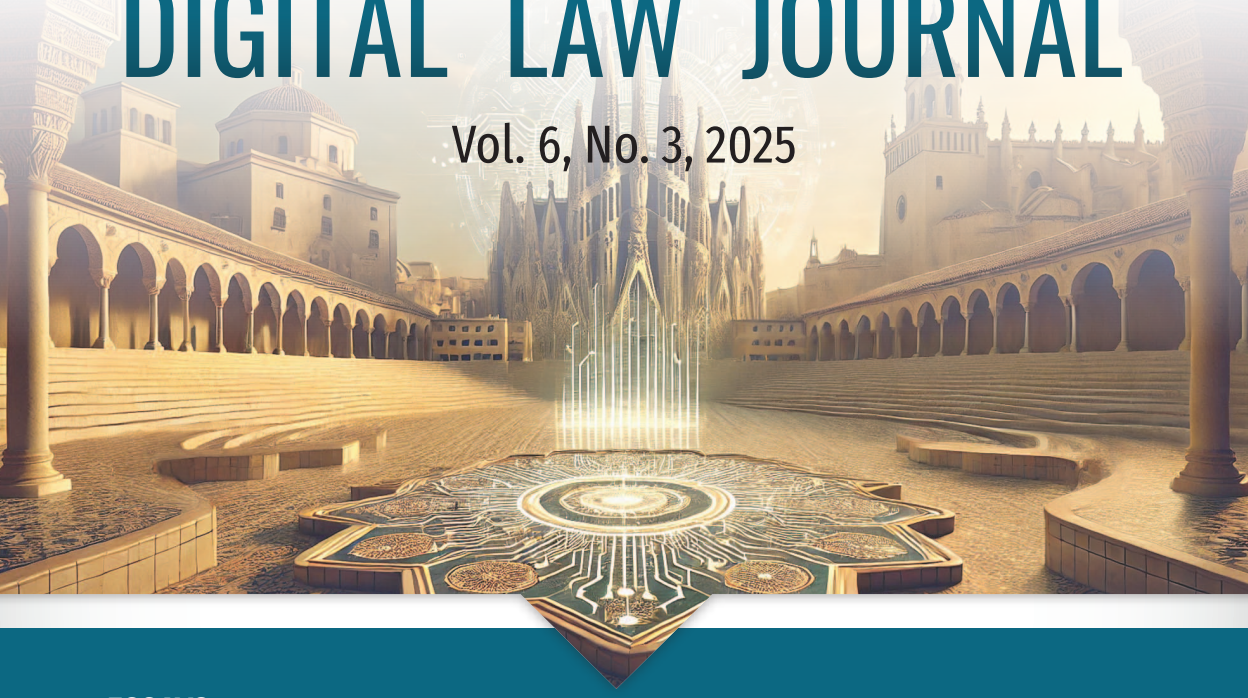
ISSN 2686-9136 (Online)

DIGITAL LAW JOURNAL

Vol. 6, No. 3, 2025



ESSAYS

ARTICLES

DIGITAL LAW JOURNAL

DIGITAL LAW JOURNAL

Journal of research and practice

Published since 2020
4 issues per year

Vol. 6, No. 3, 2025

ЦИФРОВОЕ ПРАВО

Научно-практический журнал

Журнал издается с 2020 г.
4 выпуска в год

Том 6, № 3, 2025

Contents

Essays

Articles

Содержание

Эссе

Статьи

DIGITAL LAW JOURNAL

AIMS AND SCOPE

The Digital Law Journal is a peer-reviewed open-access academic journal publishing theoretical and applied research on the legal regulation of digital technologies. It is an international academic journal primarily oriented toward the academic community, while also welcoming submissions from legal practitioners whose research demonstrates a high level of analytical depth and scholarly rigor.

The journal accepts manuscripts in the fields of national, international, and comparative law. It is committed to an international perspective and seeks to publish research of international relevance that contributes to the development of global legal scholarship. Interdisciplinary and empirical legal research is considered within the journal's scope, provided that it maintains a clear legal focus and adheres to established standards of academic legal methodology.

The journal encourages research across a broad range of legal areas related to digitalization, including:

- Theoretical and philosophical foundations of digital law
- Constitutional and human rights discourse in the digital environment
- Legal aspects of artificial intelligence
- Legal regulation of data governance, privacy protection, and information security
- Online platforms: consumer protection and antitrust law
- Legal regulation of fintech, digital assets, and decentralized finance
- Electronic commerce and contract law in the online environment
- Intellectual property in the information age
- Tax and administrative law in the context of digitalization
- Labor law protection of workers in the digital era
- Legal aspects of the digital transformation of the justice system
- International legal regulation of cyberspace and issues of digital sovereignty

FOUNDER, PUBLISHER:

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

Founded:	The journal has been published since 2020
Frequency:	Four issues per year
DOI Prefix:	10.38044
ISSN online:	2686-9136
Mass Media Registration Certificate:	No. FS 77-76948 (Roskomnadzor, October 9, 2019)
Distribution:	Content is distributed under Creative Commons Attribution 4.0 License
Publication Languages:	Russian, English
Editorial Office:	76, ave. Vernadsky, Moscow, Russia, 119454
Published online:	30 September 2025
Copyright:	© Digital Law Journal, 2025
Price:	Free of charge

REGION GROUP OF COMPANIES Supported by REGION Group of Companies

ЦИФРОВОЕ ПРАВО

ЦЕЛИ И ЗАДАЧИ

Журнал «Цифровое право» (Digital Law Journal) — это рецензируемый научный журнал открытого доступа, публикующий теоретические и прикладные исследования в области правового регулирования цифровых технологий. Журнал выступает международным изданием прежде всего для академического сообщества, вместе с тем предлагая возможность публикации практикующим юристам, чьи исследования характеризуются высоким уровнем аналитичности и научной обоснованности.

Журнал принимает работы, охватывающие национальное, международное и сравнительное право. Журнал «Цифровое право» (Digital Law Journal) поддерживает международную перспективу и стремится публиковать исследования, которые находят отклик у международного юридического сообщества и обогащают его. Допускаются междисциплинарные и эмпирико-правовые исследования при условии, что они сохраняют четкую правовую направленность и соответствуют стандартам академической юридической методологии.

