Loboda, A. I. (2020). Prodolzheniye obsuzhdeniya problemy: Izmeneniya v podkhode k tolkovaniyu arbitrazhnogo soglasheniya v prave Rossii [Continuing the discussion of the problem: Changes in the approach to the interpretation of the arbitration agreement in the law in Russia]. *Treteyskiy Sud,* (1/2), 363–372.
13. Nathenson, I. S. (1997). Showdown at the domain name corral: Property rights and personal jurisdiction over squatters, poachers and other parasites. *University of Pittsburgh Law Review, 58*(4), 911–990.
14. Rozeeva, A. R. (2016). Rossiyskaya praktika rasprostraneniya arbitrazhnogo soglasheniya na tret'ikh lits [Russian practice of extending arbitration agreements to third parties]. *Aktual'nyye Problemy Gumanitarnykh i Estestvennykh Nauk,* (7-2), 58–63.
15. Rozhkova, M. A. (2018). Prava na domennoe imya [Rights to domain name]. In M. A. Rozhkova (Ed.), *Pravo v sfere Interneta* [Law in the sphere of the internet] (pp. 195–223). Statut.
16. Rozhkova, M. A., & Kopylov, S. A. (2022). Domennye imena: napravleniya sovershenstvovaniya pravovogo regulirovaniya [Domain names: Directions for improvment of legal regulation]. *Zhurnal Suda po Intellektual'nym Pravam,* (2), 99–113.
17. Rozhkova, M. A., Eliseev, N. G., & Skvortsov, O. Yu. (2008). *Dogovornoye pravo: soglasheniya o podsudnosti, mezhdunarodnoy podsudnosti, primiritel'noy protsedure, arbitrazhnoye (treteyskoye) i mirovoye soglasheniya* [Contract law: Agreements on jurisdiction, international jurisdiction, mediation, arbitration and settlement agreements]. Statut.
18. Ruje, N. (2018). Spory o domennykh imenakh: vybor mezhdu chastnymi procedurami (UDRP i prochimi) i razbiratel'stvom v gosudarstvennom sude [Domain name disputes: Choosing between private procedures (UDRP and Others) and proceedings before state courts]. In M. A. Rozhkova (Ed.), *Pravo v sfere Interneta* [Law in the sphere of the internet] (pp. 495–502). Statut.
19. Sergo, A. G. (2023). Vnesudebnoe razreshenie domennykh sporov: mirovaya praktika i otechestvennye perspektivy [Extrajudicial domain dispute resolution: World practice and domestic prospects]. *Zhurnal Suda po Intellektual'nym Pravam,* (2), 128–145. https://doi.org/10.58741/23134852_2023_2_128
20. Skvortsov, O. Yu. (2017). *Arbitrazh (treteyskoye razbiratel'stvo) v Rossiyskoy Federatsii: Uchebnik* [Arbitration (commercial arbitration) in the Russian Federation: Textbook]. Yurayt.
21. Skvortsov, O. Yu., Savransky, M. Yu., & Sevastyanov, G. V. (Eds.). (2018). *Mezhdunarodnyy kommercheskiy arbitrazh* [International commercial arbitration] (2nd ed.). Statut.
22. Snow, N. (2005). The constitutional failing of the Anticybersquatting act. *Willamette Law Review, 41*(1), 1–84.

23. Terent'eva, L. V. (2020a). Arbitrazhnye ogovorki v soglasheniyah s uchastiem potrebitelya [Arbitration clauses in agreements involving consumers]. *Pravo. Zhurnal Vysshej Shkoly Ekonomiki,* (2), 28–44. https://doi.org/10.17323/2072-8166.2020.2.28.44
24. Terent'eva, L. V. (2020b). Pravovaya priroda arbitrazhnykh tsentrov, rassmatrivayushchikh spory po procedure UDRP [Legal nature of UDPR arbitration centers]. *Actual Problems of Russian Law, 15*(9), 131–149. https://doi.org/10.17803/1994-1471.2020.118.9.131-149
25. Titov I.E. (2025). Iskovyye trebovaniya v domennykh sporakh: sravnitel'no-pravovoye issledovaniye rossiyskogo i germanskogo pravovykh podkhodov [Statements of claim in domain disputes: Comparative law research of Russian and German legal approaches]. *Zhurnal Suda po Intellektual'nym Pravam,* (1), 159–177. https://doi.org/10.58741/23134852_2025_1_14
26. Ware, S. J. (2002). Domain-name arbitration in the arbitration-law context: Consent to, and fairness in, the UDRP. *Journal of Small and Emerging Business Law, 6,* 145–179.
27. Woodard, E. C. (2009). The UDRP, ADR, and arbitration: Using proven solutions to address perceived problems with the UDRP. *Fordham Intellectual Property, Media and Entertainment Law Journal, 19*(4), 1169–1213.
28. Yakushev, M. V., Rozhkova, M. A., & Afanas'ev, D. V. (2017). O pravovoy prirode al'ternativnykh razbiratel'stv domennykh sporov [On the legal nature of alternative proceedings in domain name disputes]. *Vestnik Mezhdunarodnogo Kommercheskogo Arbitrazha,* (1), 173–179.

Сведения об авторах:

Рожкова М. А. — доктор юридических наук, главный научный сотрудник Института законодательства и сравнительного правоведения при Правительстве РФ, профессор Российской государственной академии интеллектуальной собственности, президент объединения экспертов в сфере интеллектуального, IT- и цифрового права «IP CLUB», Москва, Россия.
rozhkova-ma@mail.ru
ORCID: https://orcid.org/0000-0001-8071-174X

Алымова Е. В. — магистр права (НИУ ВШЭ), аспирант, Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, Москва, Россия.
ekaterinaeuteeva@yandex.ru
ORCID: https://orcid.org/0009-0005-8635-8103

Information about the authors:

Marina A. Rozhkova — Dr. Sci. in Law, Chief Researcher at the Institute of Legislation and Comparative Law under the Government of the Russian Federation, Professor of the Russian State Academy of Intellectual Property, President of the association of experts in Intellectual Property, IT and Digital Law — IP CLUB, Moscow, Russia.
rozhkova-ma@mail.ru
ORCID: https://orcid.org/0000-0001-8071-174X

Ekaterina V. Alymova — LL.M. (HSE University), Ph.D. Student, Institute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow, Russia.
ekaterinaeuteeva@yandex.ru
ORCID: https://orcid.org/0009-0005-8635-8103

https://doi.org/10.38044/2686-9136-2025-6-8

СТАТЬИ

ТЕМНЫЕ ПАТТЕРНЫ В ЭПОХУ POST-COOKIE: КАК РЕГУЛИРОВАНИЕ ИНТЕРФЕЙСОВ МЕНЯЕТ ЦИФРОВУЮ РЕКЛАМУ В ЕС И США

Д. В. Корж

Аппарат Общественной палаты Российской Федерации
125993, Россия, Москва, Миусская пл., 7-1

Аннотация

Переход к так называемой эпохе *post-cookie*, обусловленный отказом крупнейших технологических компаний от сторонних *cookie-файлов*, существенно изменил архитектуру цифровой рекламы. По мере сужения возможностей традиционного онлайн-трекинга возрастающее значение приобрели интерфейсные практики получения согласия и взаимодействия с пользователем. Именно в этих практиках все чаще проявляются так называемые «темные паттерны». Соответственно возникает необходимость оценить, как различные правовые системы реагируют на подобные вызовы. Поскольку именно ведущие юрисдикции задают ориентиры для глобального регулирования поведения в информационно-телекоммуникационных сетях, в том числе в сети Интернет, ключевую роль здесь играют Европейский союз и Соединенные Штаты Америки. Исходя из обозначенной проблематики в работе анализируются сходства и различия между европейским и американским подходами к регулированию темных паттернов. Поставленная цель обусловила выбор источников и методов исследования, которые включают нормативные правовые акты ЕС и США, практику надзорных органов по защите данных, методические документы, научные публикации, а также результаты собственного эмпирического анализа. Последний охватывал анализ интерфейсных практик на ряде популярных сайтов и сервисов. Полученные результаты показали, что европейская модель основывается на превентивном регулировании, ограничивающем возможность использования манипулятивных практик уже на стадии проектирования интерфейсов, тогда как американская модель преимущественно функционирует по принципу последующего вмешательства. В совокупности это позволило сформулировать вывод о том, что эффективное регулирование цифровой рекламы требует не столько ограничения манипулятивных практик, сколько стимулирования формирования такой архитектуры цифровой среды, которая основывается на принципах предсказуемости, прозрачности и минимизации данных, обеспечиваемых применяемым законодательством и алгоритмами, создаваемыми технологическими компаниями.

Ключевые слова

темные паттерны, манипулятивные интерфейсы, проектирование интерфейсов, цифровая реклама, данные пользователей, персональные данные, ФТК, недобросовестная практика

Конфликт интересов Автор сообщает об отсутствии конфликта интересов.

Финансирование Исследование не имеет спонсорской поддержки.

Для цитирования Корж, Д. В. (2025). Темные паттерны в эпоху post-cookie: как регулирование интерфейсов меняет цифровую рекламу в ЕС и США. *Цифровое право, 6*(2), 72–90. https://doi.org/10.38044/2686-9136-2025-6-8

Поступила: 07.04.25, принята в печать: 21.05.25, опубликована: 30.06.2025

ARTICLES

DARK PATTERNS IN THE POST-COOKIE ERA: HOW INTERFACE REGULATION TRANSFORMS DIGITAL ADVERTISING IN THE EU AND THE US

Denis V. Korzh

Executive Office of the Civic Chamber of the Russian Federation
7-1, Miusskaya Sq., Moscow, Russia, 125993

Abstract

The transition toward the so-called post-cookie era, driven by the decision of major technology companies to abandon third-party cookies, is significantly reshaping the architecture of digital advertising. In the context of narrowing possibilities for conventional online tracking, interface practices for obtaining consent and interacting with users have been gaining importance. However, these practices are increasingly being associated with so-called dark patterns. Accordingly, there arises a need to assess how different legal systems respond to such challenges. Since leading jurisdictions set the benchmarks for global regulation of behavior in information and telecommunication networks, including the Internet, the European Union and the United States play a key role in this process. In this light, the present study examines the similarities and differences between European and American approaches to regulating dark patterns. The stated objective has determined the selection of sources and research methods, which include EU and US legal acts, enforcement practices undertaken by data protection authorities, methodological documents, academic publications, and the results of the author's own empirical analysis. The latter encompassed an examination of interface practices across several popular websites and services. The findings indicate that the European model is based on preventive regulation, which restricts the use of manipulative practices already at the design stage of user interfaces. At the same time, the American model functions predominantly on a post-intervention basis. Taken together, this leads to the conclusion that effective regulation of digital advertising requires the development of a digital environment architecture grounded in the principles of predictability, transparency, and data minimization, rather than on restricting manipulative practices. These processes should be ensured by both applicable legislation and specific algorithms designed by technology companies.

Keywords
dark patterns, manipulative interfaces, interface design, digital advertising, user data, personal data, FTC, unfair practice

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Korzh, D. V. (2025). Dark patterns in the post-cookie era: How interface regulation transforms digital advertising in the EU and the US. *Digital Law Journal, 6*(2), 72–90. https://doi.org/10.38044/2686-9136-2025-6-8

Submitted: 7 Apr. 2025, accepted: 21 May 2025, published: 30 June 2025

Введение

В последние годы цифровая реклама претерпела существенные трансформации, обусловленные как технологическими изменениями, так и эволюцией регуляторной среды. Одним из наиболее значимых факторов, повлиявших на архитектуру цифровых платформ, стало последовательное вытеснение сторонних *cookies*[1], представляющих собой традиционный инструмент отслеживания пользовательской активности. Так, крупнейшие технологические корпорации, такие как *Google LLC* и *Apple Inc.*, реализуют стратегии отказа от сторонних *cookie*-файлов (*third-party cookies*), обосновывая свои действия необходимостью усиления защиты персональных данных и соблюдения требований конфиденциальности.

Однако наступление так называемой эпохи *post-cookie* — условного этапа развития цифровой среды, связанного с переходом от сторонних *cookie*-файлов к иным технологиям мониторинга пользовательской активности — не ознаменовало отказа от инвазивных практик цифрового влияния. Наоборот, на смену *cookies* пришли более скрытые, часто непрозрачные технологии и поведенческие практики, включая цифровой отпечаток (*device fingerprinting*)[2], вероятностное отслеживание (*probabilistic tracking*) и архитектурные приемы в пользовательских интерфейсах,

[1] Под *cookies* понимаются небольшие текстовые файлы, хранящиеся на устройствах, подключенных к информационно-телекоммуникационной сети Интернет. Файлы *cookie* могут выполнять различные функции, например запоминать действия пользователя на веб-сайте, отслеживать введенную на таком сайте информацию и аутентифицировать пользователей при доступе к соответствующим онлайн-сервисам. См. об этом, в частности, разъяснения ирландской комиссии по вопросам защиты данных: Irish Data Protection Commission. (2020). *Guidance note: Cookies and other tracking technologies.* https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf

[2] Цифровой отпечаток формируется с учетом таких параметров устройств, как идентификаторы аппаратной части, версия операционной системы, версия установленного на устройстве браузера, и других системных и аппаратных параметров устройства. Основная сложность в его формировании состоит в поиске баланса между уникальностью цифрового отпечатка и частотой изменения параметров, которые применяются для его получения. См.: Стандарт Банка России «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств» СТО БР БФБО-1.7-2023. Приказ Банка России «О введении в действие стандарта Банка России СТО БР БФБО-1.7-2023» от 1 марта 2023 г. № ОД-335.

направленные на сокрытие реального характера обработки данных или затруднение отказа от ее осуществления[3].

Именно в этом контексте существенно возрос интерес к феномену темных паттернов, представляющих собой манипулятивные элементы дизайна интерфейса, используемые для искажения свободы выбора пользователя и навязывания поведенческих сценариев, выгодных поставщику цифровых услуг.

По данным Европейской комиссии и партнерских организаций[4], в 2023 г. анализ 399 онлайн-магазинов показал, что 40% из них используют как минимум один из трех наиболее распространенных темных паттернов (от скрытых подписок до создания ложного чувства срочности). Еще более масштабное исследование 2022 г., охватившее наиболее популярные сайты и приложения на территории ЕС, выявило, что 97% из них прибегают к манипулятивным интерфейсным практикам[5].

В глобальном контексте, согласно отчету Международной сети по защите и обеспечению соблюдения прав потребителей за 2024 г., 76% проанализированных сайтов и приложений содержат темные паттерны[6].

Сегмент *cookie*-баннеров также демонстрирует системную проблему. Так, согласно некоторым оценкам, 72% баннеров содержат хотя бы один темный паттерн (Berens et al., 2024, p. 8). Результаты другого исследования показывают, что в США техники вроде пристыживания при подтверждении (*confirmshaming*)[7] либо двусмысленных формулировок[8] используются в 80,9% уведомлений о согласии на *cookies* (Li, 2022, p. 570).

В совокупности эти цифры свидетельствуют, что в условиях трансформирующейся цифровой среды, где отказ от *cookies* сопровождается внедрением новых практик обработки данных, несмотря на видимый упор на конфиденциальность, темные паттерны продолжают функционировать как системный и глобальный инструмент сбора данных и воздействия со стороны цифровых платформ.

---

[3] Например, *Mozilla* открыто заявляет, что браузер *Firefox* по умолчанию блокирует известные методы снятия цифрового отпечатка. См.: Firefox. (n.d.). *Firefox blocks fingerprinting*. Retrieved April 4, 2025, from https://www.firefox.com/en-US/features/block-fingerprinting/
Одновременно с этим *Google* разрабатывает инициативу *Privacy Sandbox* с целью создания новых веб-стандартов, которые должны заменить сторонние файлы *cookie*. *Google* указывает, что цель проекта — сделать текущие механизмы отслеживания устаревшими и блокировать скрытые методы отслеживания, такие как цифровой отпечаток (https://privacysandbox.com/intl/en_us/).

[4] Arntz, P. (2023, January 31). *40% of online shops tricking users with "dark patterns".* Malwarebytes. https://www.malwarebytes.com/blog/news/2023/01/european-commission-goes-after-dark-patterns-in-web-shops

[5] Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., Liva, G., Lechardoy, L., & Rodríguez de las Heras Ballell, T. (2022). *Behavioural study on unfair commercial practices in the digital environment: Dark patterns and manipulative personalisation.* European Commission. https://data.europa.eu/doi/10.2838/859030

[6] International Consumer Protection and Enforcement Network. (2024). *ICPEN Dark Patterns in Subscription Services Sweep*. https://www.icpen.org/sites/default/files/2024-07/Public%20Report%20ICPEN%20Dark%20Patterns%20Sweep.pdf

[7] Пристыживание при подтверждении (*confirmshaming*) является манипулятивной практикой, при которой пользователю внушается чувство вины или стыда за отказ от предоставления согласия, например, посредством формулировок, подразумевающих негативную оценку отказа (Li, 2022, p. 566).

[8] Двусмысленные формулировки представляют собой темный паттерн, который использует неясный или вводящий в заблуждение язык, чтобы побудить пользователя к определенному действию. Например, вместо четкого «согласен» и «не согласен» используются фразы вроде «продолжить с оптимальными настройками», где «оптимальность» не определена.

С правовой точки зрения темные паттерны представляют собой многоаспектное явление, находящееся на пересечении различных сфер правового регулирования, в частности защиты персональных данных, регулирования конкуренции, прав потребителей, а также этики цифрового дизайна[9]. Их правовая квалификация осложняется трансграничной природой цифровых платформ, а также значительными различиями в подходах к регулированию в Европейском союзе и Соединенных Штатах Америки.

В связи с этим в условиях отказа от *cookies* темные паттерны приобретают не столько технологическую, сколько выраженную нормативную релевантность, поскольку становятся инструментом замещения прежних практик сбора данных при одновременном обходе применимых требований, связанных с информированным согласием, прозрачностью и добросовестной коммерческой практикой. На таком фоне закономерно встает вопрос: способны ли действующие правовые инструменты ЕС и США обеспечить эффективное противодействие манипулятивным практикам интерфейсного дизайна, или же темные паттерны становятся способом обхода предписаний нормативно-правового характера, направленных на защиту пользователей?

Соответственно, настоящее исследование направлено как на выявление правовых рисков, порождаемых использованием темных паттернов, так и на анализ инструментов правового реагирования, формирующихся в ответ на это явление.

Следует также отметить, что несмотря на растущий научный и профессиональный интерес к темным паттернам преобладающее большинство исследований концентрируется на их поведенческих и технических аспектах, включая дизайн взаимодействия с пользователем (*user experience design*, или *UX-design*), человеко-компьютерное взаимодействие и поведенческую экономику (Berens et al., 2024). При этом представляется, что наибольший вклад в формализацию понятия «темные паттерны», их типологизацию и эмпирическое обнаружение в интерфейсах внесли работы дизайнеров-исследователей Г. Бригналла, Ч. Грэя и их соавторов (Brignull et al., 2015; Gray et al., 2018).

В то же время правовой анализ данного феномена остается фрагментарным и преимущественно представлен в методических документах контрольных (надзорных) органов. Определенную нормативную базу в этой связи формируют решения национальных органов по защите данных стран ЕС и правоприменительная практика Федеральной торговой комиссии США (далее — ФТК).

Настоящая же работа преследует цель обозначить направления сравнительно-правового исследования регулирования темных паттернов в условиях перехода к архитектуре *post-cookie* цифрового пространства, сочетающего нормативно-правовой анализ с оценкой технологических решений и рыночных моделей поведения цифровых платформ. Тем самым гипотеза этой работы заключается в предположении, что именно различия между правовыми системами ЕС и США в части регулирования защиты данных и защиты прав потребителей определяют степень восприимчивости цифровых платформ к использованию темных паттернов и предопределяют эффективность правового реагирования.

В свою очередь, новизна настоящего исследования заключается в интеграции правовой и технологической перспектив, что позволяет рассматривать темные паттерны не только как проблему дизайна, но и как объект правового регулирования в рамках комплексной политики, ориентированной на обеспечение прозрачности обработки данных и соблюдение принципов добросовестного взаимодействия с пользователями.

[9] Под этикой цифрового дизайна понимается система ценностных ориентиров, предполагающих добросовестность, прозрачность и уважение к автономии пользователя при разработке интерфейсов (Gjorgjieski, 2024, pp. 575–578).

Анализ проблематики и подходов к регулированию

Понятие темных паттернов (*dark patterns*) все чаще оказывается в центре научных и правовых дискуссий о цифровом регулировании.

Впервые введенное дизайнером Гарри Бригналлом в 2010 г., оно охватывает совокупность приемов проектирования пользовательских интерфейсов, направленных на манипулирование поведением пользователя в интересах оператора платформы (Brignull et al., 2015, pp. 21–23). Сущностной характеристикой таких паттернов является сознательное конструирование визуальных или структурных решений интерфейса таким образом, чтобы пользователь принимал решения, противоречащие его собственным предпочтениям, ожиданиям или интересам (Nouwens et al., 2020, p. 3).

В условиях действия Общего регламента по защите данных (*General Data Protection Regulation,* далее также — *GDPR*)[10] особую значимость приобретает вопрос действительности согласия на обработку персональных данных, которое может быть получено с помощью подобных манипулятивных практик. Так, в соответствии со ст. 4(11) и 7(4) *GDPR* согласие должно быть добровольным, конкретным, информированным и недвусмысленным[11], что ставит под сомнение возможность соблюдения этих критериев при использовании темных паттернов.

Существующая научная и практическая литература предлагает различные классификации темных паттернов.

Так, в работах некоторых исследователей предложено как эмпирическое, так и концептуальное обоснование рассматриваемых классификаций (Brignull et al., 2015, pp. 21–23; Gray et al., 2018, pp. 5–9; Kollmer et al., 2023, pp. 202–205; Edidin et al., 2024, pp. 6–7). Однако наиболее распространенные типологии исходят из следующих критериев (рисунок 1):

- обман (например, использование двусмысленных формулировок или визуально замаскированных кнопок);
- принуждение (вынужденные действия, не относящиеся к основной услуге);
- сокрытие (затруднение отзыва согласия или выхода из подписки);
- асимметрия интерфейса (визуальное или структурное преимущество одной опции над другими);
- создание ложной срочности или страха упущенной выгоды.