Журнал поощряет исследования по широкому спектру направлений изучения права, связанных с цифровизацией, включая:

- Теоретические и философские основы цифрового права
- Конституционный и правозащитный дискурс в цифровой среде
- Правовые аспекты искусственного интеллекта
- Правовое регулирование управления данными, защита конфиденциальности и информационная безопасность
- Онлайн-платформы: защита прав потребителей и антимонопольное право
- Правовое регулирование финтеха, цифровые активы и децентрализованные финансы
- Электронная коммерция и договорное право в онлайн-среде
- Интеллектуальная собственность в информационную эпоху
- Налоговое и административное право в условиях цифровизации
- Трудоправовая защита работников в цифровую эпоху
- Правовые аспекты цифровой трансформации системы правосудия
- Международно-правовое регулирование киберпространства и вопросы цифрового суверенитета

УЧРЕДИТЕЛЬ, ИЗДАТЕЛЬ:

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

РЕДАКЦИЯ:

Нектов А.В., ответственный редактор
Степанов С.К., научный редактор
Доев А.М., редактор
119454, Россия, Москва, просп. Вернадского, 76

История издания журнала:	Журнал издается с 2020 года
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
Язык публикации:	Русский, английский
Редакция:	119454, Россия, Москва, просп. Вернадского, 76
Дата публикации:	30.09.2025
Копирайт:	© Цифровое право, 2025
Цена:	Бесплатное распространение

РЕГИОН ГРУППА КОМПАНИЙ При поддержке Группы компаний «РЕГИОН»

https://doi.org/10.38044/2686-9136-2025-6-10

ESSAYS

PROTECTING HUMAN RIGHTS IN THE DIGITAL AGE: LEGAL FRAMEWORKS AND MEDIA LITERACY AS A COMPLEMENTARY SAFEGUARD

Nour Nfissi

Autonomous University of Barcelona
Carrer de la Vinya, Bellaterra, Barcelona, Spain, 08193

Abstract

The expansion of digital technologies has reshaped the exercise of fundamental rights, prompting growing scholarly and regulatory attention to the notion of digital human rights. As digital platforms increasingly structure communication, access to information, and social participation, existing legal categories face conceptual and practical strain. While some accounts portray digital rights as a straightforward extension of classical human rights, others emphasize their transformative impact on constitutional principles, enforcement mechanisms, and the distribution of power between public authorities and private actors. This paper situates digital rights within contemporary academic debates and emerging regulatory frameworks in order to clarify their normative scope and conceptual boundaries. It advances the argument that digital rights cannot be adequately understood through purely legal or purely technological lenses. Instead, they emerge at the intersection of constitutional law, digital governance, and public policy, where regulatory instruments, institutional design, and educational strategies jointly shape the conditions for rights protection. The analysis highlights the constitutional paradox of digital platforms, which exercise functions traditionally associated with public authority while remaining only partially subject to democratic accountability and judicial oversight. Drawing on European constitutional principles, supranational regulation, and policy initiatives, the study demonstrates how current legal frameworks seek to respond to private digital power while revealing their structural limits in data-driven and algorithmic environments. At the same time, scholarship on Media and Information Literacy is mobilized to show how citizens' informational capacities function as a normative complement to legal safeguards, enabling individuals to exercise their rights meaningfully rather than merely formally. By integrating legal doctrine, public policy analysis, and MIL, this article contributes a coherent analytical framework for understanding digital rights as a hybrid normative construct. It concludes that the effective protection of digital rights depends not only on legal guarantees and regulatory enforcement, but also on policy choices that strengthen individual and collective capacities within the digital public sphere.

Keywords

digital human rights, cybersecurity, digital law, data protection, legal framework, media and information literacy

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.

For citation Nfissi, N. (2025). Protecting human rights in the digital age: Legal frameworks and media literacy as a complementary safeguard. *Digital Law Journal, 6*(3), 8–33. https://doi.org/10.38044/2686-9136-2025-6-10

Submitted: 8 July 2025, accepted: 15 Aug. 2025, published: 30 Sep. 2025

ЭССЕ

ЗАЩИТА ПРАВ ЧЕЛОВЕКА В ЦИФРОВУЮ ЭПОХУ: ПРАВОВЫЕ ОСНОВЫ И МЕДИАГРАМОТНОСТЬ КАК ДОПОЛНИТЕЛЬНАЯ ГАРАНТИЯ ИХ ОСУЩЕСТВЛЕНИЯ

Н. Нфисси

Автономный университет Барселоны
08193, Испания, Барселона, Беллатерра, Пласа Сивика

Аннотация

Распространение цифровых технологий изменило осуществление прав человека, что привело к росту внимания ученых и регулирующих органов к понятию цифровых прав человека. Поскольку цифровые платформы все больше структурируют коммуникацию, доступ к информации и социальное взаимодействие, существующие правовые категории сталкиваются с концептуальными и практическими трудностями. В то время как некоторые исследования представляют цифровые права как прямое продолжение классических прав человека, другие подчеркивают их преобразующее воздействие на конституционные принципы, механизмы обеспечения соблюдения прав и распределение власти между государственными органами и частными субъектами. В данной статье цифровые права рассматриваются в контексте современных академических дискуссий и формирующихся нормативных рамок с целью уточнения их нормативного охвата и концептуальных границ. В ней выдвигается аргумент о том, что цифровые права не могут быть адекватно поняты исключительно с юридической или исключительно технологической точки зрения. Вместо этого они возникают на пересечении конституционного права, цифрового управления и государственной политики, где регулирующие инструменты, институциональный дизайн и образовательные стратегии совместно формируют условия защиты прав. Автор подчеркивает конституционный парадокс цифровых платформ, которые выполняют функции, традиционно связанные с государственной властью, оставаясь при этом лишь частично подлежащими демократической подотчетности и судебному надзору. Опираясь на европейские конституционные принципы, наднациональное регулирование и политические инициативы, исследование демонстрирует, как правопорядки реагируют на цифровую власть частных субъектов, одновременно выявляя свои структурные ограничения в средах, основанных на данных и алгоритмах. В то же время используются исследования в области медиа- и информационной грамотности, чтобы показать, как информационные возможности граждан функционируют в качестве нормативного дополнения к правовым гарантиям, позволяя людям осуществлять свои права осмысленно, а не просто формально. Интегрируя правовую доктрину, анализ государственной политики и медиа- и информационную грамотность, эта статья предлагает целостную аналитическую основу для понимания цифровых прав как гибридной нормативной конструкции. В заключение делается вывод,

что эффективная защита цифровых прав зависит не только от правовых гарантий и правоприменения, но и от политических решений, которые укрепляют индивидуальные и коллективные возможности в цифровой публичной сфере.

Ключевые слова

цифровые права человека, кибербезопасность, цифровое право, защита данных, правовое регулирование, информационная грамотность

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.
Для цитирования	Нфисси, Н. (2025). Защита прав человека в цифровую эпоху: правовые основы и медиаграмотность как дополнительная гарантия их осуществления. *Цифровое право, 6*(3), 8–33. https://doi.org/10.38044/2686-9136-2025-6-10

Поступило: 08.07.2025, принято в печать: 15.08.2025, опубликовано: 30.09.2025

Introduction

Digital human rights encompass all the fundamental rights and essential protections to which users are entitled when engaging with digital platforms. They include both traditional human rights—such as freedom of expression and access to information— and new forms of rights.

This paper's claim that a new generation of rights, commonly referred to as digital rights, should be delineated due to profound digital transformations of society. However, it would be a significant overstatement to assert that these rights are entirely separate from traditional human rights; rather, they represent their extension and adaptation to the digital sphere: they are bound to them by indissoluble ties of shared principles.

The corpus of digital rights should include, among others, the right to privacy online, the right to control one's personal data, the right to access reliable digital information, the right to digital literacy, and the right to protection from algorithmic discrimination.

In the digital era, these rights have already become essential to ensuring that individuals can fully participate in social, economic, and political life while preserving their autonomy and dignity. Their recognition and protection are now central to any legal system that seeks to uphold fundamental rights in a technology-driven world.

At the same time, the digital revolution has introduced a new wave of digital threats that pose serious and complex risks to well-known human rights, such as privacy, equitable access to information, and the existing principles of exploitation personal data.

These threats make the protection of digital human rights by their theoretical and practical recognition more crucial than ever, and a robust legal and regulatory framework governing digital spaces is vital for understanding the mechanisms that ensure compliance with fundamental rights and democratic values.

In this context, the intersection between human rights and digital spaces raises a wide range of questions. How has the digital revolution reshaped the interpretation and application of fundamental human rights? In what ways do digital technologies challenge the enforcement of rights such as

privacy, freedom of expression, and access to information? What challenges and threats do they face in the digital age? What is the legal and practical significance of international instruments and conventions in regulating digital platforms and protecting users? What are the normative foundations of digital rights, and how should they guide legal regulation? Beyond legal measures, what educational and media literacy strategies can empower individuals to understand and assert their digital rights? And how can educational tools contribute to the protection of human rights within broader legal strategies?

This research aims to provide an overview comprehensive of how the digital revolution has transformed the interpretation and application of fundamental human rights. In the course of this study, I will address some of the questions outlined above, explore the complex challenges posed by digital technologies, particularly regarding privacy, freedom of expression, and access to information, as well as examine the emergence of new categories of digital rights.

Through a normative analysis of international human rights instruments, the study assesses their practical relevance in regulating digital platforms and safeguarding users. It also considers the theoretical foundations of digital rights, advocating for a regulatory approach that is both legally sound and socially responsive. In doing so, it integrates educational and media literacy strategies as complementary tools that empower individuals to understand, exercise, and protect their digital rights within a broader legal and democratic framework.

Digital Human Rights in the General Context: Insights from History and Legal Scholarship

In the 21st century, digital technologies have become an inseparable part of everyday human experience. The internet, social media, and digital platforms are now essential tools for communication, education, governance, and civic participation. As societies increasingly move into digital spaces, the exercise and protection of human rights are being redefined in real time.

Contextualizing human rights in the digital age therefore requires more than a mere technical update of legal texts; it calls for a deep reflection on how human dignity and freedom are being reshaped by technological forces. This reflection must also include an examination of the historical development of human rights and the ways in which they have adapted or struggled to adapt to successive waves of technological change. Furthermore, understanding the practical application of new digital human rights is essential. Finally, this discussion must remain sensitive to multicultural perspectives, recognizing that the interpretation and implementation of digital rights are influenced by cultural, political, and socio-economic contexts.

The Historical Background: From Classical to Digital Human Rights

The foundational principles of human rights were first formally articulated in the Universal Declaration of Human Rights of 1948.[1] However, the understanding and scope of these rights have evolved significantly over time, particularly following the development of the theory of the "generations of human rights, which provided a nuanced classification and expansion of rights concept in response to emerging social, political, and technological realities.

The evolution of human rights has often been viewed through the lens of the "three generations" theory developed by the French jurist Karel Vasak. Karel Vasak's late-1970s classification proposed that human rights evolved in three successive waves, ranging from civil and political freedoms to socio-economic guarantees and collective entitlements. Today, scholars question whether this model

[1] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

still reflects the complexity of contemporary rights frameworks (Domaradzki et al., 2019, pp. 424-425). The so-called "first generation" encompasses civil and political rights, such as freedom of expression and the right to privacy (Domaradzki et al., 2019, p. 424). The "second generation" includes economic, social, and cultural rights, while the "third generation" refers to collective and solidarity rights, including the right to development and the right to a healthy environment (Domaradzki et al., 2019, 425).

Vasak's tripartite model later influenced scholarly and institutional debates on the development of human rights. However, only the first two generations of rights he identified are reflected in the Universal Declaration of Human Rights,[2] whereas the third generation emerged gradually in later instruments of a declaratory character, such as the Stockholm Declaration[3] and the Rio Declaration.[4]

During the latter half of the 20th century, the first forms of digital human rights began to emerge. In Europe, the development of digital human rights started at the national level, led by pioneering countries such as Sweden and West Germany (Dowd, 2022, p. 72).

Sweden was the first to take the lead, enacting the world's first data protection law in 1973 (Dowd, 2022, p. 81). This law was designed to regulate the use of computers to ensure the protection of personal data and safeguard individuals' privacy. The core aim of Sweden's Data Act was to protect citizens' personal data from misuse and to ensure that the growing use of computerized systems did not infringe upon individual privacy rights.[5] As Lee Bygrave observes, Swedish data protection law has operated under a very stringent individuation requirement (Bygrave, 2002, p. 47).

A similar development took place in Germany, where a data protection law was introduced to safeguard personal privacy through the principles of data minimization and purpose limitation. The first national multimedia law in Germany was adopted in 1997 to regulate the internet and online services, setting out the conditions for information and communication services and harmonizing state media laws (Wuermeling, 1998, pp. 41–44).

Spiros Simitis, a Greek-German jurist and the principal pioneer of data protection and digital law, is widely regarded as the father of data protection in Germany. His work established the conceptual and normative foundations of data protection, emphasizing that it is not merely an administrative or technical issue, but a fundamental right tied to the preservation of human dignity (Schwartz, 2025, p. 111).

Simitis argues that data protection must encompass normative dimensions beyond mere technical control, particularly in the field of employment (Simitis, 1999). He also develops a conceptual framework in which data protection becomes an indispensable component of democratic societies undergoing rapid digital transformation (Schwartz, 2025, pp. 105–106.)

The concrete efforts of Sweden and Germany in developing security and data protection policies later influenced European digital frameworks and laid the groundwork for national initiatives in countries such as France and Spain.

In 1978, France adopted a law aimed at regulating the increasing use of data within both public and private sectors[6]. Following its adoption, France established the National Commission on Informatics

[2] Ibid.

[3] Declaration of the United Nations Conference on the Human Environment, June 16, 1972, U.N. Doc. A/CONF.48/14 (1972).

[4] Rio Declaration on Environment and Development, June 14, 1992, U.N. Doc. A/CONF.151/26 (Vol. I) (1992).