Например, в сервисе «Кинопоиск» пользователю при регистрации для бесплатного пробного периода необходимо ввести данные банковской карты, и по истечении этого срока подписка продлевается автоматически, что нередко приводит к неожиданным списаниям денежных средств (рисунок 2).

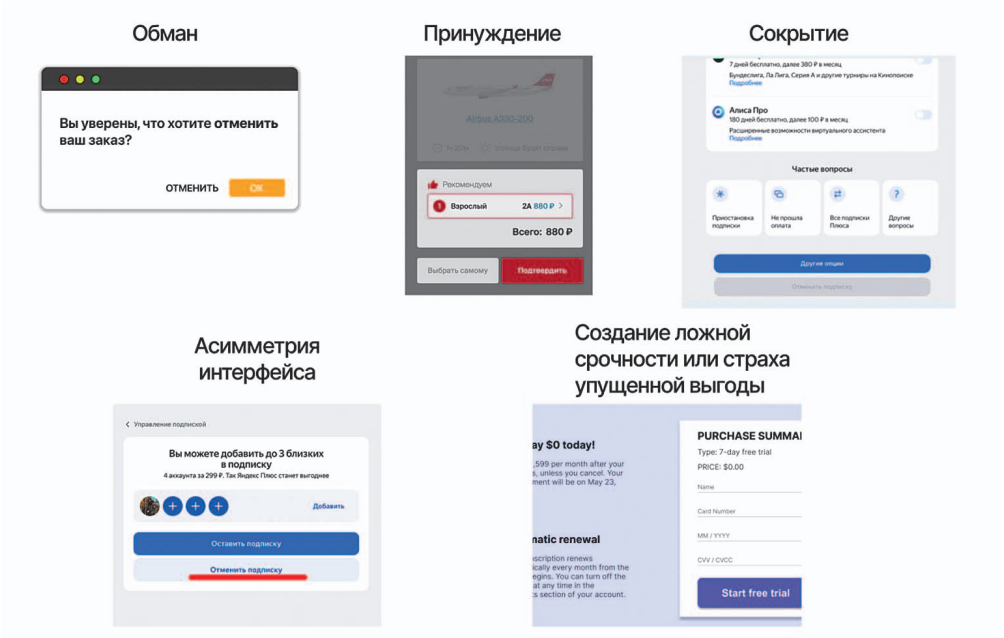
Похожий сценарий можно встретить и при покупке авиабилетов (рисунок 3). Так, например, пользователь выбирает рейс, вводит личные данные, переходит к оплате и внезапно обнаруживает, что стоимость перелета выросла в связи с автоматически активированным страхованием или СМС-информированием либо выбором места на борту самолета. Для отказа от подобных услуг пользователю необходимо вернуться на предыдущий этап и найти малозаметную галочку, спрятанную в интерфейсе.

[10] 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 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[11] General Data Protection Regulation, 2016 O.J. (L 119) 34, 37.

Рисунок 1 / Figure 1

Основные типы темных паттернов / Main types of dark patterns



Примечание. Составлено автором.

Примечательно появление и регуляторных типологий, отраженных, например, в политике ФТК[12] и некоторых разъяснениях европейских надзорных органов по защите данных[13].

Следует отметить, что в условиях постепенного отказа от сторонних *cookie*-файлов, обусловленного как правовыми ограничениями, так и инициативами технологических компаний, интерфейсы становятся основным каналом сбора пользовательских предпочтений и иных данных[14].

Таким образом, архитектура выбора в интерфейсе начинает выполнять регулирующую функцию, способствуя либо соблюдению принципа прозрачности, либо его нарушению. Правовое значение интерфейса как ключевого «пункта входа» в цифровую среду также находит подтверждение в общем направлении правоприменительной практики ст. 6 и 7 *GDPR*[15].

[12] U.S. Federal Trade Commission (2021, April 29). *Bringing dark patterns to light: An FTC workshop.* https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop

[13] См., к примеру, European Data Protection Board. (2023, February 24). *Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them.* https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

[14] Подобная трансформация связана с тем, что при ограничении традиционных инструментов отслеживания именно интерфейсные решения позволяют собирать согласия, направлять поведение пользователя и косвенно извлекать данные через дизайн-механику взаимодействия.

[15] General Data Protection Regulation, 2016 O.J. (L 119) 36–37.

Рисунок 2 / Figure 2

Пример подключения подписки «Яндекс.Плюс» с обязательным указанием данных банковской карты / An example of activating a "Yandex.Plus" subscription that requires mandatory entry of bank card details

Примечание. Подготовлено автором при обращении к сайту «Яндекс Плюс» (https://plus.yandex.ru/).

При этом проблематика темных паттернов тесно связана с вопросами этики цифрового дизайна, порождая дилемму между дизайном, ориентированным на пользователя, и дизайном, направленным на бизнес-цели, которые зачастую достигаются за счет пользователя.

Впрочем, использование манипулятивных практик ставит под угрозу реализацию основных прав пользователей, включая право на защиту персональных данных. Это особенно проблематично в отношении уязвимых категорий пользователей, в частности несовершеннолетних, пожилых людей, лиц с пониженной цифровой грамотностью, на которых такие приемы могут оказывать непропорционально сильное воздействие. Так, в контексте исследований по когнитивной психологии и поведенческой экономике особое внимание уделяется тому, как архитектура онлайн-выбора взаимодействует с нерефлексивными эвристиками (автоматическими и зачастую неосознаваемыми стратегиями мышления, которыми руководствуется потребитель). Если интерфейс сознательно спроектирован так, чтобы вызвать предвзятость и исказить восприятие выгод и рисков, можно утверждать, что это воздействие направлено

Рисунок 3 / Figure 3

Пример покупки билетов на сайте авиакомпании «Победа», подтверждающий автоматическое предоставление согласия на дополнительные услуги /
An example of purchasing tickets on the "Pobeda" airline website that demonstrates the automatic granting of consent to additional services

Примечание. Подготовлено автором при обращении к сайту авиакомпании «Победа» (https://www.flypobeda.ru).

на подсознательные процессы принятия решений, которые пользователь не способен критически осмыслить.

Поскольку такие процессы не отражают рационального выбора, они не могут служить обоснованием или оправданием принятого решения (Blumenthal-Barby, 2016, pp. 5–15). Именно эта логика лежит в основе аргументации в научной литературе, утверждающей, что автономия личности подрывается присутствием искусственно вызванной предвзятости и манипулятивных эвристик в процессе принятия решений (Brenncke, 2023, pp. 8–9; Cohen, 2019, pp. 33–36, 40–44).

В результате в доктрине усиливается тенденция к переходу от регулирования технических инструментов слежения (таких как *cookie*-файлы) к регулированию самого интерфейса как пространства принятия решения[16]. В этом контексте темные паттерны представляют собой не только технический или дизайнерский феномен, но и правовую категорию, которая требует переосмысления принципов, действующих в рассматриваемой сфере правового регулирования.

С учетом вышеизложенного можно сделать вывод, что одним из наиболее значимых трансформационных процессов в цифровой экономике последних лет является отказ от использования сторонних *cookie*-файлов — технологии, десятилетиями служившей основным инструментом слежения за пользователями и персонализации цифровой рекламы.

[16] См., например: Mathur et al. (2021); Leiser & Santos (2024).

Впрочем, данный сдвиг знаменует собой начало так называемой эпохи *post-cookie*, характеризующейся переосмыслением способов сбора, обработки и монетизации пользовательских данных. Причины же отказа от сторонних *cookie*-файлов носят как нормативный, так и технологический характер. Так, растущая строгость правового регулирования в сфере защиты персональных данных в Европейском союзе и отдельных юрисдикциях Соединенных Штатов Америки сделала невозможным дальнейшее использование *cookie*-файлов в прежнем виде без нарушения положений законодательства в области персональных данных. В частности, Общий регламент по защите данных, принятый в 2016 г., установил в ЕС строгие требования к получению согласия субъектов данных, требуя добровольного, конкретного, информированного и однозначного волеизъявления, посредством которого субъект данных с помощью заявления или четкого утвердительного действия дает согласие на обработку своих персональных данных (ст. 4, 11 *GDPR*)[17], что, как представляется, распространяется и на любые технологии слежения, включая *cookie*-файлы. Аналогичные по содержанию акты стали принимать и в США на уровне штатов. Дополнительные ограничения были закреплены в Директиве о конфиденциальности в электронных коммуникациях (*ePrivacy Directive*)[18].

В свою очередь, технологические корпорации, такие как *Apple Inc.* и *Google LLC*, отреагировали на растущие нормативные и репутационные риски, внедрив собственные ограничения на использование сторонних *cookie*-файлов. Так, *Apple Inc.* реализовала принцип конфиденциальности по замыслу (*privacy by design*)[19] в экосистеме *iOS* в целом и браузере *Safari* в частности, включая обязательное получение согласия через механизм *App Tracking Transparency* (*ATT*)[20]. В то же время *Google LLC* объявила о планомерном отказе от сторонних *cookie*-файлов в браузере *Chrome*, развивая альтернативные инициативы, такие как *Privacy Sandbox* и *Topics API* (https://privacysandbox.com), направленные на менее инвазивные методы персонализации рекламы[21].

Однако следует отметить, что на фоне отказа крупнейших технологических компаний от сторонних *cookie*-файлов бизнес активно адаптируется, развивая альтернативные методы сбора пользовательской информации.

В этой связи одним из ключевых направлений стало усиление роли данных первого уровня (*first-party data*), собираемых бизнесом непосредственно с собственных платформ.

---

17 General Data Protection Regulation, 2016 O.J. (L 119) 33–35.

18 Directive 2002/58/EC, of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201), 37.

19 Согласно ст. 25 *GDPR* необходимо применять соответствующие технические и организационные меры, такие как псевдонимизация, предназначенные для эффективной реализации принципов защиты данных, таких как минимизация данных, и интеграции необходимых мер безопасности в процесс обработки для соблюдения требований названного Регламента и защиты прав субъектов данных (General Data Protection Regulation, 2016 O.J. (L 119) 48). Иначе говоря, необходимо соблюдать принцип конфиденциальности по замыслу или спроектированной приватности (*privacy by design*).

20 Apple Inc. (n.d.). *User privacy and data use*. Apple Inc. Retrieved April 5, 2025, from https://developer.apple.com/app-store/user-privacy-and-data-use/

21 *App Tracking Transparency (ATT)* является фреймворком, который требует, чтобы приложения получали явное разрешение от пользователя, прежде чем отслеживать его данные на других сайтах и в других приложениях.
В то время как *Privacy Sandbox* представляет собой набор инициатив *Google*, направленный на создание новых веб-стандартов для рекламы. *Topics API* является частью этого набора, которая позволяет браузерам определять интересующие пользователя темы (например, «спорт» или «путешествия») на основе истории его просмотров, не передавая при этом индивидуальные данные.

Представляется, что такие данные менее проблематичны с правовой точки зрения при условии обоснования законных целей их обработки, получения надлежащего согласия и соблюдения иных положений законодательства в области персональных данных.

Параллельно указанной практике развивается контекстная реклама[22], основанная на содержании страницы и параметрах сессии, а не на истории поведения пользователя. Данный подход сравнительно с использованием стандартных *cookie*-файлов представляется менее инвазивным и потенциально более совместимым с положениями законодательства в области персональных данных, однако его коммерческая эффективность все еще обсуждается[23].

Следует обратить внимание на то, что в этих условиях интерфейсные практики приобретают первостепенное значение как способ получения согласия и управления ожиданиями пользователей. В то же время с исчезновением «невидимых» *cookie*-файлов возрастает давление на интерфейс как основной канал коммуникации между пользователем и цифровой платформой.

Это приводит к усилению использования темных паттернов, таких как затруднение или создание препятствий (*obstruction*)[24], асимметрия кнопок согласия[25] и искусственные ограничения в настройках конфиденциальности[26].

Вместе с тем такие интерфейсные решения, формально соответствующие законодательству в области персональных данных, фактически подрывают его эффективность. Именно поэтому темные паттерны становятся значимым правовым и политическим вызовом, создавая иллюзию добровольного согласия при отсутствии реальной свободы выбора.

Учитывая вышеизложенное, важно отметить, что на рассматриваемом этапе развития цифровой среды проблема злоупотреблений в цифровой рекламе не была устранена, а лишь претерпела трансформацию.

---

[22] Контекстная реклама представляет собой тип таргетинга, при котором рекламные объявления показываются в соответствии с содержанием веб-страницы, которую просматривает пользователь. Такой подход не требует отслеживания личных данных и истории поведения.
Дополнительно о механизмах работы контекстной рекламы можно узнать в справочных материалах *Google Ads* (см., например: Google Inc. (n.d.). Контекстный таргетинг. https://support.google.com/google-ads/answer/1726458?hl=ru) или на портале «Яндекс.Директ» (Яндекс Директ. (2024, 1 сентября). *Что такое контекстная реклама и как она работает*. https://direct.yandex.ru/base/articles/kontekstnaya-reklama-chto-eto).

[23] Речь идет о том, что контекстная реклама не обеспечивает того уровня таргетинга и персонализации, который достигается за счет поведенческих данных, поэтому бизнес оценивает ее как менее результативную с точки зрения конверсий и доходности, несмотря на ее большую правовую совместимость с принципами, касающихся обработки персональных данных.

[24] Затруднение или создание препятствий (*obstruction*) представляет собой стратегию создания искусственных препятствий для отказа от *cookies*, включающую усложненные или запутанные процедуры отклонения, направленные на повышение вероятности согласия пользователя.

[25] Асимметрия кнопок согласия является темным паттерном, при котором кнопки согласия и отказа визуально неравнозначны. Например, кнопка «Согласен» может быть выделена ярким цветом и крупным шрифтом, в то время как кнопка «Отклонить» — быть тусклой, мелкой или скрытой в тексте.

[26] Под искусственными ограничениями понимаются приемы, которые создают ложное ощущение дефицита или срочности, чтобы побудить пользователя к немедленному принятию решения, не давая ему времени на обдуманный выбор. Примерами могут служить таймеры обратного отсчета («Предложение действует только 10 минут!») или счетчики остатков товара («Осталось всего 2 штуки!»).

В свою очередь, технологическая замена поведенческого таргетинга усилила значение интерфейсов как ключевого пространства пересечения интересов бизнеса, прав пользователей и деятельности контрольных (надзорных) органов. Анализ же новых форм поведения цифровых платформ и методов их регулирования является необходимым условием для построения этичной и правомерной цифровой среды. Так, обладая комплексной и скоординированной системой регулирования, ЕС развивает модель, включающую как универсальные требования в сфере защиты данных, так и дифференцированные (Santos et al., 2025, pp. 364–367).

Общий регламент по защите данных, хотя и не упоминает напрямую темные паттерны, в то же время создает нормативную основу для их пресечения через принципы минимизации данных и требований к их законной, справедливой и прозрачной обработке (ст. 5(1) *GDPR*)[27].

Важно также учитывать, что в соответствии со ст. 7(3) *GDPR* согласие должно быть легко отзывным и предоставляться без какого-либо принуждения или искажения[28], в результате чего, как представляется, возможность получения действительного согласия с помощью интерфейсных манипуляций исключается.

С принятием Закона о цифровых услугах (*Digital Services Act* (далее — *DSA*))[29] и Закона о цифровых рынках (*Digital Markets Act* (далее — *DMA*))[30], вступивших в силу в 2024 г., регулирование приобрело новое измерение, ориентированное не только на защиту данных, но и на поведенческие аспекты функционирования цифровых платформ. Так, в п. 67 преамбулы *DSA* темные паттерны определяются как онлайн-интерфейсы онлайн-платформ и практики, которые существенно искажают или ухудшают — намеренно или фактически — способность получателей услуг делать самостоятельный и осознанный выбор или принимать решения[31].

В статье же 25 *DSA* закрепляется прямой запрет на использование темных паттернов[32]. В частности, предусматривается, что поставщики онлайн-платформ не должны проектировать, организовывать или эксплуатировать свои онлайн-интерфейсы таким образом, чтобы это вводило в заблуждение или манипулировало пользователями их услуг, или таким образом, чтобы это иным образом существенно искажало или затрудняло возможность пользователей принимать свободные и обоснованные решения.

В свою очередь, *DMA*, в частности в ст. 6, вводит обязательства для «привратников» (*gatekeepers*), включая запрет на навязывание подписок или затруднение отказа от услуг, что может также квалифицироваться как использование темных паттернов[33].

---

27 General Data Protection Regulation, 2016 O.J. (L 119) 35.

28 General Data Protection Regulation, 2016 O.J. (L 119) 37.

29 Regulation 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1.

30 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 O.J. (L 265) 1.

31 Digital Services Act, 2022 O.J. (L 277) 18.

32 Digital Services Act, 2022 O.J. (L 277) 58–59.

33 Digital Markets Act, 2022 O.J. (L 265) 34–36.

Вместе эти акты формируют нормативную правовую базу для обеспечения цифровой справедливости (*digital fairness*)[34], где ключевым понятием является «архитектура выбора»[35].

Впрочем, важно обратить внимание на то, что отправной точкой в правовом закреплении проблемы темных паттернов в ЕС стали решения национальных надзорных органов по защите данных в рамках *GDPR*. Так, например, Национальная комиссия по персональным данным и свободам Франции (*Commission nationale de l'informatique et des libertés*) оштрафовала *Google LLC* и *Meta Platforms, Inc.*[36] за *cookie*-баннеры, где принятие было облегчено, а отказ затруднен, что было признано нарушением требований к добровольному, конкретному, информированному и недвусмысленному согласию (ст. 4(11) и 7 *GDPR*)[37] и *ePrivacy Directive*[38]. Решение Комиссии по защите персональных данных Ирландии в отношении *Meta Platforms, Inc.*[39], касающееся персонализированной рекламы, также показало недопустимость введения пользователей в заблуждение относительно оснований обработки данных, что может нарушать не только правила защиты данных, но и принципы конкуренции. Данные решения формируют практику признания незаконными интерфейсных элементов, направленных на обход требований согласия.

В то же время регулирование темных паттернов в США осуществляется в условиях фрагментированной нормативной среды, где компетенции распределены между федеральным уровнем (в первую очередь практика ФТК) и законодательством отдельных штатов[40].

Хотя федеральное законодательство не содержит прямого запрета на использование темных паттернов, ФТК последовательно квалифицирует их как недобросовестные или вводящие в заблуждение действия. Так, в 2022 г. ФТК выпустила разъяснения, прямо указывающие на нарушение темными паттернами норм добросовестной коммерческой практики и стандартов информированного согласия, акцентируя внимание на затруднении отписки, психологическом

[34] В настоящий момент Европейская комиссия активно анализирует действующее законодательство о защите прав потребителей на предмет его пригодности в цифровую эпоху. Данная инициатива, известная как *Fitness Check of EU consumer law on digital fairness*, направлена на оценку того, насколько эффективно текущее законодательство (включая Директиву о недобросовестной коммерческой практике (Directive 2005/29/EC, of the European Parliament and of the Council of 11 May 2005 concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market and Amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive), 2005 O.J. (L 149) 22) противостоит новым вызовам, таким как темные паттерны и манипулятивные интерфейсы. См.: European Commission. (2022, November 28). *Consumer protection: Commission launches a public consultation on the Fitness Check of EU consumer law on digital fairness*. https://ec.europa.eu/newsroom/just/items/767499/en

[35] В работах отдельных авторов (см., например: Kahneman, 2013, pp. 8–29) подробно и последовательно развивается концепция архитектуры выбора (*choice architecture*), которая неизбежно присутствует в любой системе, где пользователям предоставляется выбор.

[36] По решению органов государственной власти Российской Федерации организация *Meta Platforms, Inc.* признана экстремистской, ее деятельность запрещена на территории России.

[37] General Data Protection Regulation, 2016 O.J. (L 119) 34, 37.

[38] Directive on Privacy and Electronic Communications, 2002 O.J. (L 201), 37. См. об этом: Data Privacy Manager. (2022, January 12). *CNIL fines Google and Facebook a total of €210 million over cookies.* https://dataprivacymanager.net/cnil-fines-google-and-facebook-a-total-of-e210-million-over-cookies/

[39] Irish Data Protection Commission. (2023, January 4). *Data Protection Commission announces conclusion of two inquiries into Meta Ireland.* https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland

[40] Federal Trade Commission Act § 5, 15 U.S.C. § 45(a).

давлении, дезориентирующих элементах дизайна и ложном представлении о правах пользователя[41].

В свою очередь, дело в отношении *Amazon.com, Inc.* за использование темных паттернов при оформлении и отмене подписки на *Amazon Prime* стало прецедентным; в нем впервые как часть аргументации явно был использован термин «темные паттерны», определяемые как «обманный интерфейс»[42]. Аналогичный иск был подан против *Adobe Inc.*[43] Особое внимание ФТК уделила и *TikTok Inc.*, выявив элементы интерфейса, затрудняющие изменение настроек конфиденциальности и недобросовестно вовлекающие несовершеннолетних пользователей. Досудебное урегулирование с *TikTok Inc.* включало выплату значительной суммы компенсации и изменения в интерфейсе[44].

На уровне штатов наиболее развитое регулирование по рассматриваемому вопросу представлено в Калифорнии, где впервые в американской практике на уровне закона штата были разрешены вопросы использования темных паттернов (*California Consumer Privacy Act*[45] и *California Privacy Rights Act*[46]). На это же обращают внимание и некоторые исследователи (Tran et al., 2024, pp. 4–5).

Следует отметить, что Агентство по защите конфиденциальности Калифорнии использует термин «темные паттерны» и предлагает критерии их выявления[47]. Аналогичные положения появляются и в законах штатов Колорадо, Коннектикут, Вирджиния и Юта[48], что, как было отмечено выше, свидетельствует о формировании фрагментарного, но в некоторой степени скоординированного подхода к регулированию манипулятивных практик.

Впрочем, важно также подчеркнуть, что данный подход делает практику правоприменения более казуистичной и зависимой от конкретных дел, создавая менее предсказуемую среду для цифровых платформ.