[5] DATALAG (Svensk författningssamling [SFS] 1973:289) (Swed.). See the English translation available at: https://www.worldlii.org/int/other/NDPrivLegis/1973/1.pdf

[6] Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Jan. 7, 1978, p. 227.

and Liberties (*Commission nationale de l'informatique et des libertés*, *CNIL*), an independent administrative authority empowered to oversee compliance, safeguard citizens' privacy, and ensure that data processing respected fundamental freedoms. This piece of legislation was a landmark act that laid the foundations for modern data protection in Europe. It was particularly significant because it explicitly recognized that the regulation of personal data was not merely a technical or administrative matter, but one directly tied to the preservation of civil liberties and fundamental rights (Dowd, 2022, pp. 185–187).

In the late 20th century, Spain adopted its first comprehensive legal framework on data protection through the enactment of Organic Law 5/1992 of 29 October on the Regulation of the Automatic Processing of Personal Data.[7] In response to the growing use of computerized systems for data collection, storage, and processing, Spain introduced a legal framework in 1992 designed to regulate the protection of personal data and limit potential misuse (Dowd, 2022, p. 185).

Over time, the European Union has remained at the forefront of digital regulation, continuously adapting to new technological challenges and innovations in the digital age. The digital era has brought about conceptual transformations in the content, understanding, implementation, and protection of human rights (Razmetaeva et al., 2022, pp. 55–56). Accordingly, this first part seeks to explore the real impact of digital technologies on users and human rights, as well as the emergence of new forms of human rights—digital human rights—within the technological and digital domain.

The Place of Digital Human Rights in Contemporary Legal Thought

The emergence of digital rights has become a prominent topic in contemporary legal scholarship, reflecting the growing intersection between technology and fundamental rights. Scholars have debated how traditional constitutional, human rights, and international law frameworks should adapt to the challenges posed by the digital environment.

For instance, Balkin (2004, p. 47) argued that existing constitutional rights—such as freedom of expression and privacy—should be reinterpreted to encompass digital contexts rather than replaced by entirely new legal categories.

According to Floridi, the digital revolution has reconfigured the "infosphere," transforming the conditions of informational privacy and personal identity; this conceptual shift suggests the need to reinterpret traditional rights, such as the right to privacy, in light of modern technologies (Floridi, 2005, pp. 185–188). And yet, it seems, that the reinterpreting approach was also supported by scholarship. As Hildebrandt argues, smart-technologies increasingly "invalidate previous forms of legal protection" by enabling profiling and control that current law cannot adequately address. In her book she further demonstrates how data-driven agency threatens traditional rights such as privacy, identity, due process and calls for a reconfiguration of legal guarantees under the conditions of a data-driven society (Hildebrandt, 2015, pp. 77–90; 186–200).

Constitutional Law Perspectives

Constitutional law has traditionally served as the cornerstone for the protection of fundamental rights within national legal systems. With the advent of the digital age, however, constitutional frameworks face unprecedented challenges, as rights originally conceived for the offline world must be reinterpreted and adapted to new technological realities. Issues such as data protection, online privacy, freedom of expression on digital platforms, and equal access to digital infrastructures have

[7] Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal [Organic Law on the Regulation of Automated Processing of Personal Data; L.O.R.T.A.D.], (B.O.E. 1992, 262) (Spain).

raised the question of whether existing constitutional guarantees remain sufficient or whether new, explicitly recognized concept of "digital rights" is needed.

This intersection between constitutional law and digital rights has given rise to the notion of digital constitutionalism, which highlights the role of constitutional principles in regulating the digital environment and safeguarding individual freedoms in cyberspace (De Gregorio, 2022, pp. 1–25). The rapid expansion of digital technologies has challenged traditional constitutional frameworks, prompting scholars to reconsider how fundamental rights can be effectively protected in online environments.

Several European scholars have made significant contributions to the theoretical and constitutional understanding of digital rights in the age of algorithmic governance. For instance, Oreste Pollicino, in his research, introduced the concept of the "constitutionalization of the Internet" within the European context. He argues that as private digital platforms increasingly perform functions traditionally carried out by public authorities, constitutional safeguards—particularly those concerning democracy and pluralism—must be extended into the digital sphere. While Mireille Hildebrandt highlights the profound implications of algorithmic systems for constitutional guarantees. She examines how data-driven environments undermine classical legal safeguards by shifting regulation from ex-ante legal norms to real-time computational architectures, arguing that constitutional rights must be re-conceptualized to remain effective in an algorithmic society (Hildebrandt, 2015, p. 223). Building on a more philosophical foundation, Luciano Floridi introduces the concept of the infosphere to describe the totality of digital interactions that shape contemporary human existence (Floridi, 2016). From an institutional perspective, Giovanni De Gregorio adopts a more structural approach, where he formalizes the notion of digital constitutionalism (De Gregorio, 2022, pp. 1–25). He emphasizes the need to adapt constitutional structures to regulate private digital actors and to uphold fundamental rights within the European Union. His work identifies the EU's emerging digital legal framework as a prototype for global digital governance (De Gregorio, 2022, pp. 290–296).

These scholars offer complementary yet distinct perspectives on the intersection between digital technology and constitutional law. I largely concur with Pollicino's claim that digital platforms have assumed quasi-governmental roles and that constitutional principles must evolve accordingly. However, his framework tends to idealize the capacity of constitutional law to restrain private power without fully addressing the limitations of enforcement mechanisms in the digital environment[8].

The contributions of these authors are both persuasive and intellectually rigorous. Yet, their analyses leave several crucial questions unresolved: What is missing from the current debate? Which normative and institutional challenges remain insufficiently explored? And, most importantly, how is constitutional law itself evolving and adapting in the digital age?

From my perspective, the relationship between constitutional law and emerging digital rights demonstrates both continuity and transformation. On the one hand, constitutional law continues to serve as the primary normative framework for the protection of fundamental rights, ensuring that liberties such as privacy, freedom of expression, and equality remain legally enforceable even within digital environments. On the other hand, the rapid expansion of algorithmic governance reveals the limitations of constitutions drafted in a pre-digital era, which are still deeply rooted in national boundaries.

So, in this context, several new key challenges emerge.

[8] Pollicino, O. (2019). *Digital private powers exercising public functions: The constitutional paradox in the digital age and its possible solutions*. European Court of Human Rights. https://www.echr.coe.int/documents/d/echr/Intervention_20210415_Pollicino_Rule_of_Law_ENG

The first is *the temporal gap* between constitutional frameworks and the accelerating pace of digitalization. Constitutions, often rigid and slow to adapt, struggle to keep up with the disruptive innovations of digital platforms and algorithmic systems, creating normative vacuums where rights are insufficiently protected.

A second challenge lies in *the ambiguity surrounding the constitutional status of digital rights*. While courts and legislatures increasingly interpret traditional rights in light of digital realities, the absence of explicit constitutional recognition leaves digital rights in a fragile and uncertain position. This makes the clear constitutional enshrinement of digital rights a pressing necessity, both to ensure their legal force and to reinforce their legitimacy as fundamental rights.

Third, there is *the displacement of power from the state to private actors*. Global technology companies now perform functions once reserved for public authorities, from moderating speech to managing digital infrastructures. This shift raises profound questions about accountability and the role of constitutional safeguards in regulating entities that often operate beyond the reach of national jurisdictions.

Finally, *the tension between judicial activism and democratic legitimacy* adds yet another layer of complexity. Courts often intervene to fill the constitutional void left by legislative inertia, but their actions may raise concerns about the democratic legitimacy of judge-made digital rights and the balance of powers within constitutional systems.[9]

In this regard, constitutional law is evolving in the context of digitalization through two interconnected dynamics. First, courts engage in evolutionary interpretation, extending traditional rights to digital contexts—for instance, construing the right to privacy as encompassing data protection, or recognizing online freedom of expression as essential to democratic participation. Second, we are witnessing the emergence of explicit digital rights frameworks, whether through constitutional reforms or supranational initiatives (e.g. EU Charter of Fundamental Rights[10] or EU Declaration on Digital Rights and Principles[11]), which already provides a normative foundation for digital constitutionalism.

Nevertheless, these developments demonstrate that constitutional law can no longer remain confined within its traditional boundaries. In my view, its future in the digital age requires a pluralist and layered conception of constitutionalism—one that recognizes constitutional guarantees must operate not only within states but also across regional and global levels, while simultaneously engaging with the regulatory power of private actors.

Only such a multi-level approach can reconcile technological transformation with constitutional legitimacy and preserve human dignity, autonomy, and the democratic values placed under unprecedented pressure by digitalization.

Human Rights in the International and European Law Discourse

Digital technologies have transformed the ways in which fundamental human rights are exercised and protected. Rights are increasingly shaped by online platforms, social networks, and digital

[9] For example, the German Federal Constitutional Court, in case 1 BvR 370/07 (27 February 2008), established a new fundamental right protecting the confidentiality and integrity of computer systems, illustrating how courts can regulate digital matters in the absence of clear legislation. *See,* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], 1 BvR 370/07, Feb. 27, 2008.

[10] Charter of Fundamental Rights of the European Union, art. 7, 8, 11, 2012 O.J. (C 326) 391, 397–398.

[11] The European Commission proposed a "European Declaration on Digital Rights and Principles" in 2022, outlining rights such as digital inclusion, online privacy, and access to digital services, aimed at guiding both EU institutions and Member States in the digital transition. *See,* European Declaration on Digital Rights and Principles for the Digital Decade, 2023 O.J. (C 23) 1.

services. International organizations including the United Nations, the Council of Europe, and the European Union have acknowledged that the digital environment presents both opportunities and challenges for human rights.

Through various declarations, resolutions, and policy frameworks, these organizations emphasize that digital rights represent an extension of classical human rights and require adaptation to ensure their protection in the digital age. This perspective provides a normative foundation for understanding digital rights as integral to the promotion and safeguarding of human dignity, freedom, and equality in the online sphere.

Several scholars have expanded the discussion on digital rights into the international and transnational arena, placing human rights at the core of digital governance. Ian Brown and Douwe Korff emphasize in their report the central importance of privacy and data protection within the European human rights framework.[12] They argue that classical rights enshrined in international human rights treaties must be reinterpreted and strengthened to address the complex challenges posed by digital technologies, particularly in relation to surveillance and data exploitation. From a more intersectional and socio-legal perspective, Sonia Katyal examines the tensions between privacy, freedom of expression, and intellectual property enforcement (Katyal, 2005). She advocates for a digital civil rights approach that acknowledges the overlap—and at times, the conflict—between these rights in online regulation, calling for balanced policies that avoid undermining one right in the name of another (Katyal, 2005).

These scholars contribute valuable to the discourse on digital rights, particularly at the international level. They emphasize the importance of grounding digital rights in robust, adaptable, and globally aware legal systems. Their work complements European constitutional perspectives by extending the conversation beyond the EU and highlighting the inherently global nature of digital freedoms.

While the contributions of Katyal as well as Brown & Korff offer significant insights, they also expose certain unresolved challenges, which as previously discussed are equally characteristic of constitutional law. The first is *the legal and territorial fragmentation of digital rights protection* (Brown & Korff, 2012). Katyal highlights the *conflicts between privacy, freedom of expression, and intellectual property enforcement* (Katyal, 2005). A second issue concerns *the ambiguous constitutional and legal status of digital rights*, which makes them vulnerable to selective or inconsistent application across jurisdictions. A third challenge lies in *the conflicts between fundamental rights*, such as privacy versus freedom of expression or intellectual property versus access to information, which remain insufficiently resolved at the international level, creating uncertainty for both individuals and regulators. Finally, the *temporal gap* between rapid technological change and the slow evolution of international institutions continues to undermine effective governance in the digital sphere.

Key International Instruments Contributing to the Development of Digital Rights within the Human Rights Framework

At the institutional level, several key international and regional organizations have established the normative foundations for the recognition and protection of digital rights, often by extending classical human rights into the digital environment.

[12] Brown, I., & Korff, D. (2012). *Digital freedoms in international law: Practical steps to protect human rights online.* Global Network Initiative. https://ssrn.com/abstract=2085342

The United Nations, through the Universal Declaration of Human Rights, provides the foundational framework: Article 12 protects the right to privacy, and Article 19 guarantees freedom of expression.[13] Although these principles were drafted in a pre-digital era, they are increasingly interpreted as applicable to online spaces, serving as the moral and legal basis for the global digital rights discourse (De Gregorio, 2022, pp. 45–47).[14]

The International Covenant on Civil and Political Rights further reinforces this applicability. Article 17 safeguards the right to privacy, while Article 19 ensures freedom of expression and access to information, all of which are directly relevant to digital communication, surveillance, and data collection practices.[15] These provisions have been invoked by NGOs and courts, to frame violations of digital rights as infringements of human rights.[16]

At the regional level, the Council of Europe has taken proactive steps to articulate digital rights more explicitly. The Committee of Ministers' Recommendation on Human Rights and the Internet urges member states to ensure that core human rights including privacy, freedom of expression, and access to information are effectively upheld in the digital sphere. It also encourages national legal systems to adapt to the realities of cyberspace.[17]

Complementing this, the European Declaration on Digital Rights and Principles, adopted by the European Union in 2022 seeks to systematize digital rights, aligning them more clearly with existing human rights law.[18] The Declaration highlights key issues such as transparency, access, digital education, and protection from harm in online environments, advocating for a comprehensive and people-centered digital rights agenda.

These institutional initiatives provide an essential normative backbone for the protection of digital rights. The UN frameworks—particularly the Universal Declaration of Human Rights[19] and the International Covenant on Civil and Political Rights[20]—remain foundational. However, their broad and non-binding nature limits their effectiveness in addressing complex cross-border digital threats. Their implementation depends heavily on the political will and institutional capacity of states, which vary considerably.