С учетом изложенного следует отметить, что решения французской и ирландской комиссий привели к повсеместному изменению интерфейсов *cookie*-баннеров

---

41 U.S. Federal Trade Commission. (2022, September). *Bringing dark patterns to light*. https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf

42 United States v. Amazon.com, Inc., No. 2:23-cv-00932 (W.D. Wash. filed June 21, 2023).

43 United States v. Adobe Inc., No. 5:24-cv-03630-BLF (N.D. Cal. filed July 11, 2024). См. также: U.S. Federal Trade Commission. (2024, June 17). *FTC takes action against adobe and executives for hiding fees, preventing consumers from easily cancelling software subscriptions* [Press release]. https://www.ftc.gov/news-events/news/press-releases/2024/06/ftc-takes-action-against-adobe-executives-hiding-fees-preventing-consumers-easily-cancelling

44 In Re TikTok, Inc., Consumer Privacy Litig., No. 1:20-cv-04699, ECF No. 161 (N.D. Ill. July 28, 2021).

45 Cal. Civ. Code § 1798.140(l) (2025), https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf

46 Cal. Code Regs. tit. 11, § 7004(b), (c) (2023), https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf

47 California Privacy Protection Agency. (2024, September 4). *Enforcement Advisory No. 2024-02: "Avoiding Dark Patterns: Clear and Understandable Language, Symmetry in Choice"*. California Privacy Protection Agency. https://cppa.ca.gov/pdf/enfadvisory202402.pdf

В этом документе агентство разъясняет, как применять принципы *California Privacy Rights Act* для выявления и предотвращения темных паттернов, а также подчеркивает, что они оцениваются по их эффекту, а не по намерениям.

48 См.: Colo. Privacy Act, ch. 483, 2021 Colo. Sess. Laws 3180 (codified at Colo. Rev. Stat. § 6-1-1301 et seq. (2023))., Connecticut Data Privacy Act, Pub. Act No. 22-15, 2022 Conn. Acts 109 (Reg. Sess.) (codified at Conn. Gen. Stat. §§ 42-515–525 (2023))., Virginia CDPA (2023), Utah Consumer Privacy Act, 2022 Utah Laws 1911 (codified at Utah Code Ann. §§ 13-61-101–404 (2023).

в Европе[49]. В то же время дела ФТК способствовали реформе интерфейсов на американских сайтах, особенно в сфере электронной коммерции и подписных сервисов[50].

В свою очередь, данные изменения демонстрируют растущее влияние правоприменительной практики на дизайн, ранее считавшийся исключительно сферой ответственности бизнеса и *UX*-команд (*user experience teams*)[51]. Одновременно с этим прослеживается формирование международного тренда на развитие более прозрачных и этичных интерфейсов, где ограничение применения темных паттернов становится важным элементом в обеспечении справедливой и сбалансированной архитектуры платформенного взаимодействия.

Вместе с тем применяемые санкционные режимы в рассматриваемой сфере общественных отношений в анализируемых юрисдикциях все же различаются. Так, при европейском подходе нарушения могут повлечь административные штрафы, в частности, достигающие 4% от глобального годового оборота компании (ст. 83(5) *GDPR*)[52], или до 6% согласно ст. 74 *DSA*[53] и 10% в соответствии со ст. 30 *DMA*[54], что среди прочего создает высокий уровень регуляторного давления.

В свою очередь, при американском подходе санкции, как правило, носят индивидуальный характер и определяются в каждом конкретном деле, однако потенциальные суммы компенсаций и предписания о реструктуризации интерфейсов делают их достаточно эффективным инструментом[55]. При этом различие в правовой природе норм — административного права в ЕС и конкурентного/потребительского права в США — приводит к различной интерпретации границ

---

[49] Например, в декабре 2024 г. французская комиссия по персональным данным и свободам направила формальные уведомления ряду издателей с требованием привести *cookie*-баннеры в соответствие с законодательными требованиями (они должны позволять так же легко отклонять *cookies*, как и принимать их, не иметь вводящего в заблуждение оформления). Данное обстоятельство однозначно побудило веб-ресурсы внести изменения в интерфейсы. См.: CNIL. (2024, December 12). *Dark patterns in cookie banners: CNIL issues formal notice to website publishers.* https://www.cnil.fr/en/dark-patterns-cookie-banners-cnil-issues-formal-notice-website-publishers

[50] Например, в октябре 2021 г. ФТК выпустила заявление об ужесточении регулирования в отношении темных паттернов при оформлении подписок, требуя, чтобы пользовательские интерфейсы предоставляли понятную информацию, обеспечивали добровольное согласие и простой способ отмены. См.: U.S. Federal Trade Commission. (2021, October 28). *FTC to ramp up enforcement against illegal dark patterns that trick or trap consumers into subscriptions* [Press release]. https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions

В сентябре 2022 г. ФТК опубликовала отчет, в котором демонстрируется рост количества совершенно скрытых или замаскированных интерфейсных приемов. См.: U.S. Federal Trade Commission. (2022, September 15). *FTC report shows rise in sophisticated dark patterns designed to trick and trap consumers* [Press release]. https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers

В июле 2024 г. совместный обзор ФТК, Международной сети по защите и обеспечению соблюдения прав потребителей и Глобальная сеть обеспечения защиты конфиденциальности (*Global Privacy Enforcement Network*) выявил распространенность лишь отдельных темных паттернов. См.: U.S. Federal Trade Commission. (2024, July 10). *FTC, ICPEN, GPEN Announce Results of Review of Use of Dark Patterns Affecting Subscription Services, Privacy* [Press release]. https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-icpen-gpen-announce-results-review-use-dark-patterns-affecting-subscription-services-privacy

[51] *UX*-команды (*user experience teams*) представляют собой группы специалистов, ответственных за проектирование пользовательского опыта. Их задачей является сделать продукт (сайт, приложение и т. д.) удобным, понятным и эффективным для конечного пользователя.

[52] General Data Protection Regulation, 2016 O.J. (L 119) 83.

[53] Ст. 74 *DSA* (Digital Services Act, 2022 O.J. (L 277) 94).

[54] Ст. 30 *DMA* (Digital Markets Act, 2022 O.J. (L 265) 51–53).

[55] Как, например, в вышеупомянутых делах Adobe, No. 5:24-cv-03630-BLF (N.D. Cal.), Amazon, No. 2:23-cv-00932 (W.D. Wash.).

допустимого. Так, в отличие от европейского подхода, где активно формируется превентивная (*ex ante*) модель с детальной регламентацией интерфейсных решений (например, как было отмечено выше, положения *GDPR, DSA* и *DMA* формулируют детализированные запреты и обязанности, которые ограничивают использование манипулятивных интерфейсных решений), американский подход преимущественно строится на регулировании *ex post* (как указывалось выше, в практике ФТК и законодательстве отдельных штатов), представляющем собой такой способ правоприменения, при котором соответствующие категории носят оценочный характер и позволяют квалифицировать поведение как недопустимое только после выявления последствий для конкуренции или потребителей[56].

Таким образом, сравнительный анализ подходов ЕС и США выявляет как сходство (консенсус относительно недопустимости манипулятивного поведения), так и различие (универсализм в ЕС и фрагментарность в США, превентивные меры в ЕС и регулирование *ex post* в США) между ними.

Вместе с тем на фоне изложенного особенно важно подчеркнуть, что проблема темных паттернов требует не столько применения мер регулирования *ex post*, реализуемых посредством правоприменительной практики, сколько формирования превентивных мер, направленных на предотвращение манипуляций на этапе разработки интерфейсных решений.

Так, опираясь на результаты анализа, можно предложить несколько взаимодополняющих подходов, направленных на ограничение манипулятивных практик и укрепление пользовательской автономии. В частности, в условиях продолжающегося отказа от сторонних *cookie*-файлов, повышения интенсивности регулирования и общественного запроса на этичную цифровую среду целесообразным представляется развитие как технологических, так и правовых инструментов обеспечения баланса между интересами бизнеса, государства и пользователей. Одним из таких перспективных направлений видится внедрение принципов этичного дизайна в процессы разработки пользовательских интерфейсов, ставящего во главу угла автономию пользователя, прозрачность обработки данных и минимизацию рисков.

Указанное включает создание симметричных интерфейсов выбора, отказ от предустановленных опций, визуальное равновесие кнопок согласия, а также структурирование контента без создания ложного ощущения срочности или давления. В литературе подобные решения описываются как примеры так называемых «светлых паттернов» (см., к примеру, Edidin et al., 2024, p. 26).

Как уже было отмечено, принцип конфиденциальности по замыслу (*privacy by design*) является нормативно закрепленным ориентиром для минимизации воздействия на поведенческую автономию пользователя[57]. Технологическим же дополнением к реализации этого принципа представляется использование искусственного интеллекта и автоматизированных инструментов пользовательского аудита интерфейсов (*user experience audit*, или *UX audit*)[58] для выявления темных паттернов, которые могут быть интегрированы в процедуры

[56] В юридической литературе термин *«ex ante»* применяется для обозначения превентивных механизмов регулирования, действующих до возникновения нарушения и направленных на предупреждение потенциальных злоупотреблений (например, установление стандартов проектирования интерфейсов). Напротив, *«ex post»* означает меры, принимаемые после совершения нарушения, такие как расследования, судебные иски и санкции (Baldwin et al., 2011).

[57] Этому посвящена ст. 25 *GDPR*. См.: General Data Protection Regulation, 2016 O.J. (L 119) 48.

[58] Пользовательский аудит интерфейсов представляет собой систематическую оценку интерфейсных решений на предмет их соответствия нормативным требованиям, стандартам юзабилити и этическим принципам проектирования.

оценки воздействия (*data protection impact assessment*) и использоваться для внутреннего контроля[59].

В свою очередь, одним из направлений институционального развития может стать сертификация пользовательских интерфейсов и поведенческих моделей цифровых платформ, включая создание отраслевых стандартов, разработку чек-листов и участие сторонних лиц в оценке интерфейсных решений. Такой подход может позволить системно сдерживать манипулятивное поведение до его выхода на рынок[60].

В то же время бизнесу необходимо выстраивать более сбалансированные модели монетизации, совместимые с правами пользователей (например, контекстную рекламу и работу с данными первого уровня (*first-party data*)), исходя из добросовестных и обоснованных пользовательских отношений. В этом контексте темные паттерны утрачивают свою эффективность, поскольку экономика внимания смещается к формированию доверительных связей с пользователем[61].

Таким образом, перспективы регулирования рекламы на современном этапе развития сферы информационно-коммуникационных технологий определяются не столько запретом отдельных практик, сколько формированием согласованной архитектуры цифровой среды, основанной на уважении автономии пользователя. Как представляется, в центре этой архитектуры должны находиться ключевые принципы предсказуемости, прозрачности и минимизации данных, обеспечиваемые применяемым законодательством и алгоритмами, создаваемыми технологическими компаниями.

В то же время синергия этичного дизайна, возможностей искусственного интеллекта и правовых гарантий защиты прав пользователей может создать условия, при которых цифровая реклама перестанет зависеть от манипуляций и перейдет к взаимным ответственности и доверию.

Заключение

Учитывая вышеизложенное, важно подчеркнуть, что феномен темных паттернов представляет собой значимую правовую проблему, возникшую на фоне трансформации цифровой рекламы и перехода к так называемой эпохе *post-cookie*. Изначально являясь проблемой дизайна пользовательских интерфейсов, темные паттерны приобрели выраженную нормативную релевантность в связи с их широким применением для обхода требований к получению согласия, сокрытия реальных практик обработки данных и создания неравных условий при осуществлении выбора пользователем.

Проведенное сравнительно-правовое исследование позволило прийти к ряду ключевых выводов, касающихся правовых рисков, существующих подходов к регулированию в Европейском

[59] Включение автоматизированных инструментов пользовательского аудита интерфейсов в процедуры оценки воздействия позволяет не только повысить эффективность выявления манипулятивных практик, но и продемонстрировать соблюдение организациями принципа подотчетности, закрепленного, в частности, в ст. 7 *GDPR* (См.: General Data Protection Regulation, 2016 O.J. (L 119) 37).

[60] Имеется в виду использование превентивных механизмов контроля качества, сопоставимых с практикой сертификации в иных высокорисковых сферах (например, в области медицинских изделий или финансовых услуг), что позволяет минимизировать риски для пользователей еще до начала массового применения соответствующих решений.

[61] Подобный сдвиг отражает тенденцию к переориентации бизнес-моделей с краткосрочной максимизации кликов и конверсий на долгосрочное укрепление пользовательской лояльности, что соответствует как принципам, касающимся обработки персональных данных, так и экономической логике устойчивого цифрового рынка.

союзе и Соединенных Штатах Америки, а также перспектив борьбы с манипулятивными интерфейсными практиками, среди которых видится необходимым отметить следующие.

1. Отказ от сторонних *cookie*-файлов и смещение фокуса на интерфейс как основной инструмент взаимодействия с пользователем привели к значительному возрастанию значимости темных паттернов. Они стали ключевым способом обхода требований к информированному согласию и прозрачности обработки данных, что обусловило активизацию деятельности контрольных (надзорных) органов в обеих анализируемых юрисдикциях.
2. Темные паттерны представляют собой многоаспектное правовое явление, затрагивающее сферы защиты данных, конкурентного права, прав потребителей и этики цифрового дизайна.
   В ЕС они рассматриваются преимущественно как нарушения положений действующего законодательства, касающихся действительности согласия и прозрачности обработки данных. В США ФТК квалифицирует их как недобросовестные или вводящие в заблуждение коммерческие практики.
3. Анализ судебных и административных споров в ЕС и США показал, что правоприменительная практика оказывает значительное влияние на поведение цифровых платформ и способствует реформированию интерфейсных решений в сторону большей прозрачности и уважения к выбору пользователя.
4. Применение исключительно мер регулирования *ex post*, реализуемых посредством правоприменительной практики, недостаточно — необходимо создание превентивных мер, направленных на предотвращение манипуляций на этапе разработки интерфейсных решений.
5. Несмотря на различия в правовых системах и подходах, наблюдается формирование общего международного вектора в сторону признания недопустимости манипулятивного интерфейсного поведения и необходимости обеспечения прозрачности обработки данных и защиты автономии пользователя.

В заключение представляется важным подчеркнуть, что на современном этапе развития сферы информационно-коммуникационных технологий в условиях, когда интерфейс выступает ключевым элементом взаимодействия с пользователем, комплексное решение проблемы темных паттернов является необходимым условием для построения сбалансированной, этичной и правомерной цифровой среды.

Список литературы / References

1. Baldwin, R., Cave, M., & Lodge, M. (2011). *Understanding regulation: Theory, strategy, and practice* (2nd ed.). Oxford University Press. https://doi.org/10.1093/acprof:osobl/9780199576081.001.0001
2. Berens, B. M., Bohlender, M., Dietmann, H., Krisam, C., Kulyk, O., & Volkamer, M. (2024). Cookie disclaimers: Dark patterns and lack of transparency. *Computers & Security, 136*, Article 103507. https://doi.org/10.1016/j.cose.2023.103507
3. Blumenthal-Barby, J. S. (2016). Biases and heuristics in decision making and their impact on autonomy. *The American Journal of Bioethics, 16*(5), 5–15. https://doi.org/10.1080/15265161.2016.1159750
4. Brenncke, M. (2024). Regulating dark patterns. *Notre Dame Journal of International & Comparative Law*, *14*(1), 39–79.
5. Brignull, H., Miquel, M., Rosenberg, J., & Offer, J. (2015). Dark patterns-user interfaces designed to trick people. *In Proceedings of the Poster Presentation, Australian Psychological Society Congress*, 21–23.

6. Cohen, J. (2019). Bringing down the average: the case for a "less sophisticated" reasonableness standard in US and EU consumer law. *Loyola Consumer Law Review*, 32(1), Article 2.
7. Edidin, B., Kochetkova, K., & Sarankina, N. (2024). Digital abuse: How dark patterns manipulate our lives. *Legal Issues in the Digital Age*, *5*(4), 4–27. https://doi.org/10.17323/2713-2749.2024.4.4.27
8. Gjorgjieski, V. (2024). Ethical standards in graphic design. *Knowledge International Journal*, *66*(5), 575–578.
9. Gray, C., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. (2018). The dark (patterns) side of UX design. In R. Mandryk (Ed.), CHI EA '18: Extended abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (Article 534). *Association for Computing Machinery*. http://dx.doi.org/10.1145/3173574.3174108
10. Kahneman, D. (2013). Foreword. In E. Shafir (Ed.), The behavioral foundations of public policy (pp. VII–IX). *Princeton University Press*.
11. Kollmer, T., & Eckhardt, A. (2023). Dark patterns. *Business & Information Systems Engineering*, 65(2), 201–208. https://doi.org/10.1007/s12599-022-00783-7
12. Leiser, M., & Santos, C. (2024). Dark patterns, enforcement, and the emerging digital design acquis: Manipulation beneath the interface. *European Journal of Law and Technology*, 15(1), 1–30. https://ejlt.org/index.php/ejlt/article/view/990
13. Li, D. (2022). The FTC and the CPRA's regulation of dark patterns in cookie consent notices. *The University of Chicago Business Law Review*, 1(1), 561–590.
14. Mathur, A., Mayer, J., & Kshirsagar, M. (2021). What makes a dark pattern... dark?: Design attributes, normative considerations, and measurement methods. In Y. Kitamura, A. Quigley, K. Isbister, T. Igarashi (Eds.), *CHI EA '21: Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (Article 360). Association for Computing Machinery. https://doi.org/10.1145/3411764.3445610
15. Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In R. Bernhaupt, F. Mueller, D. Verweij, J. Andres (Eds.), *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)* (pp. 1–13). Association for Computing Machinery. https://doi.org/10.1145/3313831.3376321
16. Santos, C., Morozovaite, V., & De Conca, S. (2025). No harm no foul: How harms caused by dark patterns are conceptualised and tackled under EU data protection, consumer and competition laws. *Information & Communications Technology Law,* 34(3), 329–375. https://doi.org/10.1080/13600834.2025.2461958
17. Tran, V. H., Mehrotra, A., Sharma, R., Chetty, M., Feamster, N., Frankenreiter, J., & Strahilevitz, L. (2024). *Dark patterns in the opt-out process and compliance with the California Consumer Privacy Act (CCPA).* ArXiv. https://doi.org/10.48550/arXiv.2409.09222

Сведения об авторе:

Корж Д. В. — магистр права, факультет права, Национальный исследовательский университет «Высшая школа экономики»; юрист-аналитик, Аппарат Общественной палаты Российской Федерации, Москва, Россия.
dvkorzh@icloud.com
ORCID: https://orcid.org/0009-0002-0624-7664

Information about the author:

Denis V. Korzh — LL.M, Faculty of Law, HSE University; lawyer-analyst, Executive Office of the Civic Chamber of the Russian Federation, Moscow, Russia.
dvkorzh@icloud.com
ORCID: https://orcid.org/0009-0002-0624-7664

https://doi.org/10.38044/2686-9136-2025-6-2-91-111

СТАТЬИ

ВИРТУАЛЬНОЕ ПРОСТРАНСТВО И ИГРОВОЕ ИМУЩЕСТВО: АСПЕКТЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

А. Ж. Пагов

Санкт-Петербургский государственный университет
199034, Россия, Санкт-Петербург, Университетская наб., 7–9

Аннотация

Статья посвящена анализу правового режима виртуального игрового имущества как особого вида виртуального мира, обладающего уникальными характеристиками и правовыми аспектами. Актуальность работы определяется отсутствием четкого нормативно-правового регулирования оборота виртуального игрового имущества и его защиты в условиях стремительного развития гейминг-индустрии в цифровой среде, что создаёт правовые пробелы и угрозы законным интересам миллионов пользователей. Целью исследования является выявление ключевых характеристик виртуального игрового имущества и определение адекватных правовых механизмов его защиты посредством анализа как международных, так и национальных подходов к регулированию данного феномена. Методология включает сравнительный анализ существующих концепций правового регулирования виртуального игрового имущества, систематическое изучение пользовательских соглашений ведущих игровых платформ, критический анализ правомерности применения традиционных терминов «собственность» и «имущество» в цифровой среде, а также историко-правовой анализ развития подходов к регулированию цифровых активов. Основные результаты определяют виртуальное игровое имущество через совокупность его характеристик: экономическую ценность, возможность передачи и отчуждения третьим лицам, а также существование исключительно в пределах виртуального игрового пространства. Проведённый анализ выявляет границы юрисдикции виртуальных игровых миров, механизмы обеспечения баланса законных интересов разработчиков и рядовых пользователей. Автором дополнительно проводится историческая параллель между «цифровой властью» разработчиков и концепцией недвижимого имущества в странах общего права (*real estate*). Исследование разграничивает результаты интеллектуальной деятельности разработчиков на созданные ими цифровые объекты и права пользователей, детализируя механизмы владения, установленные в пользовательских соглашениях. В заключение сформулированы ключевые дефиниции, определяющие правовой режим виртуального игрового имущества, а также предложены практические рекомендации по совершенствованию правоприменения и законодательного урегулирования, направленные на адекватную защиту прав игроков-потребителей с учетом уникальной природы виртуального игрового имущества и его растущей экономической значимости.

Ключевые слова

магический круг, виртуальное игровое имущество, свобода договора, пользовательское соглашение, защита прав потребителей, имущественные права, законный интерес

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

Благодарность Автор выражает благодарность В. В. Архипову за ценнейшие замечания при подготовке настоящей работы.

Для цитирования Пагов, А. Ж. (2025). Виртуальное пространство и игровое имущество: аспекты правового регулирования. *Цифровое право, 6*(2), 91–111. https://doi.org/10.38044/2686-9136-2025-6-2-91-111

Поступила: 03.04.25, принята в печать: 21.05.25, опубликована: 30.06.2025

ARTICLES

VIRTUAL SPACE AND IN-GAME PROPERTY: ASPECTS OF LEGAL REGULATION

Astemir Zh. Pagov

Saint Petersburg State University
7–9, Universitetskaya Embankment, St. Petersburg, Russia, 199034

Abstract

This article examines the legal regime of virtual in-game property as a distinctive phenomenon of the digital environment, characterized by specific attributes and legal implications that differentiate it from traditional forms of property. The study's especially relevant because of the absence of clear statutory regulation governing the transfer, exchange, and alienation of virtual in-game assets and the mechanisms for their legal protection amid the rapid expansion of the gaming industry in digitally mediated markets. This regulatory gap generates legal uncertainty and exposes the legitimate interests of millions of users to heightened risks. The purpose of the research is to identify the core characteristics of virtual in-game property and to determine adequate legal instruments for its protection by analyzing both international and domestic approaches to regulating this phenomenon. The methodology combines: comparative analysis of existing regulatory concepts addressing virtual in-game property; a systematic review of end-user license agreements and terms of service of leading gaming platforms; a critical assessment of the doctrinal and practical appropriateness of applying traditional categories such as "property" and "ownership" to digital environments; and a historical analysis of the evolution of approaches to digital assets. The principal findings define virtual in-game property through a set of cumulative features: economic value, functional transferability and potential alienability vis-à-vis third parties, and existence exclusively within the boundaries of a virtual game space. The analysis also delineates the jurisdictional contours of virtual game worlds and identifies mechanisms for maintaining a balance between the lawful interests of developers and ordinary users. Additionally, the author draws a historical parallel between developers' "digital power" and the common-law concept of real estate, highlighting structural similarities in control over access, use, and exclusion. The study differentiates the developers' intellectual creations embodied in digital objects from users' entitlements, detailing the possession and use models embedded in contractual user agreements. The article concludes by proposing key definitions shaping the legal regime of virtual in-game property and offering practical recommendations for improving law enforcement practice and legislative policy, aimed at ensuring effective protection of player-consumers' rights while accounting for the unique nature of virtual in-game assets and their increasing economic significance.