The Place of Digital Rights in Media and Information Literacy as a Complement to Legal Approaches

While legal frameworks provide the formal recognition and protection of digital rights, Media and Information Literacy (MIL) offers a complementary, people-centered dimension that focuses on individuals' ability to understand, exercise, and defend those rights in practice.

The literature increasingly recognizes that laws alone are insufficient to safeguard freedoms in digital spaces: citizens must also possess the critical skills to navigate information flows, detect

13 G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948).

14 Human Rights Council Resolution 32/13, U.N. Doc. A/HRC/32/L.20, at 48 (27 June 2016).

15 International Covenant on Civil and Political Rights, art. 17, 19, Dec. 16, 1966, 999 U.N.T.S. 171.

16 Human Rights Council Res. 32/13, U.N. Doc. A/HRC/32/L.20, at 48 (June 27, 2016). Rep. of the Spec. Rapport. on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, ¶ 1, U.N. Doc. A/HRC/29/32 (2015).

17 Council of Europe, Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States on a Guide to Human Rights for Internet Users (Apr. 16, 2014).

18 European Declaration on Digital Rights and Principles for the Digital Decade, 2023 O.J. (C 23) 1.

19 G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

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

misinformation, and assert their rights online (Livingstone & Bulger, 2014, pp. 321–325; Potter, 2013, pp. 45–50).[21]

Scholars in the field of MIL emphasize the interplay between regulation and empowerment, arguing that digital rights cannot be fully realized without informed and literate users. This dual perspective—law as a structural safeguard and MIL as a practical enabler—constitutes an emerging discourse in academic research, underscoring that the protection of rights in the digital age requires not only robust legal instruments but also educational strategies that strengthen resilience among individuals and communities.

Key Scholarly Contributions on Media and Information Literacy and Their Role in Advancing Digital Rights

Several authors regard Media and Information Literacy as a crucial tool for protecting fundamental rights and strengthening democratic values in the digital age. José Manuel Pérez Tornero, working with various collaborators, consistently emphasizes that MIL fosters civic responsibility, critical thinking, and what he describes as a "new humanism." For him, it serves not only as a defensive measure against misinformation and manipulation but also as an active means of promoting peace, tolerance, and freedom of expression.[22]

Howard Tumber and Silvio Waisbord similarly view MIL as a mechanism for empowering citizens to challenge human rights violations, resist disinformation, and reinforce democratic accountability (Tumber & Waisbord, 2017, pp. 10–11). While José Manuel Pérez Tornero focuses on education and value formation, Howard Tumber and Silvio Waisbord broaden the focus by highlighting the political dimension of MIL, emphasizing its role in empowering citizens to demand accountability, resist misinformation, and defend democratic rights (Tumber & Waisbord, 2017, pp. 10–12; 24–28).

Likewise, José Julio Fernández Rodríguez and Jackeline Argüello Lemus examine both the opportunities and risks that digital media pose to fundamental rights. Recognizing the importance of MIL, they argue that education alone cannot safeguard democracy and personal freedoms legal and policy frameworks must evolve alongside it (Fernández Rodríguez & Argüello Lemus, 2019, pp. 45–48; 72–75).

Despite these nuanced differences, a common thread runs through all these works: media literacy is inseparable from human rights protection in the digital age. Each scholar views MIL as a means of resisting manipulation, promoting democratic participation, and fostering resilience against extremism. Taken together, these authors offer complementary yet distinct perspectives on how MIL supports fundamental rights in the digital era.

While much of the literature highlights the transformative potential of MIL for the protection of human rights and fundamental freedoms, the discourse often overlooks the practical and structural challenges that hinder its effectiveness.

First, the *problem of unequal implementation* is crucial. While Torero's vision is inspiring, it risks remaining somewhat idealistic if MIL is confined solely to the educational domain. Given the unprecedented economic and political power of digital platforms in shaping the public sphere, MIL should not be viewed merely as an educational or cultural initiative, but also as a protective and juridical tool that operates alongside legal frameworks to ensure accountability, transparency, and the safeguarding of human rights.

---

[21] See also: UNESCO. (2013). *Global media and information literacy assessment framework: Country readiness and competencies*. https://unesdoc.unesco.org/ark:/48223/pf0000224655

[22] Pérez Tornero, J. M., & Varis, T. (2010). *Media literacy and new humanism*. UNESCO Institute for Information Technologies in Education. https://iite.unesco.org/pics/publications/en/files/3214678.pdf

Indeed, Tornero now engages precisely with this intersection, exploring how MIL can be integrated with law to create a more robust architecture for the protection of rights in the digital age. This evolution in his thinking is reflected in his shift from an early emphasis on MIL as a primarily educational and cultural project to a later recognition of its legal and policy dimensions within European digital governance (Pérez-Tornero & Martire, 2017). Second, although scholars such as Howard Tumber and Silvio Waisbord rightly emphasize that MIL fosters political participation and empowers citizens to defend human rights, their analysis does not fully address the problem of **global inequality of access**.

In Europe, MIL initiatives are often integrated into public education systems and policy frameworks, whereas in many other regions, MIL remains underdeveloped or limited to elite groups.[23]

This creates a paradox: those who most need MIL as a tool for empowerment and the protection of digital rights—communities subject to censorship, manipulation, or digital exclusion—are often the least likely to have access to it. In this sense, MIL risks becoming a privilege of advanced democracies rather than a universal safeguard for all citizens.

Third, and perhaps most fundamentally, *the literature continues to treat MIL primarily as a "pedagogical tool"* rather than recognizing it as a potential fundamental right in itself.[24] MIL is conceived as an adjunct to regulation rather than as a right that should be codified alongside freedom of expression, the right to information, and the right to education. The lack of recognition of MIL as a fundamental right remains a significant shortcoming. By contrast, if MIL were recognized as a normative right enforceable at the constitutional or international level, it could operate not only as an educational framework but also as a legal safeguard against disinformation, manipulation, and violations of digital rights.

---

[23] For evidence that MIL is comparatively more integrated into public education and policy frameworks in Europe while remaining patchy elsewhere, see: European Commission, Digital Education Action Plan (2021–2027) (setting out the EU strategy for digital and media competences) (*See*, Opinion of the European Committee of the Regions — Digital Education Action Plan 2021–2027, 2021 O.J. (C 300) 65). See also the Commission's requirement that Member States submit national reports on media-literacy measures under the Audiovisual Media Services Directive (*See,* Directive 2010/13/EU, of the European Parliament and of the Council of 10 March 2010 on the Coordination of Certain Provisions laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive), 2010 O.J. (L 95) 1 as amended by Directive 2018/1808, of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the Coordination of Certain Provisions laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) in view of Changing Market Realities, 2018 O.J. (L 303) 69), which documents national MIL initiatives across the EU. For an EU assessment of programme activity and coordination, see the European Digital Media Observatory (EDMO) report on media literacy in Europe (Goodman, E. (2021). Media literacy in Europe: Current programmes and initiatives. EDMO. https://edmo.eu/wp-content/uploads/2022/02/Media-literacy-in-Europe-and-the-role-of-EDMO-Report-2021.pdf). By contrast, UNESCO's global assessments and recent issue briefs document significant gaps in MIL policy and education internationally and provide global statistics on public exposure to disinformation and low fact-checking practices, demonstrating uneven uptake of MIL outside Europe. (UNESCO. (2013). Global media and information literacy assessment framework: Country readiness and competencies. https://unesdoc.unesco.org/ark:/48223/pf0000224655).

[24] UNESCO. (2013). *Global media and information literacy assessment framework: Country readiness and competencies* (pp. 17–20). https://unesdoc.unesco.org/ark:/48223/pf0000224655; Frau-Meigs, D. (2023). Declaration on Media and Information Literacy (pp. 21–24). UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000386080.locale=en; Carlsson, U. (Ed.). (2019). *Understanding media and information literacy (MIL) in the digital age: A question of democracy* (pp. 9–14). University of Gothenburg. https://www.gu.se/sites/default/files/2020-08/JMG_understanding-mil.pdf

From Traditional Rights to Digital Realities: Confronting the Gaps in the Court and Building New Concepts in the Regulatory Field

Building on the analysis of human rights frameworks and the identification of key gaps in the previous part, this section examines how these shortcomings have led to the emergence of new digital human rights. The unprecedented scale of digitalization—combined with algorithmic governance, transnational data flows, and the growing power of private platforms—has exposed the limitations of classical rights and prompted courts, legislators, and international bodies to adapt existing protections or create new ones.

Moreover, Media and Information Literacy (MIL) emerges as a crucial complementary mechanism within this legal and juridical context. While legal instruments provide formal protections, MIL empowers citizens to understand, claim, and exercise their rights in digital spaces, fostering civic responsibility, critical awareness, and democratic participation. Yet, its potential remains constrained by its current treatment as primarily an educational tool rather than a recognized instrument of legal protection. Integrating MIL into legal frameworks can enhance both the enforceability and the effectiveness of digital rights, bridging the gap between normative guarantees and practical empowerment.

In sum, this section explores how deficiencies in traditional frameworks have catalyzed the development of new rights, the challenges they face today, and the synergistic solutions that combine law and MIL to safeguard fundamental rights in the digital age.

Evolving Rights in the Digital Era: A New Birth through Case Studies

The emergence of digital rights has not occurred in a vacuum. Unlike traditional human rights, which were often proclaimed in foundational texts following revolutions or political declarations, digital rights have evolved gradually and reactively, shaped by the concrete challenges of the digital age.

Two main vectors explain this evolution. On the one hand, judicial cases in which courts were confronted with unprecedented issues such as mass data collection, algorithmic bias, restrictions on online freedom of expression, and both state and private surveillance, forcing them to adapt or reinterpret classical rights. On the other hand, Media and Information Literacy (MIL) initiatives, although primarily educational in nature, have played a crucial role in raising public awareness and empowering citizens to defend their fundamental rights in digital environments.

Thus, it is not through abstract proclamations but through engagement with real-world situations that new rights—such as the right to be forgotten, the right to algorithmic transparency, and the right to equitable access to information—have gradually emerged. This section therefore examines a series of emblematic cases that illustrate this process.

Decisions of the European and National Courts

Mario Costeja González v. Google Spain

In 1998, a Spanish newspaper published a legal notice concerning the auction of a property belonging to Mario Costeja González, following the seizure of assets due to outstanding debts. Years later, when searching for his name on Google, this outdated information still appeared prominently in the search results. Although the debt had long since been resolved, the

continued accessibility of this information harmed Mr. Costeja's reputation and his right to privacy.[25]

Mr. Costeja therefore lodged a complaint with the Spanish Data Protection Agency (AEPD), requesting that Google remove links to these outdated and prejudicial notices.[26] At the time, the applicable legal framework was the 1995 EU Data Protection Directive, which had been designed for traditional forms of data processing but did not explicitly regulate search engines or reflect the realities of the digital environment.[27]

The case ultimately reached the Court of Justice of the European Union (CJEU), which delivered a landmark judgment in 2014. The Court held that Google was indeed a data controller under the Directive and could therefore be held responsible for processing personal data through its indexing activities.[28]

More importantly, the Court articulated a new principle: individuals have the right to request the delisting of search results that are inaccurate, irrelevant, no longer relevant, or excessive in relation to the purposes of processing.[29]

This decision marked the birth of a new digital right the right to be forgotten. It demonstrated how traditional legal instruments, when confronted with new digital realities, must be reinterpreted and expanded by the judiciary. The ruling also highlighted the inherent tension between classical rights and emerging digital rights, particularly the delicate balance between the right to privacy and the right to freedom of information.

Delfi AS v. Estonia

Freedom of expression, as a classical right, is considered a pre-digital right under Article 10 of the European Convention on Human Rights.[30] It was originally designed to safeguard the ability to express oneself through the press and other traditional media within a stable legal framework. However, in today's digital environment, online platforms carry new risks, particularly regarding the publication of hate speech, cyberbullying, and other harmful content.

A clear illustration of this challenge is the Delfi case.[31] Delfi is a news portal that publishes political, economic, and social articles while allowing users to comment freely on the published content[32]. On one occasion, a woman became the target of defamatory comments posted on the site and decided to pursue legal action against Delfi.[33]

The European Court of Human Rights ultimately held that Delfi had a duty to moderate content proactively. The Court's judgment established a new rule—the proactive responsibility of online platforms to protect individuals from harmful content.[34] This case demonstrates how classical rights,

25 Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) & González, ECLI:EU:C:2014:317, ¶ 14 (May 13, 2014).

26 Ibid.

27 Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. (L 281) 31 (repealed 2018).

28 Case C-131/12, Google Spain, ECLI:EU:C:2014:317, ¶¶ 45–60.

29 Ibid., ¶¶ 89–99.

30 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), art. 10, Nov. 4, 1950, 213 U.N.T.S. 221.

31 Delfi AS v. Estonia, App. No. 64569/09 (June 16, 2015), https://hudoc.echr.coe.int/fre?i=001-155627

32 Ibid., ¶¶ 11–15.

33 Ibid., ¶¶ 16–31.

34 Ibid., ¶¶ 125–129.

when confronted with digital realities, can evolve into new digital rights, creating legal obligations for platforms to safeguard users while maintaining a balance with freedom of expression.

VZW Klimaatzaak v. Kingdom of Belgium & Others

In Belgium, the Youth for Climate movement mobilized thousands of young citizens around climate issues, relying heavily on social media platforms to inform, raise awareness, and organize public demonstrations.[35] As part of their legal actions, the activists sought access to specific environmental data essential to substantiate their arguments before the courts.