Keywords

magic circle, virtual gaming assets, freedom of contract, user agreement, consumer protection, property rights, legal interest

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
Acknowledgments	The author expresses gratitude to V. V. Arkhipov for his invaluable comments during the preparation of this work.
For citation	Pagov, A. Zh. (2025). Virtual space and in-game property: Aspects of legal regulation. *Digital Law Journal, 6*(2), 91–111. https://doi.org/10.38044/2686-9136-2025-6-2-91-111

Submitted: 3 Apr. 2025, accepted: 21 May 2025, published: 30 June 2025

Введение

Согласно аналитическим оценкам платформы *Newzoo,* к концу 2026 г. объем мирового рынка игр составит 205,7 млрд долл., а число игроков в мире достигнет 3,79 млрд[1]. С учетом представленных подсчетов кажущаяся ранее многим исследователям в сферах экономики, культурологии и юриспруденции в онтологическом понимании несерьезной (Arkhipov, 2019b, p. 14) тема видеоигр трансформируется в предмет различных дискуссий как на уровне лекционных занятий в университете, так и на уровне международных конференций.

Одним из вопросов, с которыми приходится сталкиваться не только в рамках социально-гуманитарного исследования, но и на практике, является проблема подходящего механизма регулирования оборота *виртуального игрового имущества*. Так, в большинстве онлайн-видеоигр вроде *Call of Duty: Warzone, Counter-Strike 2, Dota 2* пользователи имеют возможность приобрести напрямую за реальные деньги определенный облик для персонажа игры или любой другой атрибут, существующий в игровом пространстве. Стоимость таких атрибутов разнится в зависимости от наличия уникальной способности, качества, уровня, косметической составляющей.

На важность рынка виртуального игрового имущества указывает тот факт, что в марте 2025 г. общая капитализация рынка *скинов* (от *skin* — «кожа») в игре *Counter-Strike 2* превысила 4,3 млрд долл.[2] Актуальность исследования, помимо прочего, подтверждается резонансной инициативой игрового сообщества *Stop Killing Games.* В 2025 г. петиция в рамках программы *European Citizens' Initiative* собрала 1,4 млн подписей, что позволило напрямую направить в Европейскую комиссию предложение обязать разработчиков видеоигр либо обеспечивать полноценную офлайн-поддержку проектов, либо раскрывать их исходный код, предоставляя игрокам возможность самостоятельного технического обслуживания (https://www.stopkillinggames.com/).

Правовой режим цифровой среды предопределяет оборотоспособность игровых объектов, особенности которых равным образом влияют на нормативное регулирование виртуального игрового пространства, как части цифровой среды. Так, задача любого автора состоит в том, чтобы его сформированное научное мнение по итогу стало продуманным и отрефлексированным знанием читателя, что, в свою очередь, станет частью научного дискурса в широком смысле. Поэтому для повышения уровня научности знания необходимо представить многообразие критически оцененных идей и концепций, также используя сравнительно-правовой метод.

[1] Newzoo. (2023). *Newzoo's Global Games Market Report 2023.* https://newzoo.com/resources/trend-reports/newzoo-global-games-market-report-2023-free-version

[2] D'Anastasio, C. (2025). Market for "Counter-Strike 2" digital items hits new high. Bloomberg. https://www.bloomberg.com/news/articles/2025-03-07/market-for-counter-strike-2-digital-items-hits-all-time-high

Понятие виртуального игрового пространства

Анализ и поиск решения конфликта между реальным и виртуальным невозможны без четких дефиниций соответствующих категорий и понимания сути проблемы, поскольку, помимо отсутствия универсальных правовых средств, позволяющих урегулировать серые зоны, с каждым днем множатся коллизии, возникающие не столько из-за быстроты научно-технического процесса, что также важно, сколько из-за отставания разработки устойчивых социальных регуляторов, в частности правовых. Ниже будут представлены определения, релевантные для целей и задач данной научной работы.

Виртуальное игровое пространство есть нечто, симулируемое компьютерными алгоритмами, создающими мнимую для физической реальности площадку, объединяющую пользователей с целью коммуникации между собой и самой программой, а также помогающую выстраивать игроку свою психологическую идентичность (Shevtsov, 2018, p. 102) в процессе осуществления действий в определенных границах функционала игры.

По мнению Эдварда Кастроновы[3], виртуальные миры имеют три определяющие характеристики:

- *интерактивность* (*interactivity*): виртуальный мир существует на одном компьютере, но возможен доступ удаленно, т. е. через интернет-соединение, также одновременно с присутствием большого количества пользователей-аватаров[4], которые осуществляют дозволенные действия через ввод команд, пользуясь специально предназначенным устройством вроде компьютерной мыши, клавиатуры, геймпада и т. д.;
- *физичность* (*physicality*): пользователи-аватары получают доступ к программе через интерфейс, который имитирует физическое окружение (чаще всего от первого лица) на экране используемого устройства. Степень физичности окружения обычно зависит от вида виртуального мира и проработанности его имитации законов реального мира;
- *постоянство* (*persistence*): виртуальный мир продолжает работать независимо от того, использует его кто-либо или нет, так как алгоритм мира «запоминает» положение виртуальных объектов и их принадлежность после сохранения системой или самим пользователем-аватаром.

Эти основные качества виртуального пространства раскрывают его специфику по отношению к реальному. Однако предметом исследования является именно виртуальное игровое пространство, так как виртуальное пространство родилось и развилось до современного уровня в первую очередь как игровая среда (Fairfield, 2005, p. 1052). Виртуальное игровое пространство имеет дополнительные характеристики.

Первым ключевым свойством виртуального игрового пространства как разновидности виртуального пространства является предоставление пользователю способности реализовать суть игрового процесса — ***аутотеличность***[5]. Самоценность игрового процесса отмечал

[3] Castronova, E. (2001). *Virtual worlds: A first-hand account of market and society on the cyberian frontier* (Working Paper No. 618, pp. 5–6). CESifo. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=294828

[4] Руне Клевьер считает, что *аватар* — это инструмент или механизм, который определяет для пользователя виртуального мира цифровую проекцию самого себя. Функционал аватара зависит от вида виртуального мира (игровое пространство, *URL*, конкретный аккаунт в социальной сети), и он действует как динамически рефлексивный объект по отношению к окружению (Klevjer, 2022, pp. 93–101).

[5] Аутотеличность (лат. *autotelic* — «цели в самом себе») — свойство деятельности, обусловливающее желание индивида участвовать в ней с целью получения опыта данной деятельности; самоценность; самодостаточность (Kazakova, 2017, p. 14).

нидерландский философ Йохан Хёйзинга, указывая на то, «что есть игра сама по себе и что она означает для самих играющих лишь второстепенное место» (Huizinga, 1997, p. 22), ведь игровой процесс интересен чаще всего не столько генерацией внутриигровых смыслов и ценностей, сколько возможностью быть вовлеченным в этот процесс по своей воле, иногда бесцельно. Из этого вытекает второе ключевое свойство — ***напряжение*** от игры (Huizinga, 1997, p. 30), так как оно подвергает игрока испытанию: его физические силы, умственные способности, упорство, умение следовать правилам.

Через аватара игрок становится частью процесса, который может и не иметь заключительного этапа или уровня, однако сам процесс от этого не становится хуже, ведь чаще всего результатом игры является не полученный титул или предмет в инвентаре (материальный и нематериальный), а ***катарсис*** — высвобождение эмоций при восприятии произведений искусства, что особо применимо к современным видеоиграм, если брать не столько стоимость разработки игр, а их качество и эстетическую наполненность. Именно катарсис является третьим свойством как игры в целом, так и виртуального игрового пространства в частности, проявляясь в каждом игроке с различной степенью воздействия на эмоциональный фон, ибо, путешествуя в цифровой оболочке аватара, игрок может испытывать азарт, страх, вдохновение, безразличие, увлеченность.

Применение концепции очерченного магического круга и аналогии с реальным

Проблематика соотношения правил реального и виртуального мира поднимается в рамках не только дискурса о правовом регулировании оборота виртуального игрового имущества, но и выделения гипотетической границы действия норм права по отношению к игрокам внутри виртуального мира. Концепции, старающиеся очертить таковые гипотетической пределы, соотносятся с метафорой Й. Хёйзинги, описывающей временны́е, а также пространственные ограничения игры — магического круга (Huizinga, 1997, p. 28).

Идея отграничения виртуального от реального должна иметь отражение не только в правовой науке, но и законе. Э. Кастронова утверждает, что «в прошлом закон проявлял себя благосклонно к построению магических кругов и фантастических творений и энергично защищал их. Например, корпорация определяется в законе как вымышленное лицо» (Castronova, 2004, p. 186).

В научном пространстве выделяют три культуролого-социологические интерпретации феномена магического округа, но, как отмечается правоведами, два подхода не универсальны для юридической науки и практики (Fairfield, 2009, pp. 834–835), а третий применяется лишь при междисциплинарном анализе возможных юридически значимых качеств предмета общественных отношений, которые возникают и развиваются в условиях медиального поворота (Arkhipov, 2019b, pp. 247–264). Поэтому для целей данной работы сто́ит ограничиться концепцией правового регулирования отношений, связанных исключительно с оборотом виртуального игрового имущества, представив следующий подход и интерпретацию магического круга, которые основываются на синергии различных частей вышеуказанных подходов.

Разумным можно считать то просачивание реального права (чаще всего с целью наложить санкции) в виртуальную коммуникацию по поводу оборота игрового имущества, которое обусловлено грубым нарушением правил игры пользователем[6].

[6] Например, см.: *Take-Two Interactive Software, Inc. v. James*, [2020] EWHC 179 (Pat) (Eng.), http://www.bailii.org/ew/cases/EWHC/Patents/2020/179.html

Для применения данного подхода нужно соблюдение следующих условий:

- игровое имущество должно иметь валютную ценность не только для ограниченного круга лиц[7];
- грубым нарушением признается только то, что позволяет игроку обогатиться, не прикладывая усилий или не заключая разрешенных сделок с получением игровых объектов;
- нарушение баланса законных интересов сторон: разработчики целенаправленно запрещают пользователям производить оборот игрового имущества, опираясь лишь на свой экономический интерес.

Неотъемлемой частью поиска ответа на вопрос, насколько возможно применять правила реального мира к виртуальному, представляется выбор релевантной аналогии. Ниже будут представлены два кажущихся логичными и взвешенными примера того, насколько реальное право в широком смысле конструирует правила виртуального пространства.

Юрисдикционный подход к определению пределов компетенций и полномочий властного субъекта – разработчика / издателя видеоигры, на базе которой существует виртуальное пространство

Несмотря на отсутствие в мировом сообществе единого понимания категории «юрисдикция», для целей настоящей работы примем нейтральное определение. Государство осуществляет свою юрисдикцию посредством установления правил (законодательная юрисдикция), процедур выявления нарушений и определения последствий нарушений (судебная юрисдикция) и принудительного применения последствий за предполагаемые нарушения (правоприменительная юрисдикция) (Tebenkova, 2024, p. 180). То есть юрисдикция представляется в виде очерченного круга полномочий и компетенций властного субъекта, распространяющего свою власть внутри устойчивой системы на своих подданных.

Разработчики игр устанавливают обязательные нормы поведения в рамках пользовательских соглашений, правил сообщества, игровых механик. Эти правила игры обязательны для всех участников, их принятие и соблюдение являются условием доступа к виртуальному пространству. Это функционально аналогично законодательной юрисдикции государства, устанавливающего обязательные правовые нормы в пределах своей юрисдикции (территории и зоны влияния).

Кроме того, игровые платформы обладают техническими средствами контроля и принуждения: они могут блокировать аккаунты за нарушение правил, ограничивать доступ к виртуальному имуществу. Принуждение осуществляется за счет контроля над самим кодом виртуального игрового пространства.

Судебная юрисдикция раскрывается через службу поддержки или центры медиации у разработчиков, которые применяют их в качестве собственных механизмов разрешения споров.

[7] Тест на социальную валютную ценность состоит из двух обязательных элементов, применяемых последовательно. Во-первых, это наличие у предмета коммуникативного значения, определяемого контекстом социального взаимодействия. Во-вторых, это конвертируемость данного коммуникативного значения в произвольный обобщенный символический посредник. В теоретической социологии и политической науке с достаточной ясностью разработаны лишь два таких символических посредника: деньги и политическая власть (Arkhipov, 2019a, p. 87).

Концепция *real estate* как попытка объяснить отличительные черты научного подхода, сформированного под влиянием социокультурного мироощущения зарубежных исследователей

Ни для кого не является секретом, что первыми исследователями в области виртуального пространства стали юристы и правоведы, воспитанные и обученные в рамках англосаксонской правовой семьи: Грег Ластовка, Эдвард Кастронова, Лоуренс Лессиг, Ричард Бартл, Дэн Хантер и др. Следовательно, для более глубокого погружения в проблематику нужно понять, как и на основании чего были сделаны выводы о необходимости правового регулирования виртуального пространства. Предпринятая попытка увенчалась выдвижением гипотезы о том, что концепция цифровой власти» (см. ниже), когда фактическое обладание виртуальным объектом существует с иллюзией права собственности, так как формальная власть принадлежит суверену (в противовес институту собственности в романо-германской правовой семье), косвенно связана с понятием *real estate.* Поэтому обращение к истокам земельного права в Великобритании позволит проследить по аналогии, как юридическое закрепление фактического обладания объектом суверенной власти за пользователем может эволюционировать в сторону признания правомочий этого пользователя.

Основой британского земельного права стал Закон 1925 г. «О регистрации прав на земельные участки», в котором были упорядочены разрозненные и противоречивые акты средневековой Британии[8]. Положениями этого Закона сформулированы два основных вида прав на землю: право собственности *(estate in fee simple, freehold)* и аренда на указанный в годах срок *(estate for term of years, leasehold)*[9]. В современном земельном праве Англии по-прежнему отсутствует понятие «собственник земли» или «право собственности на землю», поскольку *любая земля находится в собственности Короны как суверена, а ее подданные могут приобретать лишь ленные права.* С юридической точки зрения Корона до сих пор является единственным собственником всей земли в Великобритании, а все остальные землевладельцы владеют землей под покровительством Короны.

Таким образом, с определенными оговорками уместна аналогия, в соответствии с которой цифровая власть создателя виртуального пространства является не чем иным, как властью суверена над территорией и подданными, т. е. игроками. Это подтверждает возможность применять правовые нормы к взаимоотношениям, строящимся в виртуальном игровом пространстве.

Применение понятий «собственность» и «имущество» в виртуальном игровом пространстве

Конституция РФ в ст. 35 раскрывает право иметь имущество в собственности лишь в общих чертах через указание на триаду правомочий владения, пользования и распоряжения как в единоличном, так и совместном с другими собственниками порядке[10]. Статья 209 ГК РФ[11] посвящена уже более подробному содержанию права собственности и указывает на то, что собственник

[8] Land Registration Act 1925, 15 & 16 Geo. 5 c. 21 (U.K.).

[9] Husselbee, R., & Allen, A. (2024, December 16). *Real estate laws and regulations: England & Wales 2025.* ICLG.com. https://iclg.com/practice-areas/real-estate-laws-and-regulations/england-and-wales

[10] Конституция Российской Федерации, принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020, www.pravo.gov.ru

[11] Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ. Собрание законодательства РФ. 1994. № 32. Ст. 3301.

вправе по своему усмотрению совершать любые действия в отношении принадлежащего ему имущества, т. е. называет в качестве объекта права собственности довольно размытую правовую категорию «имущество» (Rybalov, 2017, p. 14).

Вводя в систему размышлений еще одну статью, а именно посвященную объектам гражданских прав статью 128 ГК РФ[12], отметим, что категория «имущество» является родовой, так как включает вещи (наличные деньги и документарные ценные бумаги), имущественные права (бездокументарные ценные бумаги, цифровые права, безналичные денежные средства), иное имущество и т. д. Определенным умозаключением из вышенаписанного будет то, что право собственности в силу своей природы юридически закрепляет принадлежность имущества конкретному лицу, однако возникает вопрос о принадлежности имеющих имущественную ценность объектов виртуального игрового пространства к имуществу не только в бытовом понимании, но и с точки зрения права (Sklovsky, 2023, pp. 296–301).

Пытаясь найти обоснование отнесения виртуальной собственности (в частности, игровой) к уже сформированным в правовом поле формам собственности, большинство ученых проецируют отношения, возникающие по поводу виртуальных игровых объектов, на регулирование схожих отношений в реальном мире через переосмысление существующих теорий собственности, философских рассуждений, а также через анализ экономических сдержек и противовесов. Лучше всего это описано в научном дискурсе Грега Ластовки и Дэна Хантера (Lastowka & Hunter, 2004, p. 43): для них очевидно, что виртуальные активы можно охарактеризовать как собственность при соблюдении разумных ограничений. Ластовка и Хантер опирались на анализ трех ключевых, по их мнению, концепций: трудовую теорию собственности Локка[13], утилитаризм Бентама и Милля[14], учение о личности Гегеля[15]. Нельзя не согласиться с выводами Грега Ластовки и Дэна Хантера о том, что в соответствии с традиционными концепциями собственности нет никаких оснований для исключения виртуальной собственности из сферы правовой защиты, поскольку не существует колоссального описательного разрыва между системой собственности в реальном мире и виртуальными активами (Lastowka & Hunter, 2004, p. 49). То, какая теория больше подходит

[12] Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ. Собрание законодательства РФ. 1994. № 32. Ст. 3301.

[13] Смысл теории Локка заключается в том, что человек, затративший труд на превращение «вещи в природе» в ценную форму, заслуживает того, чтобы пожинать плоды своих усилий, что в итоге переводит вещь в разряд его собственности после процесса «перемешивания труда с элементом природы». Это представляется метафорой для обозначения производительной деятельности (Locke, 2021, p. 24). В контексте виртуального мира можно сделать вывод, что игрок не может претендовать на имущественные интересы во всем мире, но вправе законно претендовать в какой-то меньшей части — виртуальном объекте (например, игровые предметы или объекты виртуальной недвижимости), в котором его труд составляет бóльшую часть стоимости.

[14] Базовый принцип утилитаризма Д. Бентама заключается в стремлении к наибольшему благу для наибольшего числа людей и обеспечивает основу и для современного применения экономики почти к каждому виду человеческой деятельности. С утилитарной точки зрения общественное благо состоит из совокупности индивидуальных благ (Bentham, 1998, p. 9; Mill, 1900, p. 115). Так, для миллионов игроков, трудящихся над созданием и получением ценных объектов, существуют утилитарные основания для признания виртуальных активов собственностью.

[15] Личностная теория впервые была выведена Г. Гегелем и представляет констатацию того, что собственность есть продолжение личности. Собственность расширяет естественную сферу свободы человеческого индивида за пределы его тела до соответствующей части материального мира (Hegel, 2021, p. 45). Эта концепция находит отражение и в контексте виртуального имущества, поскольку основывается на влиянии любого (реального или виртуального) имущества на такие человеческие потребности, как свобода и идентичность, порождающем ценность.

для получения такого вывода, остается на усмотрение исследователей и относится к разряду юридических предпочтений.

Возвращаясь в прикладную область настоящей работы, нельзя не отметить следующее. Верховный Суд РФ неоднократно указывал, что право собственности, согласно ст. 209 ГК РФ, может признаваться только на индивидуально определенную вещь, которая реально существует в натуре[16], поэтому виртуальные объекты формально не могут регламентироваться нормами о праве собственности ввиду их выраженного цифрового и нематериального характера. Значит, на данном этапе развития отечественной цивилистики право не готово признать виртуальные объекты в качестве подлежащих охране.

Впрочем, если рассматривать конструкции некоторых договоров, то можно подвергнуть расширительному толкованию понятие «вещь» не только в теории, но и на практике: можно наблюдать фактическое распространение правового режима вещей на некоторые объекты, не являющиеся вещами в традиционном понимании; например, электроэнергия выступает товаром в договоре энергоснабжения (ст. 539 ГК РФ) (Stepanov, 2016, p. 228).

Характеристики и особенности виртуального игрового имущества

Игровое имущество является специфическим видом виртуального имущества и имеет ряд отличительных характеристик. Исходя из того что вид соответствует роду в своих общих признаках и, следовательно, не может противоречить ему, можно обозначить признаки, которые присущи всем видам виртуального имущества, и вывести специфические черты исключительно виртуального игрового имущества.

Общие признаки виртуального имущества

Общими признаками, свойственными любому виду виртуального имущества, являются[17]:

- **Нематериальный характер**

Исключительно *нематериальный характер* виртуального имущества, выводимый из самого его существа, поскольку с технической точки зрения оно представляет собой не что иное, как программный код, являющийся составной частью главной программы, в отдельности от которой он не имеет ценности или вовсе не может соответствовать заданному изначально функционалу.

- **Цифровая триада правомочий управомоченного пользователя**

Разработанная по аналогии с классической моделью собственности цифровая триада правомочий предполагает выделение в цифровой среде пользования, владения и распоряжения, причем каждое из них приобретает специфическое содержание. Цифровое пользование выражается в функциональном применении виртуальных объектов по их назначению, например при отправке платных или кастомизированных смайликов в мессенджере или использовании внутриигрового предмета. Цифровое владение следует рассматривать как фактическое господство над цифровой вещью (аккаунтом, инвентарем, объектом внутриигрового имущества), обеспеченное техническими средствами аутентификации и сопровождаемое

[16] Определение Верховного суда РФ от 23 апреля 2013 г. № 5-КГ13-15.

[17] European Law Institute. (2022). *ELI principles on the use of digital assets as security* (Report of the European Law Institute). https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf

волей на удержание контроля. Оно предполагает наличие у лица инструментов доступа (логин, пароль, факторы двухфакторной аутентификации, привязанные устройства), возможность исключать иных лиц из использования объекта (смена пароля, отзыв активных сессий, деавторизация устройств), устойчивость контроля во времени (механизмы восстановления доступа) и признание этого контроля самой платформой. Внутри данного института можно разграничить непосредственное (наличие полного набора средств аутентификации у одного лица), производное (допуск иного лица волей непосредственного владельца, например через семейный доступ или передачу одноразового кода) и опосредованное владение (сохранение возможности восстановления контроля при временной передаче доступа). Так, при передаче идентификаторов и кодов *Steam Guard* другому лицу последнее получает фактическое господство, тогда как исходный владелец сохраняет способность восстановить контроль. При передаче же всех факторов аутентификации и отключении восстановлений контроль становится производным у получателя в пределах, допускаемых политикой платформы. Наконец, цифровое распоряжение проявляется в исключительной возможности определить правовую и фактическую судьбу виртуального объекта — от отчуждения предметов через внутриигровой рынок до их удаления или лишения третьих лиц доступа. Таким образом, цифровая триада воспроизводит классическую структуру, но наполняется техническими критериями доступа и архитектурой платформ, что позволяет концептуализировать специфику оборота виртуальных объектов в праве.

Так, создатели виртуального пространства и/или уполномоченные ими лица, например регистраторы доменных имен, разработчики или издатели видеоигр, руководствуясь определенными предписаниями и техническим потенциалом рабочих устройств, обладают возможностью определять судьбу виртуального имущества, использовать фактические способности для вмешательства в чужое цифровое владение или цифровое присутствие, т. е. имеют *«цифровую власть» (digital force)* (Palka, 2017, p. 172). Представленные властные субъекты, во-первых, устанавливают *правила взаимодействия в виртуальном пространстве*, во-вторых, *выступают наиболее защищенной стороной в лицензионном договоре присоединения*, в котором лицензиат акцептует предложенное соглашение без возможности внести изменения, и, наконец, в-третьих, осуществляют поддержание исправности виртуальных систем, от которых зависит осуществимость действий пользователей в рамках виртуального пространства, и т. д.

При обращении к догматике цивилистической науки концепцию цифровой власти допустимо отождествить с возможностью субъекта гражданских правоотношений односторонним волеизъявлением вызвать правовые последствия для лица, которому адресовано данное волеизъявление, т. е. с секундарными (потестативными) правами (Rybalov, 2007, pp. 41–46). Важность представленного «научного реверанса» в том, что праву субъекта, определяющего судьбу виртуального пространства и выступающего стороной в договорных отношениях с игроками, не корреспондирует обязанность другого субъекта совершить или воздержаться от определенных действий, а возникает необходимость претерпевания правомерного ограничения сферы его юридической автономии со стороны управомоченного лица. Например, когда экономически нецелесообразным становится поддержание бесперебойного функционирования серверов многопользовательской видеоигры по причине снижения активности игроков, компания-разработчик может их отключить и направить ресурсы на более перспективные проекты[18].

[18] Некоторые авторы разумно предполагают возможность передачи безвозмездно прав на такие игры с соответствующей обязанностью поддерживать и разворачивать частные серверы (Graf, 2024, pp. 37–38).

Игроку как второй стороне в правоотношениях ничего не остается, кроме как претерпевать определенные правовые последствия (расторжение соглашения и прекращение доступа к своему виртуальному игровому имуществу), возникшие из одностороннего и целенаправленного волеизъявления первой стороны[19].

- **Оборотоспособность**

По общему правилу у пользователя есть возможность распоряжаться виртуальным имуществом, имеющим для рынка виртуальных объектов экономическую ценность (Martyanova, 2020, p. 168). Однако есть примеры ограниченных в обороте объектов по соглашению с разработчиком (лицензионное соглашение с конечным пользователем для *EMEA Blizzard*[20]) или по существу (виртуальное игровое имущество в однопользовательских играх без возможности передачи).

Ключевые признаки виртуального игрового имущества

При этом *ключевыми* признаками исключительно виртуального игрового имущества, по нашему мнению, можно считать суть следующие его характеристики.

- **Неотделимость от взаимосвязанных игровых площадок и сервисов**

Виртуальное игровое имущество является частью видеоигры как программы для ЭВМ или сложного объекта в зависимости от структуры. Представляя дополнительный контент, игровое имущество функционально и эйдетически не имеет ценности за пределами конкретного виртуального мира, поскольку эксплуатируется пользователем через свой аватар в процессе игры и для ее прохождения (Perepyolkina, 2020, p. 50).

- **Зависимость от режима видеоигры (однопользовательский и многопользовательский)**

Данный признак имеет особое значение, если опираться на личностную теорию виртуальной собственности, которая устанавливает режим права собственности при условии, что объекты и права глубоко связаны с самоощущением человека при коммуникации с остальными пользователями. Указанное возможно только в многопользовательском режиме.

- **Механизм передачи**

Поскольку экономическую ценность игровое имущество представляет не только для игроков, но и для разработчиков, последние ограничивают возможность распоряжаться приобретенными объектами игрового мира в правилах и лицензионных соглашениях (пользовательских соглашениях, *EULA* (*end-user license agreement*)). Например, платформа *Steam* предлагает воспользоваться либо «Торговой площадкой» для продажи на виртуальном рынке с установлением своей цены, либо, если нужно передать определенному игроку, «Предложением обмена». Также возможно передать виртуальное игровое имущество вместе со своим аккаунтом в видеоигре, однако большинство компаний прямо запрещают сообщать другим лицам свой логин и пароль к аккаунту, ибо аккаунт возникает в рамках обязательственных правоотношений

[19] Самым актуальным примером того, как игроки пытаются оспорить действия разработчика/издателя по отключению серверов, является судебное дело *Cassell v. Ubisoft Ent. S.A.,* No. 2:24-cv-03058-DAD-CSK (E.D. Cal. filed Nov. 4, 2024), https://ru.scribd.com/document/790913960/Crew-Lawsuit-via-Polygon

[20] *End User License Agreement,* https://www.blizzard.com/en-us/legal/fba4d00f-c7e4-4883-b8b9-1b4500a402ea/blizzard-end-user-license-agreement (Mar. 10, 2025).

конкретного лица с провайдером услуг, а указанные манипуляции являются переменой лиц в обязательстве без согласия кредитора[21].

Предметный анализ подходов к правовому регулированию оборота виртуального игрового имущества

На данный момент в юридическом научном пространстве представлены несколько подходов к возможности применения норм права к виртуальному имуществу в целом. Каждая позиция имеет свою аргументацию и доктринальное обоснование, однако, интерпретируя право как коммуникативное воззрение между субъектами и опираясь на семантическое восприятие мира вещей и идей, сто́ит выделить ту концепцию, которая образует новые формы реализации правовых отношений и запустит процесс легитимации таковых.

Применение норм права об играх и пари к отношениям, связанным с оборотом виртуального имущества

В соответствии с данным подходом пользователь использует виртуальное игровое имущество на собственный страх и риск, поскольку нет гарантий того, что видеоигра и внутренний контент будут функционировать бесперебойно и непрерывно. Указанное, по мнению судов, принимающих эту позицию, свидетельствует о возможности применения пункта 1 ст. 1062 ГК РФ, согласно которому требования граждан и юридических лиц, связанные с организацией игр и пари или с участием в них, не подлежат судебной защите, за исключением требований лиц, принявших участие в играх или пари под влиянием обмана, насилия, угрозы или злонамеренного соглашения их представителя с организатором игр или пари[22].

Подход верен лишь при подробнейшем анализе пользовательского соглашения, добросовестности сторон, функциональных возможностей самой видеоигры. Если игрок вкладывает денежные средства в улучшение аватара в однопользовательской игре, и спустя некоторое время игру перестают обновлять (о чем заблаговременно предупредил разработчик), что, в свою очередь, может привести к некорректному функционированию видеоигры и ухудшению игрового опыта, то кажется разумным применение нормативных положений об играх и о пари. Однако целенаправленное ограничение оборота виртуального игрового имущества в многопользовательских играх без должного оповещения пользователей со стороны разработчиков уже не может квалифицироваться как деятельность на свой страх и риск, ибо сущностно это изъятие у виртуального собственника ограниченного сроком имущественного права вопреки его воле и без соразмерной компенсации.

Вещно-правовая концепция, определяющая режим виртуального имущества

Частично данная концепция уже была затронута, поэтому целесообразно не поднимать вопрос абсолютности имущественных прав на игровые объекты, а высказать несколько критических замечаний, которые также упоминались исследователями.

Так, «распространение режима вещей на цифровые “вещи” является закономерным результатом технического прогресса и логическим развитием вещного права в новом виртуальном пространстве» (Doiev, 2023, p. 9).

---

[21] Согласно п. 2 ст. 391 ГК РФ перевод должником своего долга на другое лицо допускается с согласия кредитора и при отсутствии такого согласия является ничтожным (особенно если под передачей аккаунта третьему лица подразумевается передача договора по смыслу ст. 392.3 ГК РФ. Собрание законодательства РФ. 1994. № 32. Ст. 3301).

[22] Определение Московского городского суда от 16 ноября 2015 г. № 4г/6-11858/2015.

Вместе с тем, как отмечает А. И. Савельев, «даже если и признать, что право собственности на виртуальные объекты возможно, здесь возникает немало проблем, связанных с тем, что его реализация неразрывно связана с правом на доступ к программному продукту, в рамках которого оно существует. <...> Вопрос в том, как быть с виртуальными земельными участками, доступ к которым невозможен без согласия правообладателя программного продукта» (Savelyev, 2014, p. 142).

Впрочем, в настоящее время вопрос о возврате виртуального игрового имущества (например, при краже из инвентаря *Steam* предмета, если служба поддержки бездействует) законному владельцу гражданско-правовыми или уголовно-правовыми механизмами еще не решен.

Концепция интеллектуальной собственности как основы регулирования оборота виртуального имущества

Игровое имущество представляет собой программный код внутри самой программы-видеоигры и предстает перед пользователем в объективной форме (п. 3 ст. 1259 ГК РФ). Однако для признания за игроком авторских прав на игровой объект нужно установить наличие творческого элемента в конечном продукте. Это возможно только в случаях, прямо предусмотренных функционалом игры и правилами, которые напрямую интегрируются уже конкретными разработчиками игр, например создание пользовательского контента в мастерской *Steam*[23].

Таким образом, появляется разграничение игрока-автора и игрока-потребителя. Автор с помощью возможностей видеоигры и игрового сервиса разрабатывает игровой контент, на который в последующем приобретает авторские права (исключительные же — передаются сервису). Рядовой игрок в облике аватара в самой игре может создать нечто приближенное, но а) по правилам виртуального пространства это неотчуждаемая от самого аватара «материя»; б) оно не создано в строгих рамках платформы. Примером может служить упомянутая мастерская *Steam,* где разработчики выбирают те игровые атрибуты, которые потом добавят в видеоигру с возможностью покупки копий разработанного продукта на торговой площадке всеми рядовыми игроками за денежные средства реального мира.

Рассмотрим следующий вариант правового регулирования оборота игрового имущества в рамках права интеллектуальной собственности. Пользователь вносит лицензионный платеж и приобретает по лицензионному договору право использования игрового атрибута. В таком случае дальнейшие операции по передаче игрового атрибута или аккаунта третьему лицу будет квалифицироваться как сублицензионный договор, границы разрешенного использования по которому устанавливаются в лицензионном соглашении, например прямой запрет на продажу игровых атрибутов и передачу аккаунтов в положениях *EULA*, или в соответствии с п. 2 ст. 1238 ГК РФ (Perepyolkina, 2020, p. 51).

Данный подход представляется наиболее релевантным для правового обоснования механизма оборота виртуального игрового имущества не только потому, что он уже применяется, но и по результатам его использования. Так, по мнению Е. Ю. Мартьяновой, помимо прочего, благоприятными последствиями являются опосредование отношений по отчуждению, использованию игрового предмета лицензионным договором, необходимость получения

[23] «Когда вы загружаете контент в *Steam*, делая его доступным для других пользователей и/или *Valve*, вы передаете компании *Valve* и ее аффилированным компаниям международное, неэксклюзивное право на использование, воспроизведение... лицензия предоставляется компании *Valve* при загрузке контента в сервис *Steam* на всё время действия прав на интеллектуальную собственность» (*Соглашение подписчика Steam*, Steam, https://store.steampowered.com/subscriber_agreement/?l=russian (дата обращения 14 марта 2024).

пользователем согласия правообладателя на заключение сублицензионного договора с другими пользователями, неприменимость к договорам, заключаемым между пользователем и правообладателем, Закона РФ от 7 февраля 1992 г. № 2300-I «О защите прав потребителей»[24], особенности в определении применимых норм налогового, таможенного, страхового законодательства (Martyanova, 2020, p. 175).

Оборот виртуального имущества через договор возмездного оказания услуг

Представленная концепция констатирует правовую квалификацию пользовательских соглашений как договоров со смешанным характером, т. е. договоров услуг в части предоставления возможности покупки внутриигровых привилегий и предметов. Однако возникают сомнения, связанных с природой договора возмездного оказания услуг между самими пользователями и разработчиками в рамках оборота игрового имущества.

Проанализируем вышеупомянутое лицензионное соглашение с конечным пользователем для *EMEA Blizzard*[25]. Согласно п. 11 § 2 соглашение регулируется законодательством Франции и толкуется в соответствии с ним. Присущее римскому праву троякое представление о договоре найма нашло прямое отражение во Французском гражданском кодексе. Соответственно, в его титул VIII «О договоре найма» включены, в частности, самостоятельные главы: «О найме вещей» и «О найме работы и услуг». Первую главу титула составляют «Общие положения». На дальнейших ступенях дифференциации в главе «О найме работы и услуг» выделен договор подряда, предметом которого служит возмездное исполнение работы. При этом по ст. 1787 Французского гражданского кодекса[26] договором может быть установлена обязанность подрядчика «предоставить лишь свою работу или свои специальные знания, или что он предоставит также и материал» (Braginsky & Vitryansky, 2011, p. 23).

Таким образом, речь идет о разграничении договора найма, предметом которого выступают труд и его результат, и договора на оказание услуг, имевшего своим предметом труд как таковой, лишенный отделенного от него результата.

Поэтому, когда пользователь покупает внутриигровую валюту, он заключает договор об оказании платных услуг[27], хотя пользователь и получает предсказуемый и гарантированный результат — валюту или единицу брони в инвентарь; пусть и не материальный объект, но пользователем приобретается нечто представленное в объективной цифровой форме. Указанный механизм передачи можно считать предметом договора возмездного оказания услуг по ст. 779 ГК РФ[28] лишь с рядом оговорок и условностей.

Обращение виртуального имущества как цифрового права

Согласно п. 1 ст. 141.1 ГК РФ[29] цифровыми являются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определя-

[24] Закон Российской Федерации «О защите прав потребителей» от 07.02.1992 № 2300-I. Российская газета. 7 апреля 1992 г.

[25] *End User License Agreement,* https://www.blizzard.com/en-us/legal/fba4d00f-c7e4-4883-b8b9-1b4500a402ea/blizzard-end-user-license-agreement (Mar. 11, 2025).

[26] Code civil [C. civ.] [ФГК] art. 1787.

[27] Определение Верховного Суда РФ от 30 сентября 2015 г. № 305-КГ15-12154.

[28] Гражданский кодекс Российской Федерации (часть вторая) от 26 января 1996 № 14-ФЗ. Российская газета. 10 февраля 1996 г.

[29] Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ. Собрание законодательства РФ. 1994. № 32. Ст. 3301.

ются в соответствии с правилами информационной системы, отвечающей установленным законом признакам. Согласно мнению М. А. Рожковой, цифровым субъективное гражданское право признается вследствие того, что оно подтверждено в информационной системе в виде кода или обозначения. То есть речь идет об электронной форме (способе оформления) существующих субъективных гражданских прав (Rozhkova, 2021, p. 46). В другом научном труде М. А. Рожкова приходит к логичному умозаключению о вероятном развитии обращения виртуального имущества как цифрового права: «...не справившись с задачей раскрытия содержания цифровых прав и выявления квалифицирующих признаков, позволяющих отграничить этот объект от иных объектов гражданских прав, законодатель решил, что будет попросту называть такие права в отдельных законах, создавая соответствующее их назначению правовое регулирование» (Rozhkova, 2021, p. 47).

В долгосрочной перспективе законодателем в отдельном федеральном законе могут быть созданы, помимо определения виртуального игрового имущества, механизмы правовой охраны и защиты такового.

Возможно было бы закончить на этом: снять с себя тяжелую ношу правовой определенности и больше не тащить глыбу концепций в гору, однако в проблематике соотнесения цифровых прав и виртуального игрового имущества есть, по нашему мнению, неразрешимое препятствие.

Как было отмечено С. В. Сарбашем, у цифрового права нет и не может быть никакой самостоятельности. Это ложная сущность в ряду субъективных гражданских прав. Цифровое право на самом деле есть лишь форма, т.е. оформление любого известного права: вещного, обязательственного, корпоративного, исключительного, личного (Novoselova et al., 2019, p. 35). Представленная позиция отражает ситуацию полого объекта, природа которого остается непонятной — форма без содержания.

Можно прийти к выводу, что применение концепции цифровых прав к предмету рассуждений на данный момент весьма туманно в связи с не до конца разработанным механизмом регулирования. Можно ли считать игровое имущество указанным в законе цифровым правом? Какие границы у правил информационной системы? Для подтверждения цифрового права в информационной системе достаточно зарегистрировать его в видеоигре или в отдельном игровом реестре, который только обременит оборот?[30]

Концепция самостоятельного объекта гражданских прав

Согласно ст. 128 ГК РФ к объектам гражданских прав относятся вещи (включая наличные деньги и документарные ценные бумаги), **иное имущество**, в том числе имущественные права (включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права); результаты работ и оказание услуг; охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага[31].

[30] Подробнее об этом: Совет при Президенте Российской Федерации по кодификации и совершенствованию гражданского законодательства, Экспертное заключение «О внесении изменений в части первую, вторую и третью Гражданского кодекса Российской Федерации» (о цифровых правах) от 17 января 2019 г. № 183-1/2019 по проекту федерального закона № 424632-7, https://old.privlaw.ru/wp-content/uploads/2019/12/%D0%A1%D0%B1%D0%BE%D1%80%D0%BD%D0%B8%D0%BA-2019-%D1%8D%D0%BA%D1%81%D0%BF%D0%B5%D1%80%D1%82%D0%BD%D1%8B%D0%B5-%D0%B7%D0%B0%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%BD%D0%B8%D1%8F.pdf

[31] Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ. Собрание законодательства РФ. 1994. № 32. Ст. 3301.

По мнению А. И. Савельева, отнесение виртуального игрового имущества к иному с дальнейшим закреплением в ст. 128 ГК РФ в большей мере отвечает потребностям оборота и обеспечивает защиту законных интересов пользователя в отношении игрового имущества, которое с очевидностью имеет определенную экономическую ценность и фактически участвуют в гражданском обороте (Savelyev, 2014, p. 147). Также это приведет к признанию игрового имущества объектом гражданских прав с соответствующими правовыми последствиями и к опосредованию оборота данных объектов заключением непоименованных договоров (Martyanova, 2020, p. 181).

Данную концепцию можно будет считать совершенно приемлемой при должной имплементации уже существующих правовых норм, но модернизированных под цифровую природу игрового имущества, в отдельную главу ГК РФ, где учтутся особые способы защиты и правовой охраны. Так, при недействительности сделки, совершенной под влиянием существенного заблуждения или обмана, насилия, угрозы или неблагоприятных обстоятельств между двумя контрагентами-игроками, суду нужно будет оценить все доказательства сторон, например скриншоты переписок или согласованность предмета сделки, подразумеваемость воли к исполнению условий сделки и т. д. При выявлении порочности сделки по требованию стороны признать оспоримую сделку недействительной и применить последствия ее недействительности по ст. 12 ГК РФ, если существует объективная возможность вернуть виртуальное игровое имущество. Например, суд обязывает ответчика или Steam восстановить цепочку транзакций индивидуально-определенного игрового артефакта (так называемый паттерн или структура скинов, отражающаяся в уникальном номере).

Представленная схема возможна лишь при следующих условиях: 1) решение суда будет обязательным для сотрудников *Valve,* которые имеют вышеуказанные полномочия; 2) единица игрового имущества не находится у добросовестного приобретателя; 3) не нарушались ли истцом и ответчиком правила видеоигры (при установлении разумно обусловленного запрета передачи аккаунтов или виртуального игрового имущества между игроками).

***

По итогу представленных выше рассуждений возможно вывести авторское ви́дение значения термина *«виртуальное игровое имущество»:* объект цифрового пространства, имеющий имущественное воплощение в определенных субъектами правоотношений рамках и над которым можно установить право владения, пользования и распоряжения в той мере, в какой их оборот допускается законом и игровыми механиками[32].

Ограничение свободы договора в целях защиты игроков через призму отечественной и зарубежной практики

Как зарубежные, так отечественные исследователи выделяют ключевые содержательные и процедурные проявления свободы договора (Karapetov & Savelyev, 2012, p. 38).

[32] В свою очередь, «игровые механики — это процедурные алгоритмы видеоигры, описывающие цель видеоигры и позволяющие сбалансировать другие конститутивные элементы игрового процесса, реализуемые в программном обеспечении» (Pagov, 2025, p. 157).

ГК РФ раскрывает принцип свободы договора в ст. 421[33], а Французский гражданский кодекс — в ст. 1102[34]. При этом смысловое наполнение принципа практически идентично, если подвергать соответствующие нормы систематическому и доктринальному толкованию:

a) заключать договор по собственной воле в любое время и на любых условиях, которые они считают нужными (свобода договора);
b) свободно обсуждать и вести переговоры об условиях, последствиях и прекращении своих обязательств с другой договаривающейся стороной (свобода обсуждения);
c) изменять последствия обязательства и прекращать его по соглашению с другой договаривающейся стороной, причем суд в принципе не может вмешаться по праву (свобода прекращения);
d) выбирать форму своего обязательства, за исключением случаев, когда этого требует закон (свобода формы выражения) (Lefebvre, 2003, p. 443).

Руководствуясь буквальным пониманием принципа свободы договора, издатели или разработчики составляют пользовательские соглашения с особой юридической техникой в части регулирования виртуального имущества. В таких соглашениях любая система виртуальных предметов имеет в своей основе ограниченную лицензию на доступ игрока к функциям игры, а не фактический обмен товарами, причем лицензия ограничивается указанием на разрешенные способы использования с рядом оговорок.

Кроме того, в любых условиях предоставления услуг и/или лицензионных соглашениях с конечным пользователем указывается, что лицензия на виртуальное имущество может быть прекращена в любое время по выбору издателя, а поскольку в целях баланса и нововведений иногда необходимо изменять игровые предметы, издатель уполномочен предпринимать любые действия, в том числе те, которые могут привести к снижению или устранению ценности любого предмета, персонажа или учетной записи (Boyd et al., 2019, p. 173).

Впрочем, автономия сторон договорных отношений по своей природе ограничена императивными положениями позитивного права. Такие ограничения обусловлены объективным характером правоотношений, возникающих из договора, и дополнительно обоснованы соображениями публичного интереса, субъективными правами и законными интересами третьих лиц, необходимостью защиты экономически или социально более слабой стороны.

Одной из сфер, в которой разумное ограничение свободы договора является нерушимым постулатом, считаются потребительские отношения. Потребитель, а в нашем случае игрок, презюмируется слабой стороной в правоотношениях с платформой *Steam* или издателем видеоигр (если иметь в виду непосредственное взаимодействие через платформу такого издателя).

[33] Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ. Собрание законодательства РФ. 1994. № 32. Ст. 3301.

[34] Анализ французского гражданского законодательства в сфере защиты прав потребителей актуален в связи с относительно недавним судебным решением против *Valve*, защищающим законные интересы игроков, что является подтверждением пристального внимания к правоотношениям в потребительской сфере (Code civil [C. civ.] [ФГК] art. 1102). Парижский суд вынес постановление, обязывающее компанию Valve предоставить пользователям платформы Steam возможность перепродажи приобретённых игр и вывода средств из онлайн-кошелька. В связи с этим решением, если судить по геймплею, в версии игры *CS:GO (CS2)* для французского региона был добавлен новый функциональный элемент — виртуальное игровое имущество P250 X-Ray, позволяющее игрокам просматривать содержимое лутбоксов до их открытия, но после покупки электронного ключа от лутбокса. При этом были введены ограничения на торговлю самими лутбоксами на Торговой площадке Steam. (См. Tribunal de Grande Instance [TGI] [Суд общей юрисдикции] Paris, 1/4 Soc., 17 сентября 2019, RG 16/01008, Portalis 352J-W-B7A-CHASA (Fr.) https://cdn2.nextinpact.com/medias/16-01008-ufc-que-choisir-c--valve.pdf)

Так, информационный дисбаланс и ограниченные возможности игрока как потребителя вести переговоры или вносить правки с профессиональным участником игровой индустрии ставят под сомнение равенство сторон при анализе правоотношений, вытекающих из договора присоединения — *пользовательского соглашения.*

Положения договора могут быть признаны недействительными не только в случае прямого противоречия действующему законодательству, но и в тех ситуациях, когда соответствующие условия нарушают права потребителя в более широком смысле, в частности, если они приводят к ухудшению его правового положения по сравнению с минимальными стандартами, закрепленными законом. При этом законодатель не устанавливает исчерпывающий перечень положений, которые могут быть квалифицированы как ущемляющие права потребителей, поэтому обычно исходят из пункта 2 ст. 6 ГК РФ[35], в соответствии с которым содержание гражданско-правовых обязанностей и прав определяется на основе общих принципов и смысла гражданского законодательства, а также требований добросовестности, разумности и справедливости (Shirvindt, 2014, p. 47). В частности, согласно ст. 16 Закона «О защите прав потребителей»[36] недопустимыми условиями договора, ущемляющими права потребителя, являются те, которые нарушают правила, установленные международными договорами Российской Федерации, Законом «О защите прав потребителя», законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, регулирующими отношения в области защиты прав потребителей. *Недопустимые условия договора, ущемляющие права потребителя, ничтожны.*

Во Франции, в свою очередь, Кодекс прав потребителей запрещает злоупотребление неосведомленностью слабой стороны, что включает в себя использование предпринимателем уязвимости или неосведомленности человека с целью склонить его или ее к заключению договора на выгодных условиях[37].

Таким образом, соглашения с игроками с явно ущемляющими условиями вроде потестативного права разработчика в одностороннем порядке прекратить функциональную поддержку серверов видеоигры, что приведет к потере всех вложенных денежных средств и нивелированию усилий, потраченных на приобретение виртуального игрового имущества, формально можно на данном этапе развития законодательства признать недействительными. Выраженное согласие чаще всего либо не является свободным и осознанным, либо подается так, чтобы информация об объеме договорных обязательств была сформирована в виде непонятных оговорок. Следовательно, договор может быть признан недействительным, независимо от того, является ли соглашение договором присоединения или договором «по взаимному согласию», на основании ст. 10 ГК РФ или вследствие ничтожности таких условий по ст. 169 ГК РФ[38].

Заключение

Нынешняя ситуация, когда регулирование отношений между пользователями и операторами виртуальных пространств отдается на откуп различным соглашениям с конечным пользователем, имеет ряд негативных последствий, описанных в работе. Однако многие правопорядки

[35] Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ. Собрание законодательства РФ. 1994. № 32. Ст. 3301.

[36] Закон Российской Федерации «О защите прав потребителей» от 07.02.1992 № 2300-I. Российская газета. 7.4.1992 г.

[37] Code de la consommation [C. cons.] [Кодекс прав потребителей] art. L. 121-8–L. 121-10.

[38] Постановление Пленума ВАС РФ «О свободе договора и ее пределах» от 14.03.2014 г. № 16.

просто игнорируют то, что у игроков могут не возникать права на только что приобретенные виртуальные предметы, т. е. они получают цифровое владение, но не имеют права на них (Palka, 2017, p. 47).

Рассмотрев суть виртуального игрового пространства как вида виртуального пространства и подробно разграничив понятия «имущество» и «собственность» в контексте виртуального мира, автор вывел характеристики и особенности виртуального игрового имущества, а также, проанализировав существующие концепции правого режима игрового имущества, предпринял попытку вывести ключевые дефиниции и авторскую теорию очерченного «магического круга», которая релевантна предмету данного исследования.

В работе был отражен плюрализм различных концепций, как наименее, так и наиболее применимых в качестве устойчивого правового регулирования оборота виртуального игрового имущества. Был сделан вывод о возможности использования института интеллектуальной собственности как основы регулирования оборота виртуального имущества (если присутствует творческий базис у игрового имущества), концепции самостоятельного объекта гражданских прав (если создать/интерпретировать существующую правовую основу и развить терпимость правоприменителей к спорам, возникающим из правоотношений в виртуальных игровых пространствах). Как и многие исследователи виртуального игрового имущества, автор видит невозможность положительной эмерджентности имущественных прав без имплементации концепций виртуального имущества.

Кроме того, показано, что эффективным инструментом по защите прав и законных интересов может быть законодательство в сфере защиты прав потребителей, так как потребители охраняются от введения в заблуждение или злоупотребления в той или иной форме. Поэтому включение проработанных условий предоставления услуг или лицензионного соглашения с конечным пользователем, которые охватывают приобретение, владение, использование виртуального имущества, не поможет издателю избежать рисков, если не будут соблюдены базовые условия получения явно выраженного волеизъявления сторон.

Список литературы / References

1. Arkhipov, V. V. (2019a). Komp'yuternyye igry, «magicheskiy krug» i smyslovyye predely prava [Computer games, "magic circle" and semantic limits of law]. *International Journal of Cultural Research*, (1), 73–87.
2. Arkhipov, V. V. (2019b). *Semanticheskiye predely prava v usloviyakh medial'nogo povorota: Teoretiko-pravovaya interpretatsiya* [Semantic limits of law in the context of the medial turn: A theoretical and legal interpretation] [Doctoral dissertation, St. Petersburg State University]. http://hdl.handle.net/11701/16362
3. Bentham, J. (1998). *Vvedeniye v osnovaniya nravstvennosti i zakonodatel'stva* [An introduction to the principles of morals and legislation] (trans. by B. G. Kapustin). ROSSPEN.
4. Boyd, S. G., Pyne, B., & Kane, S. F. (2018). *Video game law: Everything you need to know about legal and business issues in the game industry*. A K Peters/CRC Press. https://doi.org/10.1201/9780429469992
5. Braginsky, M. I., & Vitryansky, V. V. (2011). *Dogovornoye pravo. Kniga tret'ya: Dogovory o vypolnenii rabot i okazanii uslug* [Contract law. Book three: Contracts for work and services]. Statut.
6. Castronova, E. (2004). The right to play. *New York Law School Law Review, 49*(1), 185–210.
7. Doiev, A. M. (2023). O prirode virtual'nykh "veshchey" kak ob'yektov veshchnykh prav [On the concepts of virtual "things" and "thing-ness"]. *Digital Law Journal*, *4*(3), 8–15. https://doi.org/10.38044/2686-9136-2023-4-3-8-15
8. Fairfield, J. (2005). Virtual property. *Boston University Law Review*, *85*, 1047–1102.

9. Fairfield, J. (2009). The magic circle. *Vanderbilt Journal of Entertainment and Technology Law*, *11*(4), 823–840.
10. Graf, D. V. (2024). Balans interesov pol'zovateley, izdateley i razrabotchikov pri zakrytii videoigr v svete novoy yevropeyskoy initsiativy [Balancing the interests of users, publishers and developers in cases of shutdown of video games: A new European initiative]. *Digital Law Journal*, *5*(2), 24–39. https://doi.org/10.38044/2686-9136-2024-5-2-24-39
11. Hegel, G. W. F. (2021). *Filosofiya prava* [Philosophy of law] (trans. by B.G. Stolpner). Yurait.
12. Huizinga, J. (1997). *Homo ludens; Stat'i po istorii kul'tury* [Homo ludens: Articles on the history of culture] (trans. & ed. by D.V. Silvestrov). Progress-Traditsiya.
13. Karapetov, A. G., & Savelyev, A. I. (2012). *Svoboda dogovora i yeye predely* [Freedom of contract and its limits] (Vol. 1). Statut.
14. Kazakova, N. Yu. (2017). *Geym-dizayn (Khudozhestvenno-proyektnyy podkhod k sozdaniyu tsifrovoy igrovoy sredy)* [Game design (Artistic and project-based approach to creating a digital game environment)] (Doctoral dissertation abstract, Kosygin Russian State University).
15. Klevjer, R. (2022). *What is the avatar?: Fiction and embodiment in avatar-based singleplayer computer games.* (Revised and commented ed.). Transcript. https://doi.org/10.1515/9783839445792
16. Lastowka, F. G., & Hunter, D. (2004). The laws of the virtual worlds. *California Law Review*, *92*(1), 1–73. https://doi.org/10.2307/3481444
17. Lefebvre, B. (2003). Le contrat d'adhésion [The contract of adhesion]. *Revue du notariat, 105*(2), 439–490.
18. Locke, J. (2021). *The second treatise of government. Vtoroy traktat o pravlenii* [Second treatise of government] (Bilingual ed.). Yurait.
19. Mill, J. S. (1900). *Utilitarianizm. O svobode* [Utilitarianism. On liberty] (trans. by A. N. Nevedomsky, 3rd ed.). I. P. Perevoznikov.
20. Novoselova, L., Gabov, A., Savelyev, A., Genkin, A., Sarbash, S., Asoskov, A., Semenov, A., Yankovsky, R., Zhuravlev, A., Tolkachev, A., Kamelkova, A., Uspensky, M., Krupenin, R., Kisly, V., Zhuzhzhalov, M., Popov, V., & Agranovskaya, M. (2019). Tsifrovyye prava kak novyy ob"yekt grazhdanskogo prava [Digital rights as a new object of civil law]. *Zakon,* (5), 31–54.
21. Pagov, A. Zh. (2025). Videigry i igrovye mekhaniki: pravovoy rezhim i okhrana [Video games and game mechanics: Legal regime and protection]. *Pravovaya Informatika, 1*, 153–162. https://doi.org/10.24412/1994-1404-2025-1-153-162
22. Palka, P. (2017). *Virtual property: Towards a general theory* [Doctoral dissertation, European University Institute]. https://doi.org/10.2870/700083
23. Perepyolkina, Ya. A. (2020). Virtual'noye igrovoye imushchestvo: Perspektivy pravovogo regulirovaniya [Virtual game property: Prospects for legal regulation]. *Zhurnal Suda po Intellektual'nym Pravam*, (3), 45–59.
24. Rozhkova, M. A. (2021). Kategorii "tsifrovoye pravo", "tsifrovyye prava" i "tsifrovaya valyuta" v rossiyskom prave [The categories of "digital law", "digital rights", and "digital currency" in Russian law]. In: M. A. Rozhkova (Ed.), *Pravo cifrovoj ekonomiki—2021: Ezhegodnik-antologiya* [Law of the digital economy—2021: A yearbook-anthology] (pp. 10–68). Statut.
25. Rybalov, A. O. (2007). *Problemy klassifikatsii grazhdanskikh pravootnosheniy* [Problems of classification of civil legal relations] [PhD Thesis, St. Petersburg State University].
26. Rybalov, A. O. (2017). Pravo sobstvennosti (kommentariy k st. 209 GK RF) [Property law (commentary on Art. 209 of the Civil Code of the Russian Federation)]. M-Logos.
27. Savelyev, A. I. (2014). Pravovaya priroda virtual'nykh ob"yektov, priobretayemykh za real'nyye den'gi v mnigopol'zovatel'skikh igrakh [The legal nature of virtual objects purchased for real money in multiplayer games]. *Vestnik Grazhdanskogo Prava,* (1), 127–150.
28. Sklovsky, K. I. (2023). *Sobstvennost' v grazhdanskom prave* [Property in civil law] (6th ed.). Statut.

29. Shevtsov, K. P. (2018). Komp'yuternye igry kak predmet filosofskogo analiza [Computer games as a subject of philosophical analysis]. *Vestnik Sankt-Peterburgskogo Universiteta. Filosofiya i Konfliktologiya,* (1), 98–103.
30. Shirvindt, A. M. (2014). *Ogranicheniye svobody dogovora v tselyakh zashchity prav potrebiteley v rossiyskom i yevropeyskom chastnom prave* [Limitation of freedom of contract for consumer protection in Russian and European private law] (ed. by A.L. Makovsky). Statut.
31. Stepanov, S. A. (ed.). (2016). *Grazhdanskoye pravo: Uchebnik* [Civil law: Textbook] (Vol. 1, 2nd ed.). Prospekt.
32. Tebenkova, V. N. (2024). Mezhdunarodno-pravovyye printsipy ustanovleniya yurisdiktsii gosudarstv v kiberprostranstve [International legal principles of establishing state jurisdiction in cyberspace]. *Actual Problems of Russian Law*, (5), 177–191.
33. Martyanova, E. Yu. (2020). Dogovory, oposreduyushchie ispol'zovaniye ob'yektov onlayn-igr [Contracts mediating the use of online game objects]. In: M. A. Rozhkova (Ed.), *Pravo Cifrovoj ekonomiki—2020: Ezhegodnik-antologiya* [Law of the digital economy—2020: A yearbook-anthology] (pp. 164–184). Statut.

Сведения об авторе:

Пагов А. Ж. — магистр юриспруденции, аспирант, кафедра теории и истории государства и права, юридический факультет, Санкт-Петербургский государственный университет, Санкт-Петербург, Россия.
apagov.legal@gmail.com
ORCID: https://orcid.org/0009-0005-7290-7968

Information about the author:

Astemir Zh. Pagov — LL.M., Ph.D. student, Department of Legal Theory and History, Law Faculty, St. Petersburg State University, St. Petersburg, Russia.
apagov.legal@gmail.com
ORCID: https://orcid.org/0009-0005-7290-7968

https://doi.org/10.38044/2686-9136-2025-6-7

ОБЗОРНЫЕ СТАТЬИ

КОНЦЕПТ СВОБОДНОГО ПЕРЕХОДА ЦИФРОВОГО ПРАВА В РАКУРСЕ УЧЕТА ВОЛИ ОБЯЗАННОГО ЛИЦА

Ю. С. Поваров

Самарский национальный исследовательский университет
имени академика С. П. Королева
443086, Россия, Самара, Московское шоссе, 34

Аннотация

Базовым постулатом гражданского оборота цифровых прав выступает правило, в силу которого их переход на основании сделки не подлежит согласованию с обязанным лицом (п. 3 ст. 141.1 ГК РФ). Однако толкование данного законоположения вызывает определенные затруднения в доктрине и на практике. Сверх того, критике порою подвергается и сама идея универсальности концепта свободной (в контексте индифферентности мнения должника или иного обязанного лица) циркуляции цифровых прав. Основной целью исследования является установление юридического значения указанного концепта, прежде всего в ракурсе (не)целесообразности придания ему безусловного характера. Для этого автор, применяя общенаучные (формально-логический и диалектический) и частнонаучные (юридико-догматический, сравнительно-правовой, метод толкования правовых норм) методы, проводит комплексный анализ п. 3 ст. 141.1 ГК РФ (в сопряжении с иными законодательными предписаниями касательно перехода имущественных прав и функционирования информационных систем), а также изучает правила информационных систем, разработанные отдельными операторами. При этом в статье раскрываются общий смысл и ограничения сферы действия нормы п. 3 ст. 141.1 ГК РФ, обсуждается проблема (не)обоснованности ее квалификации как императивной. Автор указывает на ущербность дифференциации режимов перехода цифровых прав (в аспекте учета мнения обязанного лица), исходя из юридико-фактической основы (сделка или наступление предусмотренных законом обстоятельств). Подчеркивается, что исследуемая норма не блокирует необходимость получения согласия других, нежели обязанное по цифровому праву лицо, субъектов. Доказывается отсутствие бесспорных факторов для квалификации правила п. 3 ст. 141.1 ГК РФ как императивного (поскольку, в частности, возможность осуществления и распоряжения цифровыми правами сугубо в информационной системе без обращения к третьему лицу не детерминирует недопустимость введения разрешительного порядка). В работе признается наличие политико-правовых оснований для отказа от восприятия концепта свободного трансферта цифровых прав как безусловного. Соответственно, заявляется о принципиальной приемлемости децентрализованного регулирования вопросов согласования совершения сделки с обязанным лицом; при этом обосновывается вторичный характер локальной регламентации обращения цифровых прав в правилах информационной системы (ибо в конечном счете речь должна идти об определении его условий участниками договора).

Ключевые слова

обращение цифровых прав, переход цифрового права, обязанное лицо, должник, согласие на совершение сделки, императивная норма, диспозитивная норма, правила информационной системы, децентрализованное регулирование

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.
Для цитирования	Поваров, Ю. С. (2025). Концепт свободного перехода цифрового права в ракурсе учета воли обязанного лица. *Цифровое право, 6*(2), 112–126. https://doi.org/10.38044/2686-9136-2025-6-7

Поступила: 10.05.2025, принята в печать: 31.05.2025, опубликована: 30.06.2025

REVIEW ARTICLES

THE CONCEPT OF FREE TRANSFER OF DIGITAL RIGHTS FROM THE PERSPECTIVE OF THE OBLIGOR'S WILL

Iurii S. Povarov

Samara National Research University
34, Moskovskoe Highway, Samara, Russia, 443086

Abstract

A basic postulate of the civil transfer and exchange of digital assets consists in the rule according to which their transfer on the basis of a transaction is not subject to agreement with the obligated party (Article 141.1(3) of the Civil Code of the Russian Federation). However, the interpretation of this legal provision gives rise to certain difficulties in both doctrine and practice. Moreover, the very idea of the universalism of the concept of free (in the context of the indifference of the opinion of the debtor or other obligated party) circulation of digital rights can be subject to criticism. The present study sets out to establish the legal significance of this concept in primary terms of the (in)expediency of giving it an unconditional character. For this purpose, a comprehensive analysis of the content of the norm of Article 141.1(3) of the Civil Code of the Russian Federation (in conjunction with other legislative provisions regarding the transfer of property rights and the functioning of information systems) is carried out on the basis of general scientific (formal and dialectical logic) and specific scientific (legal-dogmatic, comparative legal, interpretation of legal norms) methods along with the rules of information systems developed by individual operators. The presented analysis of the general meaning and limitations of the scope of the norm of Article 141.1(3) of the Civil Code of the Russian Federation reveals the critical problem of the (un) reasonableness of its qualification. The inadequacy of the differentiation of the modes of transfer of digital rights (in terms of taking into account the opinion of the obligated person) based on the legal and factual basis (transaction or occurrence of circumstances provided for by law) consists in the impossibility of demonstrating

that the norm under study cannot abrogate the need to obtain the consent of subjects other than the person obligated under the digital right. The absence of indisputable factors for qualifying the rule as imperative is demonstrated in terms of the exercise and disposal of digital rights solely in the information system without recourse to a third party and not determining the inadmissibility of introducing a permit-based procedure. Since the existence of political and legal grounds for refusing to perceive the concept of free transfer of digital rights as unconditional must be acknowledged, the fundamental acceptability of decentralized regulation of issues of coordinating the conclusion of a transaction with an obligated party is confirmed. The secondary nature of local regulation of the conditions for the circulation of digital rights in the rules of the information system is substantiated in terms of necessity for such conditions to be determined by the parties to the agreement).

Keywords

circulation of digital rights, transfer of digital rights, obligated party, debtor, consent to transaction, imperative norm, dispositive norm, rules of an information system, decentralized regulation

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Povarov, I. S. (2025). The concept of free transfer of digital rights from the perspective of the obligor's will. *Digital Law Journal, 6*(2), 112–126. https://doi.org/10.38044/2686-9136-2025-6-7

Submitted: 10 May 2025, accepted: 31 May 2025, published: 30 June 2025

Введение

Корневая особенность обращения цифровых прав, получившая прямое отражение в п. 3 ст. 141.1 ГК РФ[1] при установлении рамочного юридического режима названных неординарных объектов, состоит в том, что переход цифрового права на основании сделки не требует согласия обязанного лица. Специальное законодательство, посвященное отдельным цифровым правам (Федеральный закон «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» от 2 августа 2019 г. № 259-ФЗ[2] (далее — Закон об инвестплатформах) и Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31 июля 2020 г. № 259-ФЗ[3] (далее — Закон о ЦФА)), материально-правовой составляющей оборота цифровых прав почти не касается, оставляя за скобками, среди прочего, рассматриваемый в настоящей работе узкий аспект.

Между тем толкование п. 3 ст. 141.1 ГК РФ (в том числе в срезе границ его применения предметного и субъектного толка, а равно оценки данной нормы, притом что она не содержит запрета на какую-либо корректировку, в качестве императивной или, напротив, диспозитивной) вызывает определенные интерпретационные сложности; под сомнение порою ставится и практическая целесообразность непоколебимости концепта свободной циркуляции цифровых прав.

[1] Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ. Собрание законодательства РФ. 1994. № 32. Ст. 3301.

[2] Собрание законодательства РФ. 2019. № 31. Ст. 4418.

[3] Собрание законодательства РФ. 2020. № 31 (ч. I). Ст. 5018.

Сфера действия п. 3 ст. 141.1 ГК РФ: общие замечания

Область приложения исследуемого концепта довольно обширна: в частности, п. 3 ст. 141.1 ГК РФ подлежит применению **безотносительно к природе оцифрованных прав** (обязательственная либо иная). Тем не менее она не является безграничной, причем ее сужение производится законодателем через фиксацию следующих ключевых положений.

Во-первых, речь идет о **смене обладателя** цифрового права **на основании сделки**. Конечно, данному постулату тоже присуща масштабность, так как ***набор*** соответствующих ***сделок никоим образом не ограничивается*** (они могут быть возмездными и безвозмездными, иметь различную каузу и т. п.).

Отметим, что квалификация некоторых актов как сделок, влекущих именно *переход* права (для целей применения п. 3 ст. 141.1 ГК РФ), к сожалению, является неоднозначной. Это, например, относится к договору залога, заключение которого само по себе, естественно, не вызывает указанного юридического эффекта; вместе с тем в силу п. 1 ст. 358.2 ГК РФ для залога права законом или соглашением между правообладателем и его должником может вводиться требование о согласовании с должником, тогда как для перехода цифрового права данная опция не проговаривается. Поэтому вовлечение залоговых сделок в сферу действия п. 3 ст. 141.1 ГК РФ становится возможным только при его расширительной трактовке (но лучшим способом преодоления туманности, разумеется, будет соответствующая корректировка законодательства; в любом случае ввиду рассогласованности регулирования схематика отчуждения и передачи в залог цифрового права выглядит неубедительно).

Кроме того, абсолютно очевидно, что переход цифрового права может происходить и ***по иным основаниям***, например в результате универсального правопреемства при наследовании по закону. При буквальном истолковании нормы в таких случаях ***необходимость согласования*** с обязанным лицом трансферта цифрового права априорно ***не исключается*** (и во внимание следует принимать специальные требования законодательства). Однако подобное дифференцированное регулирование, исходя из юридико-фактической основы перехода прав, причем с облегчением режима для случая совершения сделки (а не переноса права на другое лицо в силу закона при наступления предусмотренных им обстоятельств), кажется несколько странным.

Парадоксальность означенного дуализма подходов выглядит особенно рельефно при возможной квалификации наследования цифровых прав по завещанию либо наследственному договору как разновидности перехода объекта во исполнение *сделки* (правомерность совершения сделок *mortis causa* по поводу цифровых прав особых сомнений не вызывает (Zhanabilova, 2023, pp. 39–42)). Формальные резоны для подобной трактовки имеются (в частности, п. 3 ст. 141.1 ГК РФ изучаемый концепт распространяет на *переход* объекта, а не на сугубо его *передачу*), и при следовании ей преемство в цифровых правах может различаться в зависимости от основания наследования, что едва ли органично и рационально.

Во-вторых, субъектом, чье мнение индифферентно, объявляется **лицо, обязанное по цифровому праву**.

Сразу уместно оговориться, что ***законодатель отказался от использования термина «должник»***. Это, судя по всему, объясняется прежде всего тем, что цифровыми могут признаваться, помимо обязательственных, *иные* права (например, корпоративные); должником же принято именовать не всякое обязанное лицо, а участника именно обязательственно-правовой связи.

На этом фоне не вполне точными кажутся рассуждения О. А. Полежаева о том, что «по смыслу п. 3 ст. 141.1 ГК РФ для существования цифрового права необходимо существование *должника* [здесь и далее курсив в цитатах наш. — *Ю. П.*] и кредитора...» (что, в свою очередь, сигнализирует «об *обязательственно*-правовой природе цифрового права») (Polezhayev, 2023)[4], так как цифровые права, повторимся, не замыкаются на чисто обязательственные правомочия (и, соответственно, обязанное лицо не всегда может быть идентифицировано в качестве «должника» в традиционном понимании этого слова). В том числе по аналогичным мотивам не можем в полной мере поддержать и вывод Д. А. Нигматзяновой о том, что «российский правопорядок придал цифровым правам *обязательственный* характер, так как всегда должно существовать *обязанное лицо*» (Nigmatzyanova, 2024, p. 101); небезупречность этого заключения, помимо прочего, обусловливается тем, что обязанное лицо наличествует в любом правоотношении, а не только в обязательственном.

Необходимость запроса согласия иных, нежели обязанный по цифровому праву, ***субъектов п. 3 ст. 141.1 ГК РФ не отрицает*** (т. е. блокирование действия режимов согласования является избирательным, точечным). Поэтому, скажем, распоряжение цифровым правом, принадлежащим несовершеннолетнему гражданину в возрасте от 14 до 18 лет, может нуждаться в одобрении законных представителей (ст. 26 ГК РФ); не отвергается действие режима согласования совершения сделок другими участниками общей совместной собственности (ст. 253 ГК РФ) или залогодержателем (п. 2 ст. 346 ГК РФ), и т. д. В целом такой подход вполне обоснован: цифровизация инфраструктуры оборота прав не должна приводить к умалению фундаментальных условий совершения гражданско-правовых сделок.

Нет полной ясности по поводу (не)обоснованности рассмотрения в качестве обязанного по цифровому праву субъекта (для целей задействования изучаемого концепта) третьего лица, предоставившего обеспечение исполнения обязательств, удостоверенных цифровыми финансовыми активами (п. 10 ч. 1 ст. 3 Закона о ЦФА), например залогодателя, поручителя или гаранта[5]. В оптике охраны интересов обладателя цифрового права и достижения единообразия алгоритмов взаимодействия этого субъекта с иными акторами предпочтительна экстраполяция п. 3 ст. 141.1 ГК РФ и на указанных лиц (но сто́ит признать, что данный вывод из закона явным образом не следует).

Смысл и юридическое значение концепта свободного перехода цифровых прав

Итак, пункт 3 ст. 141.1 ГК РФ закрепляет принцип свободного (в плане необязательности учета мнения обязанного лица) совершения сделок, опосредующих переход цифровых прав. Это, разумеется, **усиливает оборотоспособность (ликвидность)** данных **объектов**, повышает их рыночную привлекательность.

Правда, распорядительные акты могут совершаться лишь в конкретной информационной системе (п. 1 ст. 141.1 ГК РФ), и такая «герметичность» нередко воспринимается как повод для оценки цифровых прав в качестве *ограниченно оборотоспособных* объектов. Из этой установки, например, исходит А. С. Мограбян: «...анализ ст. 141.1 ГК РФ, — констатирует

[4] Правда, отождествление обязанного лица и должника в контексте применения п. 3 ст. 141.1 ГК РФ довольно распространено (Zakirov & Shavaliyeva, 2021, p. 36).

[5] Этот вопрос актуален, поскольку, в частности, законодательство иногда устанавливает разрешительный порядок для перехода прав кредитора по обеспечительному обязательству, например, передача бенефициаром права требования к гаранту допускается по общему правилу лишь с согласия гаранта (см. п. 2 ст. 372 ГК РФ).

автор, — позволяет утверждать о законодательном ограничении в оборотоспособности цифровых прав» (Mograbyan, 2022, p. 144); с этим соглашаются Н. В. Перепёлкина и П. Е. Перепёлкин, подчеркивая (причем со ссылкой на ст. 129 ГК РФ), что императивы касаемо допустимости реализации цифровых прав и распоряжения ими «исключительно в пределах... технологической инфраструктуры» информационной системы позволяют отнести цифровые права к «объектам... с ограниченной оборотоспособностью...» (Perepyolkina & Perepyolkin, 2025, p. 117). Впрочем, приведенная интерпретация оправданна при сверхширокомпонимании ограниченной оборотоспособности объектов (а законодатель дает к тому основания: в п. 2 ст. 129 ГК РФ в ныне действующей редакции список возможных ограничений, не имеющих прямого отношения к рассматриваемой ситуации, является открытым). В любом случае важно, что рестриктивные указания п. 1 ст. 141.1 ГК РФ, имеющие преимущественно организационно-технический характер, сами по себе не ограничивают оборотоспособность цифровых прав в субъектном плане (т. е. в ракурсе принадлежности объекта только определенным участникам оборота) либо с точки зрения контроля за совершением сделок (когда легитимное совершение сделок с объектом может предполагать получение специального разрешения)[6].

Логично предположить, что сквозь призму анализируемого концепта (по крайней мере при его восприятии как безусловного и *императивного*):

а) **нейтрализуется действие** соответствующих **положений о согласовании совершения сделки** (при этом в ситуации, когда разрешительный порядок установлен *законом*, речь идет об отсутствии необходимости запроса согласия третьего лица на совершение сделки в смысле ст. 157.1 ГК РФ);

б) **блокируется возможность введения режима согласования** в порядке децентрализованной регламентации (прежде всего **договором**).

Тем самым обязанный субъект, по инициативе которого право «возникает непосредственно в цифровой среде, в привязке к электронному маркеру», как точно подмечает Л. А. Новоселова, «*заведомо соглашается* с тем, что право переходит по правилам информационной системы», не нуждаясь в его одобрительном волеизъявлении (Novoselova et al., 2019, p. 33).

В поле зрения законодателя, кстати, не попал момент (не)допустимости установления договорного *запрета* на вторичное обращение цифровых прав. Думается, что подход здесь должен быть в целом идентичным: уж если переход цифровых прав освобожден даже от санкционирования, ветирование трансферта тем более нелогично; кроме того, иное истолкование явно расходилось бы с общим посылом законодателя, стремящегося придать цифровым правам качество вполне оборотоспособного объекта[7].

Перенося данные умозаключения на циркулирующие в качестве цифровых **обязательственные права** (а таковыми являются все утилитарные цифровые права, ч. 1 ст. 8 Закона об инвестплатформах) и многие цифровые финансовые активы, в том числе оцифрованные денежные требования (ч. 2 ст. 1 Закона о ЦФА), позволительно утверждать о ***купировании*** прежде всего ***вытекающей из п. 2 ст. 382 ГК РФ возможности установления режима санкционирования должником перехода кредиторских прав законом*** (напомним, что ГК РФ закрепляет разрешительный порядок для уступки требования по обязательству, в котором личность кредитора

[6] Статья 129 ГК РФ в прежней редакции, как известно, рассматривала названные два критерия как *исчерпывающие* для квалификации объекта как ограниченно оборотоспособного.

[7] «В отношении цифровых прав, — небезосновательно пишет А. Б. Жанабилова, — законодатель... указывает на их оборотоспособность... как *конституирующий* признак...» (Zhanabilova, 2023, p. 41).

имеет существенное значение для должника (см. п. 2 ст. 388)[8], и права на получение неденежного исполнения в ситуации, когда цессия приводит к тому, что исполнение обязательства становится значительно более обременительным для должника (п. 4 ст. 388)), ***а равно договором*** (например, при уступке права на получение неденежного исполнения согласно п. 4 ст. 388 ГК РФ).

Между тем в науке присутствует мнение о сохранении силы правил о согласовании с должником перехода прав кредитора по причине их специального характера. Так, А. В. Концевой полагает, что «по отношению к нормам п. 2, 3, 4 ст. 382 ГК РФ норма п. 3 ст. 141.1 ГК РФ является *общей*, следовательно... отсутствие согласия должника при переходе цифровых прав по криптовалютному обязательству... порождает... последствия, предусмотренные в п. 3 и 4 ст. 382 ГК РФ» (Kontsevoy, 2020, p. 16).

Приведенная аргументация видится не до конца убедительной: *в приложении к предмету* сделки, вызывающей переход кредиторских прав, ***правило п. 3 ст. 141.1 ГК РФ***, наоборот, ***оправданно определить как специальное*** (ведь речь ведется о переходе не любых обязательственных прав, а исключительно цифровых). Помимо прочего, в условиях приуроченности конструкции цифровых прав в первую очередь к правам обязательственной природы устранение какого-либо влияния обсуждаемой нормы на применение стандартных предписаний о перемене лиц в обязательстве в значительной степени обесценивало бы ее значение. Другое дело, что пункт 3 ст. 141.1 ГК РФ регламентирует конкретный аспект механизма замены обладателя цифрового права (отсутствие необходимости в прохождении согласительной процедуры), а потому применение положений о перемене лиц в обязательстве, напрямую не касающихся обозначенного момента (в том числе п. 3 и 4 ст. 382 ГК РФ), отвергать сразу, конечно, нельзя.

Следовательно, стержневое «положение о перемене лиц в обязательстве, — в целом верно заявляют С. В. Одинцов и Э. Ю. Миронов, — при распоряжении цифровым правом устанавливается п. 3 ст. 141.1 ГК...» (Odintsov & Mironov, 2020)[9].

Крайне важно иметь в виду, что вывод о *приоритете* обсуждаемой нормы в сравнении с правилами о перемене лиц в обязательстве (их своеобразном вытеснении и поглощении) органичен при **отказе цифровым правам в статусе автономного объекта**, соседствующего с обязательственными и иными имущественными правами и сущностно однопорядкового им (так как при ином раскладе вопрос о (не)применении положений об обязательствах к обороту цифровых прав переводился бы в плоскость проблематики (не)обоснованности использования приема аналогии закона либо (не)целесообразности соответствующего отсылочного регулирования[10]). И законодатель, думается, дает весомые поводы для такой интерпретации: прежде всего она явно коррелирует с легальной дефиницией цифровых прав в п. 1 ст. 141.1 ГК РФ, из которой усматривается стремление «интегрировать [цифровые права. — *Ю. П.*]... в систему гражданских прав, не создавая... принципиально новой... категории, оторванной от... существующих» (Dakhayeva, 2025, p. 177). Показательна в данном контексте

[8] Но актуальность данного правила для цифровой среды невысока: выпуск права подобного рода в информационной системе маловероятен.

[9] Хотя, напомним, роль нормы этим не ограничивается, поскольку цифровые права могут быть не только обязательственными.

[10] Примечательна в этом измерении отсылка к нормам о переходе прав кредитора в п. 4 ст. 146 ГК РФ, посвященном передаче прав (в том числе обязательственных!) по именной *документарной* ценной бумаге; неизбыточность отсылки в немалой степени предопределяется тем, что документарная ценная бумага вообще считается *вещью*, а не имущественным правом.

и существенная трансформация законодательной трактовки бездокументарных ценных бумаг (конструкт которых, ставший, по точной ремарке А. В. Габова, «прообразом для создания цифрового права» (Novoselova et al., 2019, p. 34), очень близок к его модели[11]), состоявшаяся одновременно с внедрением в ГК РФ общих указаний о цифровых правах: бездокументарные ценные бумаги, определяемые, как и цифровые права, в качестве обязательственных и иных прав[12] (п. 1 ст. 142 ГК РФ), более не признаются объектами, отличными от имущественных прав. Теперь речь идет не об их размежевании внутри группы объектов, обнимаемых понятием «иное имущество», а о включении бездокументарных ценных бумаг наряду с цифровыми правами в круг имущественных прав, которые, в свою очередь, относятся к другому, нежели вещи, имуществу.

Сообразно сказанному «цифровая трансформация имущественных прав, — авторитетно указывает Л. Ю. Василевская, — не означает возникновения нового... права», нужно говорить «о цифровом *кодировании*... имущественных прав, об их цифровом способе *фиксации*» (Vasilevskaya, 2020, p. 114)[13]; при этом данная установка, думается, сама по себе не препятствует отнесению цифровых прав к объектам гражданских прав[14] (ведь имущественные права, в том числе в цифровой оболочке, таковыми являются, а обособление внутри них цифровых прав позволяет раскрыть специфику последних).

Другое дело, что оцифровка приводит к кардинальной модификации режимов соответствующих имущественных прав как объектов: их «*специфика*, — резонно подчеркивает Е. В. Вавилин, — заключается в цифровой форме... осуществления, но... *не ограничивается* исключительно *формой*» (Vavilin, 2024, p. 115); «...особенности осуществления цифровых прав, — справедливо констатирует А. А. Волос, — настолько необычны... что *вряд ли можно* их *характерные черты сводить только к вопросам фиксации*» (Volos, 2024b, p. 17) (т. е. цифровая форма существования права во многом детерминирует его содержательные параметры).

Но насколько обоснованно предложенное законодателем решение, особенно с учетом его универсальности, и адекватна ли оценка нормы п. 3 ст. 141.1 ГК РФ как императивной: что принципиально для (не)признания законным инициативно вводимого сценария оборота обязательственных прав в «цифровой обертке» с ведома должника?[15]

---

[11] Сходство явно обнаруживается, вследствие чего констатация названного обстоятельства общеупотребительна в литературе, см., напр.: Agibalova (2020, p. 92), Markina (2022, pp. 38–39).

[12] Речь, однако, не идет о любых имущественных правах: квалификация последних в качестве ценных бумаг, равно как и в качестве цифровых прав, производится исходя из *принципа легалитета*; нетождественным при этом оказывается круг источников, способных причислить права к указанным объектам (*только закон* — для цифровых прав (п. 1 ст. 141.1 ГК РФ), *закон или иной акт*, принятый в соответствии с законом, — для ценных бумаг (п. 2 ст. 142 ГК РФ)).

[13] Означенный подход снискал немалую поддержку в науке (Muratova & Druzhinin, 2023, pp. 31–37); впрочем, полемика на сей счет далека от завершения.

[14] «...цифровые объекты можно включать в перечень объектов гражданских прав в тех правопорядках, где теория объектности имеет значение» (Shipikova, 2024, p. 67), а российский — из их числа.
Но в науке высказываются и иные суждения: так, по мнению Е. Н. Агибаловой, цифровые права вообще не сто́ит относить к объектам (Agibalova, 2020, p. 95).

[15] Обсуждая применение законоположения в плоскости его сопоставления с п. 2 ст. 382 ГК РФ, И. Шенгелия справедливо отмечает, что «если суды признают норму [п. 3 ст. 141.1 ГК РФ. — *Ю. П.*] императивной, владелец ЦФА сможет оспорить решение о выпуске, ограничивающее оборот ЦФА на вторичном рынке» (Shengeliya, 2024).

Вопросы квалификации предписания п. 3 ст. 141.1 ГК РФ как императивного или диспозитивного

Пункт 3 ст. 141.1 ГК РФ не предусматривает возможность установления каких-либо изъятий при его применении, причем не только в децентрализованном порядке, но и в нормативно-правовых актах (ср. с п. 2 ст. 141.1 ГК РФ, где четко заявляется о допустимости введения законом исключений). Тем не менее она лишена категоричности, поскольку правило сформулировано **без явного запрета на пересмотр**. В этой связи и с учетом разъяснений высших судебных инстанций касаемо критериев квалификации нормы как императивной или диспозитивной[16] нельзя говорить о предустановленной императивности обсуждаемого положения.

Но, может быть, императивность вытекает из **существа и целей законодательного регулирования** отношений в области оборота цифровых прав (который соединяет два взаимосвязанных элемента: технический и правовой, что «существенно отражается на механизме взаимодействия… субъектов…» (Zaytsev, 2025, p. 96))? В данном измерении знаковым оказывается вопрос о характере ***сопряжения*** исследуемой нормы ***с базовым предписанием, в силу которого осуществление, распоряжение или ограничение распоряжения цифровыми правами возможны сугубо в информационной системе без обращения к третьему лицу*** (второе предложение п. 1 ст. 141.1 ГК РФ).

Гипотетически в п. 3 ст. 141.1 ГК РФ можно увидеть конкретное ***проявление*** означенной общей установки (притом что под третьим лицом, упоминаемым в п. 1 ст. 141.1, тогда будет мыслиться и обязанное по цифровому праву лицо). В этом ключе рассуждает З. И. Дахаева: присущий цифровым правам признак, в соответствии с которым их «осуществление и распоряжение [происходят. — *Ю. П.*] в информационной системе без обращения к *третьему лицу…*», «указывает на… возможность самостоятельной реализации прав… *без необходимости взаимодействия с* посредником или *обязанной стороной…*», что «характерно для децентрализованных систем» (Dakhayeva, 2025, p. 178).

Действительно, цифровое «бытие» имущественных прав, наряду с прочим, знаменует существенное упрощение их оборота: так, «операции с ЦФА могут быть выполнены практически мгновенно и без лишних бюрократических процедур», что «не только экономит время, но и уменьшает транзакционные издержки…» (Sarayeva, 2025, p. 644). Вместе с тем правило п. 1 ст. 141.1 ГК РФ очевидно сконструировано как *антипод* положения о распоряжении и ограничении распоряжения бездокументарными ценными бумагами (о родстве которых с цифровыми правами мы уже писали): в силу п. 3 ст. 149 ГК РФ операции с названными объектами производятся не иначе как посредством *обращения к лицу, осуществляющему учет прав на бездокументарные ценные бумаги,* для внесения соответствующих записей, тогда как пункт 1 ст. 141.1 ГК РФ, «привязав» цифровые права к информационной системе, напротив, фиксирует отсутствие потребности в обращении к третьему лицу. Соответственно, осуществление и обращение цифровых прав просто *не предполагают внешнего юридического сопровождения*, т. е. обладатель цифрового права контактирует не с субъектом, выполняющим функции регистратора, а, фигурально выражаясь, напрямую с информационной системой (именно к этому, пожалуй, в основном и сводится целеполагание императива второго предложения

[16] См.: п. 1–4 Постановления Пленума ВАС РФ «О свободе договора и ее пределах» от 14 марта 2014 г. № 16. Вестник ВАС РФ. 2014. № 5.

п. 1 ст. 141.1 ГК РФ[17]). Но и этот тезис не сто́ит понимать превратно, например в смысле отрицания наличия какой-либо системы учета: возникновение, переход, обременение и прекращение цифровых прав все равно требуют внесения соответствующей информации (записи) в информационную систему, причем такому внесению, как правило, придается правоустанавливающее значение[18] (ч. 7 ст. 8 Закона об инвестплатформах, ч. 2 ст. 1, ч. 2, 5 и 6 ст. 4 Закона о ЦФА).

Таким образом, несмотря на тесную взаимосвязь сопоставляемых норм ст. 141.1 ГК РФ, позволительно утверждать об их ***самостоятельной смысловой нагрузке***; представленное в п. 3 решение хотя и релевантно содержащемуся во втором предложении п. 1 предписанию, отнюдь не детерминируется им.

Кроме того, ***цифровому обороту разрешительный порядок совершения сделок*** (как таковой) ***не противопоказан***. Как мы уже отмечали, п. 3 ст. 141.1 ГК РФ не обнуляет предусмотренную нормативным актом или договором обязательность санкционирования другими, нежели обязанный, субъектами действий по распоряжению цифровыми правами; не отменяется, кстати, и режим согласования с обладателем цифрового права перевода долга обязанным по цифровому праву лицом на другое лицо. При этом проверочная деятельность, в принципе, может проводиться и в информационной системе (пусть и своеобразно благодаря автоматизированности процессов[19]). Так, Закон об инвестплатформах прямо предусматривает необходимость обеспечения *соблюдения* в том числе *условий обращения* утилитарных цифровых прав, определенных в инвестиционном предложении, притом что *список данных требований не является исчерпывающим* (ч. 4 ст. 11, ч. 2 ст. 13); Закон о ЦФА возлагает на оператора информационной системы обязанность обеспечения невозможности внесения и (или) изменения записей о ЦФА в обход некоторых ограничений и запретов (п. 5 и 6 ч. 1 ст. 6). Тем самым роль оператора информационной системы не сводится к *технической* модерации, от него в серьезной степени, как справедливо поясняет В. Н. Лисица, «зависит *юридическая* судьба возникших в такой системе цифровых прав…» (Lisitsa, 2024, p. 152). Приведенные обстоятельства вновь свидетельствуют об известной условности жесткого противополагания функционалов лица, осуществляющего учет прав на бездокументарные ценные бумаги, и оператора информационной системы: последний, по здравому заключению Д. С. Четвергова, «выполняет целый ряд функций, присущих различным участникам традиционного рынка ценных бумаг» (Chetvergov, 2025, p. 129).

В свете изложенного правильно разделить мнение А. А. Волоса об ***отсутствии*** на текущий момент ***бесспорных оснований для оценки изучаемой нормы как императивной*** (в самом деле, «применяя критерии, изложенные в Постановлении «О свободе договора», можно… доказать, что положения… нельзя считать строго императивными», политико-правовое обоснование противоположного вывода затруднительно (Volos, 2024a, p. 262; Volos, 2024b, pp. 21–22)).

---

[17] Но регулирование данного аспекта с позиции ясности восприятия вряд ли можно признать удовлетворительным: «смысл оговорки… „без обращения к третьему лицу“», по небеспочвенному замечанию А. В. Семенова, во многом загадочен (Novoselova et al., 2019, p. 45).

[18] «…криптозапись… — справедливо подчеркивает Д. А. Нигматзянова, — не просто передача данных, а *юридически значимое действие*, закрепляющее актив…» (Nigmatzyanova, 2024, p. 97).

[19] Более того, при переходе цифровых объектов по основаниям, предусмотренным законом (наследование, реорганизация юридического лица и пр.), неизбежно *обращение к оператору* информационной системы с представлением необходимых документов, см., например: ЦФА ХАБ. (2023). *Правила информационной системы ООО «Блокчейн Хаб»* (п. 22). Банк России. https://www.cbr.ru/Queries/XsltBlock/File/98365/1460; Сбербанк. (2025). *Правила информационной системы ПАО «Сбербанк», в которой осуществляется выпуск цифровых финансовых активов* (пп. 28–29). ЦФА РФ. https://xn--80a3bf.xn--p1ai/Pravilapolzovaniyaplatformoj/Sberbank/38

Для устранения сомнений в этом законодателю следовало проявить бóльшую решительность, установив явно выраженный запрет на отклонение от «циркуляра».

Помня, однако, об определенной востребованности в деловой среде механизмов контроля за обращением цифровых прав (по словам А. С. Генкина, «обычаи, уже сформировавшиеся на... рынке, зачастую предполагают установление... эмитентами ограничений на оборот...» (Novoselova et al., 2019, p. 36)[20]), принимая в расчет содержательный плюрализм цифровых прав (не только денежные, но и натуральные обязательственные требования и т. д.) и разнообразие информационных систем (функционирующих в том числе, но не исключительно, на базе технологии распределенного реестра), а равно имея в виду достаточно деликатное нормирование последствий игнорирования договорного режима согласования с должником цессии (п. 3 и 4 ст. 388 ГК РФ), укажем на *нецелесообразность* придания исследуемому концепту характера константы; **децентрализованная регламентация** (невзирая на снижение мобильности объектов при введении отступлений от концепта), хотя бы в некоторых случаях, **видится** вполне **приемлемой**.

Примечательно, что законопроект в первоначальной версии совершенно иначе, в сравнении с итоговой редакцией ст. 141.1 ГК РФ, подходил к разрешению разбираемой дилеммы: в нем оговаривалось, что цифровые права могут переходить *«на тех же условиях, что и объекты... права на которые они удостоверяют...»;* т. е. необходимость санкционирования распорядительного акта обязанным лицом огульно не пресекалась, напротив, подразумевалось сохранение силы специальных правил об оборотоспособности активов, подтверждаемых цифровыми правами (в логике модели «право на право», не получившей, правда, в итоге законодательного воплощения, по крайней мере последовательного).

В развитие сказанного любопытен **аспект (не)допустимости изменения** изучаемого **законоположения правилами информационной системы**. Например, А. А. Волос отстаивает подход, в русле которого отличное от п. 3 ст. 141.1 ГК РФ положение может быть введено «сторонами отношений *и (или) правилами* информационных систем» (Volos, 2024b, p. 21).

Вообще децентрализованному «делегированному нормотворчеству в киберпространстве» (правда, под серьезным надзором со стороны государства, так как, в частности, утвержденные оператором правила информационной системы должны пройти согласование с Банком России согласно ч. 5 ст. 4 Закона об инвестплатформах, ст. 7 Закона о ЦФА) в настоящее время отводится чрезвычайно важная роль, что позволяет вслед за В. В. Зайцевым уверенно говорить о *сочетании государственной и негосударственной регламентации* как одной из характерных черт механизма гражданско-правового регулирования оборота цифровых активов (Zaytsev, 2025, pp. 99, 101) (более того, такой оборот в некотором смысле, как небеспочвенно заявляет П. А. Непомнящий, «происходит в меньшей степени по требованиям законодательства и *в большей степени по правилам информационных систем*» (Nepomnyashchiy, 2024, p. 201)).

Несмотря на сказанное, легитимность локальной регламентации анализируемого аспекта довольно сомнительна. ГК РФ прямо санкционирует упорядочение правилами информационной системы отношений в части:

а) содержания цифровых прав (п. 1 ст. 141.1 ГК РФ); ясно, что этот компонент напрямую переход цифрового права не затрагивает;
б) условий осуществления цифровых прав (п. 1 ст. 141.1 ГК РФ); между тем понятия «осуществление права» и «распоряжение правом» (включая его передачу) — в логике предписаний

[20] Неудивительно, что автора «настораживает априорная возможность отчуждения цифровых прав без согласия эмитента...».

ст. 141.1 ГК РФ — не пересекаются и не подчиняются одно другому, а потому *передача цифрового права буквально не является его осуществлением* (аналогичный подход, кстати, избран законодателем и для бездокументарных ценных бумаг в соответствии с п. 1 ст. 142, п. 3 ст. 149 ГК РФ)[21]. Отсюда апеллирование для обоснования правомерности корректировки правилами информационной системы режима свободной передачи цифрового права к ч. 4 ст. 8 Закона об инвестплатформах (Volos, 2024b, p. 21) (где, как и в ГК РФ, фиксируется механизм определения условий именно осуществления цифрового права, а не распоряжения им) представляется ошибочным;

в) определения лица, имеющего возможность распоряжаться цифровым правом (приравниваемого по умолчанию к обладателю цифрового права); однако данный момент, опять же, не имеет отношения к собственно режиму (не)согласования совершения акта распоряжения цифровым правом.

Таким образом, «содержание права... и условия его осуществления... определяются не традиционными правовыми актами или договорами *в полном объеме*, а правилами конкретной информационной системы», что зримо «подчеркивает зависимость права от технологической среды его существования» (Dakhayeva, 2025, p. 178). Однако ***ГК РФ проблематику собственно оснований и условий передачи цифровых прав к предмету локальной регламентации не относит;*** не нацеливает на это и специальное законодательство (ч. 2 ст. 4 Закона об инвестплатформах, ч. 3 ст. 5 Закона о ЦФА).

Кроме того, ***поднормативное регулирование*** по интересующему нас аспекту ***должно быть сосредоточено***, как представляется, ***преимущественно на технико-процедурных моментах*** (имеется в виду технико-процессуальная детерминированность цифровых прав, когда, как верно подчеркивает Н. Ш. Газгиреев, «содержательные аспекты и механизмы исполнения цифровых правомочий устанавливаются техническими протоколами и операционными правилами информационной экосистемы» (Gazgireyev, 2025, p. 84)). Часть 8 ст. 8 Закона об инвестплатформах вменяет оператору инвестиционной платформы в обязанность обеспечение всем ее участникам, прежде всего *технической,* возможности приобретать утилитарные цифровые права при их обращении, знакомиться с их содержанием, осуществлять их, а также распоряжаться ими. При этом правила инвестиционной платформы непременно должны содержать *порядок внесения информации* о возникновении, переходе и прекращении утилитарного цифрового права (ч. 7 ст. 8 Закона об инвестплатформах). Статья 4 Закона о ЦФА также акцентирует внимание на закреплении правилами информационной системы *способов и порядка внесения* соответствующих *записей*.

Наконец, даже при признании правомерности исследуемой децентрализованной регуляции ***речь в конечном счете все равно будет идти об определении условий обращения цифровых прав сторонами*** договора инвестирования (пусть с опорой на локальные правила и с их соблюдением)[22]. Неслучайно в п. 1 ст. 141.1 ГК РФ говорится об определении содержания и условий осуществления цифровых прав не собственно правилами информационной системы, а *в соответствии* с ними (поэтому заключать, что означенные моменты «будет определять именно информационная система» (Ovchinnikov & Fatkhi, 2019, p. 109), все-таки не совсем

[21] Правда, в доктрине подобное разграничение нередко подвергается критике: так, А. В. Семёнову импонирует подход, при котором *осуществление* субъективного права *включает в себя распоряжение* им (Novoselova et al., 2019, p. 44).

[22] Показательно, что А. А. Волос, допускающий изменение представленной в п. 3 ст. 141.1 ГК РФ модели правилами информационной системы, отмечает, что они «есть неотъемлемая *часть договорных условий* между субъектами, которые совершают сделки по поводу цифрового права» (Volos, 2024b, p. 22).

обоснованно). Солидаризируемся с С. В. Сарбашем в том, что подход, при котором «примат [в регламентации содержания и условий осуществления цифровых прав. — *Ю. П.*] отдается средству (информационной системе), а не праву», ущербен и ведет к искажению основных цивилистических начал (Novoselova et al., 2019, p. 39)[23]. Еще более симптоматичны отдельные указания Закона об инвестплатформах: часть 4 ст. 8 исходит из того, что содержание и условия осуществления утилитарных цифровых прав определяет именно *лицо, привлекающее инвестиции*, хотя и руководствуясь правилами инвестиционной платформы; ч. 4 ст. 11 и ч. 2 ст. 13 предусматривают непреложность обеспечения в инвестиционной платформе соблюдения условий обращения утилитарных цифровых прав, которые определены в *инвестиционном предложении*, а не в правилах информационной платформы (притом что данные условия обязательно содержатся в инвестиционном предложении согласно ч. 2 ст. 13).

Заключение

Адаптация регулирования оборота цифровых прав к сущностной специфике последних выразилась в появлении в ГК РФ нормы о переходе цифрового права на основании сделки без согласия обязанного лица. Данное предписание при его трактовке как строгой максимы препятствует задействованию некоторых предусмотренных нормативными правовыми актами режимов согласования (например, оговоренного в п. 2 ст. 382 ГК РФ) и инициативному установлению разрешительного порядка сторонами. Между тем квалификация пункта 3 ст. 141.1 ГК РФ как императивного спорна (в том числе под углом зрения его соотнесения с существом и целями законодательной регламентации); мало того, имеются политико-правовые основания для отказа от восприятия концепта свободного трансферта цифровых прав как универсального и безусловного.

Список литературы / References

1. Agibalova, E. N. (2020). Tsifrovyye prava v sisteme ob'yektov grazhdanskikh prav [Digital rights in the system of civil rights objects]. *Yuridicheskiy Vestnik Dagestanskogo Gosudarstvennogo Universiteta*, *33*(1), 90–99. https://doi.org/10.21779/2224-0241-2020-33-1-90-99
2. Chetvergov, D. S. (2025). Pravovyye problemy posrednicheskoy deyatel'nosti na rynke tsifrovykh finansovykh aktivov [Legal issues of intermediary activities in the digital assets market]. *Actual Problems of Russian Law*, *20*(5), 124–135. https://doi.org/10.17803/1994-1471.2025.174.5.124-135
3. Dakhayeva, Z. I. (2025). Tsifrovyye prava v sisteme ob'yektov grazhdanskikh prav: problemy pravovogo regulirovaniya v Rossiyskoy Federatsii [Digital rights in the system of civil rights objects: problems of legal regulation in the Russian Federation]. *Ekonomika i Upravleniye: Problemy, Resheniya*, *12*(3 March), 175–181. https://doi.org/10.36871/ek.up.p.r.2025.03.12.021
4. Gazgireyev, N. Sh. (2025). Pravovaya regulyatsiya tsifrovykh prav v kontekste formirovaniya i razvitiya tsifrovoy sredy [Legal regulation of digital rights in the context of the formation and development of the digital environment]. *Zakon i Vlast'*, *3*, 83–87.
5. Kontsevoy, A. V. (2020). K voprosu ob elementakh konstruktsii kriptovalyutnogo obyazatel'stva i yego differentsiatsii ot denezhnykh, valyutnykh i fondovykh obyazatel'stv [On the issue of the elements of the design

[23] Поэтому значима глубокая теоретическая проработка вопроса о *пределах* рассматриваемого локального регулирования, тем более что контент правил информационных систем определяется законодателем неисчерпывающим образом (см., например, ч. 3 ст. 4 Закона об инвестплатформах).

of a cryptocurrency obligation and its differentiation from monetary, currency and stock obligations]. *Yurist*, *7*, 13–17. https://doi.org/10.18572/1812-3929-2020-7-13-17

6. Lisitsa, V. N. (2024). Tsifrovyye prava kak grazhdanskiye prava, deystvuyushchiye v informatsionnoy sisteme [Digital rights as civil rights operating in the information system]. *Pravovaya Politika i Pravovaya Zhizn'*, *3*, 149–154. https://doi.org/10.24412/1608-8794-2024-3-149-154
7. Markina, M. V. (2022). Tsifrovyye prava, prinadlezhashchiye yuridicheskim litsam, kak oborotosposobnyy ob'yekt grazhdanskikh prav [Digital rights owned by legal entities as a negotiable object of civil rights]. *Yurist*, *11*, 36–40. https://doi.org/10.18572/1812-3929-2022-11-36-40
8. Mograbyan, A. S. (2022). Tsifrovyye prava kak ob'yekty grazhdanskikh prav v Rossii [Digital rights as objects of civil rights in Russia]. *Actual Problems of Russian Law*, *17*(10), 141–147. https://doi.org/10.17803/1994-1471.2022.143.10.141-147
9. Muratova, S. A., & Druzhinin, I. D. (2023). Otdel'nyye problemy pravovogo regulirovaniya tsifrovykh prav [Certain problems of legal regulation of digital rights]. *Tsivilist*, *6*, 31–37.
10. Nepomnyashchiy, P. A. (2024). Ponyatiye, sushchnost' i znacheniye tsifrovykh prav kak ob'yektov nasledstvennykh pravootnosheniy [Concept, essence and significance of digital rights as objects of inheritance legal relations]. *Courier of Kutafin Moscow State Law University (MSAL)*, *11*(123), 199–207. https://doi.org/10.17803/2311-5998.2024.123.11.199-207
11. Nigmatzyanova, D. A. (2024). Problemy pravovogo regulirovaniya ucheta tsifrovykh finansovykh aktivov v Rossii [Legal issues in the regulation of accounting for digital financial assets in Russia]. *Digital Law Journal*, *5*(3), 95–108. https://doi.org/10.38044/2686-9136-2024-5-3-95-108
12. Novoselova, L., Gabov, A., Savel'yev, A., Genkin, A., Sarbash, S., Asoskov, A., Semenov, A., Yankovskiy, R., Zhuravlev, A., Tolkachev, A., Kamel'kova, A., Uspenskiy, M., Krupenin, R., Kislyy, V., Zhuzhzhalov, P., Popov, V., & Agranovskaya, M. (2019). Tsifrovyye prava kak novyy ob'yekt grazhdanskogo prava [Digital rights as a new object of civil law]. *Zakon*, *5*, 31–54.
13. Odintsov, S. V., & Mironov, E. Yu. (2020). Tsifrovizatsiya imushchestvennogo oborota: doktrinal'nyye traktovki i zakonodatel'naya praktika [Digitalization of property turnover: doctrinal interpretations and legislative practice]. *Sovremennoye Pravo*, *11*, 97–104. https://doi.org/10.25799/NI.2020.56.25.010
14. Ovchinnikov, A. I., & Fatkhi, V. I. (2019). Tsifrovyye prava kak ob''yekty grazhdanskikh prav [Digital rights as objects of civil rights]. *Filosofiya Prava*, *3*(90), 104–112.
15. Perepyolkina, N. V., & Perepyolkin, P. E. (2025). K voprosu o yuridicheskoy sushchnosti tsifrovykh prav [On the legal essence of digital rights]. *Vestnik Povolzhskogo Instituta Upravleniya*, *25*(3), 112–120.
16. Polezhayev, O. A. (2023). NFT-aktivy v sisteme ob'yektov grazhdanskikh prav: problemy yuridicheskoy kvalifikatsii otnosheniy [NFT-assets in the system of civil rights objects: problems of legal qualification of relations]. *Zakon*, *9*, 68–75. https://doi.org/10.37239/0869-4400-2023-20-9-68-75
17. Sarayeva, O. N. (2025). Tsifrovyye finansovyye aktivy v kontekste ikh rasprostraneniya i razvitiya v Rossiyskoy Federatsii [Digital financial assets in the context of their distribution and development in the Russian Federation]. *Pravo i Gosudarstvo: Teoriya i Praktika*, *3*, 642–646. https://doi.org/10.47643/1815-1337_2025_3_642
18. Shengeliya, I. (2024). TSFA v strukture derivativa: mekhanika i yuridicheskiye riski [DFA in the derivative structure: mechanics and legal risks]. *Bankovskoye Obozreniye. Prilozheniye «FinLegal»*, *2*, 75–79.
19. Shipikova, A. G. (2024). Podkhody k opredeleniyu tsifrovogo ob'yekta i tsifrovogo aktiva [Approaches to defining a digital object and a digital asset]. *Digital Law Journal*, *5*(2), 53–68. https://doi.org/10.38044/2686-9136-2024-5-2-1
20. Vasilevskaya, L. Yu. (2020). Tsifrovizatsiya grazhdanskogo oborota: problemy i tendentsii [Digitalization of civil turnover: Problems and trends]. *Rossiyskiy Yuridicheskiy Zhurnal*, *6*, 105–117. https://doi.org/10.34076/2071-3797-2020-6-105-117

21. Vavilin, E. V. (2024). Osushchestvleniye i zashchita grazhdanskikh prav v usloviyakh tsifrovoy transformatsii otnosheniy [Implementation and protection of civil rights in the context of digital transformation of relations]. *Vestnik Tomskogo Gosudarstvennogo Universiteta. Pravo*, *53*, 110–121. https://doi.org/10.17223/22253513/53/8
22. Volos, A. A. (2024a). Svoboda dogovora i yeye predely v tsifrovoy srede [Freedom of contract and its limits in the digital environment]. *Vestnik Permskogo Universiteta. Yuridicheskiye Nauki*, *2*(64), 254–273. https://doi.org/10.17072/1995-4190-2024-64-254-273
23. Volos, A. A. (2024b). Tsifrovyye prava: nekotoryye problemy tolkovaniya pravil stat'i 141.1 Grazhdanskogo kodeksa Rossiyskoy Federatsii [Digital rights: Some problems of interpretation of the rules of Article 141.1 of the Civil Code of the Russian Federation]. *Bankovskoye Pravo*, *3*, 16–23. https://doi.org/10.18572/1812-3945-2024-3-16-23
24. Zakirov, R. Yu., & Shavaliyeva, D. R. (2021). Tsifrovyye prava kak ob'yekt grazhdanskikh prav [Digital rights as an object of civil rights]. *Regulirovaniye pravootnosheniy v usloviyakh tsifrovizatsii v period pandemii: sovremennoye sostoyaniye i perspektivy razvitiya: sb. statey.* Kazan', Otechestvo, 33–37.
25. Zaytsev, V. V. (2025). Mekhanizm pravovogo regulirovaniya oborota tsifrovykh aktivov [The mechanism of legal regulation of the turnover of digital assets]. *Vlast' Zakona*, *1*(61), 89–103.
26. Zhanabilova, A. B. (2023). Pravovoye regulirovaniye oborota tsifrovykh aktivov i vozmozhnost' ikh nasledovaniya v Kazakhstane i Rossii [Legal regulation of the circulation of digital assets and the possibility of their inheritance in Kazakhstan and Russia]. *Notarius*, *4*, 39–42. https://doi.org/10.18572/1813-1204-2023-4-39-42

Сведения об авторе:

Поваров Ю. С. — кандидат юридических наук, доцент, доцент кафедры гражданского и предпринимательского права, Самарский национальный исследовательский университет имени академика С. П. Королева, Самара, Россия.
povus@mail.ru
ORCID: https://orcid.org/0000-0002-4728-5301

Information about the author:

Iurii S. Povarov — Ph.D. in Law, Associate Professor of the Department of Civil and Entrepreneurial Law, Samara National Research University, Samara, Russia.
povus@mail.ru
ORCID: https://orcid.org/0000-0002-4728-5301