However, a significant portion of this information was not readily accessible online, creating a tangible obstacle to exercising the right of access to environmental information as guaranteed by the Aarhus Convention (1998).[36]

In June 2021, the Brussels Court of First Instance found that the Belgian State had failed to meet its obligations both regarding environmental protection and the online accessibility of information.[37] This ruling marked the emergence of a new right: the "online right to know." Nevertheless, this right remains fragmented, indirectly recognized, and has yet to be elevated to the status of an autonomous fundamental digital right.

This case illustrates the intersection of classical rights with digital realities, demonstrating how traditional legal frameworks must adapt to guarantee access to information in the digital age, and underscoring the role of courts in shaping the contours of emerging digital rights.

Media and Information Literacy (MIL) Case Studies

Case Study 1: The Papua New Guinea Experience in Social Media

Social media platforms are widely used by adolescents and young adults worldwide. While these platforms provide opportunities for social interaction and access to information, they also expose users to risks such as cyberbullying, misinformation, and online exploitation. Scholars in Media and Information Literacy (MIL) emphasize that education in digital literacy is essential to equip young people with the skills to navigate online environments responsibly and protect their personal information (Livingstone et al., 2017, Siraba, 2019).[38]

Encouraged by the insights provided through MIL, the government of Papua New Guinea implemented several regulatory measures to complement its educational strategy. Specifically, it restricted access to social media platforms for users under the age of 14 and introduced a mandatory identification system called SevisPass for those above this age threshold. This measure aims to protect young users while simultaneously promoting safer and more responsible participation in digital space.[39]

---

35 Wouters, R., & De Vydt, M. (2019, April 12). *Youth for climate Belgium: The narrative of an exceptional protest wave*. Mobilizing Ideas. https://mobilizingideas.wordpress.com/2019/04/12/youth-for-climate-belgium-the-narrative-of-an-exceptional-protest-wave/

36 Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (Aarhus Convention), June 25 1998, 2161 U.N.T.S. 447.

37 Civ. [Tribunal of First Instance] Brussel (4th ch.), June 17, 2021, English translation available at https://cdn.climatepolicyradar.org/navigator/BEL/2014/vzw-klimaatzaak-v-kingdom-of-belgium-others_50dbc50006ca324347b2de2119ec5a0b.pdf

38 UNESCO. (2013). *Global media and information literacy assessment framework: Country readiness and competencies* (pp. 17–20). https://unesdoc.unesco.org/ark:/48223/pf0000224655

39 Anadolu Agency. (2025, October 3). *Papua New Guinea Mulls age restrictions on social media*. https://www.aa.com.tr/en/asia-pacific/papua-new-guinea-mulls-age-restrictions-on-social-media/3706540

Overall, this case underscores the crucial role of Media and Information Literacy in addressing emerging challenges in the digital environment. It illustrates how MIL can inform policymaking, enhance online safety, and contribute to the recognition of new digital rights particularly the right to data protection and the right to responsible participation in digital spaces.

Case Study 2: False Information in the United Kingdom

In the United Kingdom the rapid proliferation of misinformation and disinformation on digital platforms has emerged as a major challenge, particularly affecting young people who often lack the critical skills needed to evaluate the credibility of online content. This situation threatens informed citizenship and democratic participation, as the spread of false or misleading information can distort public understanding and decision-making.

Recognizing the seriousness of this issue, the Guardian Foundation has actively promoted the integration of MIL into the national curriculum, advocating for media literacy to become a core competency at all stages of education.[40]

Its initiatives include comprehensive teacher training programs to equip educators with the tools to foster critical thinking, as well as student-centered projects such as the Media Literacy Ambassador Program, which empowers students to teach their peers how to identify misinformation, reinforcing critical skills through peer-to-peer learning.

Through these interventions, students and young citizens gain the ability to navigate complex digital spaces, assess the reliability of information, and engage responsibly in online environments. Importantly, this work has contributed to the recognition of new digital rights, including the right to reliable information and the right to informed participation, ensuring that citizens can meaningfully engage in democratic processes with awareness and critical judgment.

This case clearly illustrates how MIL can serve not only as an educational tool but also as a mechanism for the emergence and reinforcement of digital human rights, equipping individuals to exercise their rights and responsibilities effectively within the digital sphere.

Digital Human Rights: Practical Extensions of Existing Rights

With the technological revolution, a new category of digital rights has emerged to ensure that users are protected in the digital environment just as they are in their everyday lives. These rights aim to guarantee access to essential services on digital platforms—mirroring those in the real world—and include the right to digital inclusion, the right to protection from digital violence, and the right to be forgotten.

Right to Digital Inclusion

Being connected is essential to enhancing personal and societal well-being and enabling digital livelihoods. In this sense, every individual has the right to digital inclusion. This right ensures that all people have access to digital systems and online services—particularly persons with disabilities, the elderly, young people, and communities living in low-income regions.[41]

---

[40] Harrison, T., Polizzi, F., McLoughlin, S., Clark, C., Picton, I., & Bushby, R. (2024). *Educating and measuring news literacy and civic engagement in 9 to 11 year olds*. University of Liverpool; University of Birmingham; National Literacy Trust. https://www.jubileecentre.ac.uk/wp-content/uploads/2024/02/News-Literacy-and-Civic-Engagement-Full-Report-1st-Feb.pdf

[41] United Nations. (n.d.). Definition of digital inclusion. Retrieved June 7, 2025, from https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/general/Definition_Digital-Inclusion.pdf

In a dynamic and interconnected world, digital inclusion goes beyond the conventional focus on access and skills. It seeks to promote a holistic, action-oriented approach that remains responsive to evolving global trends.[42]

The European Commission, in its 2024 report, outlines a vision aimed at ensuring the protection of rights and freedoms while effectively upholding European values in an increasingly digital world. The European Union seeks to safeguard these values by fostering solidarity and digital inclusion through enhanced connectivity, digital education, freedom of choice, and a fair digital environment; by promoting participation in the digital public sphere; by increasing online safety, security, and empowerment particularly for young people; and by advancing sustainability.[43]

Right to Protection from Digital Violence

Digital violence refers to criminal and harmful behaviors committed through digital tools and spaces. It can take various forms of abuse and harassment against both children and adults, including cyberbullying[44], doxing[45], misinformation and deepfakes, and digital blackmail. The term digital violence is a relatively new term. It has been expressed in the last twenty years and constantly rising. There are several definitions of digital violence in use, depending on the types of digital harassment or forms of digital violence (Jevtić, 2020, p. 198). Digital violence also disproportionately affects women and girls, reflecting and reinforcing gender inequalities while exposing them to new forms of abuse in online spaces. The rise of digital technologies has become a double-edged sword for women's rights, impacting them more acutely than men and children.[46]

Right to Be Forgotten

In fact, the right to be forgotten certainly belongs to the field of rights attributable to privacy, which cannot be identified as a single and well-defined right, but rather as a complex of rights relating to the sphere of a person's private life (Maietta, 2020, p. 209).

The right to be forgotten is a modern legal concept that allows users to delete information, publications, images, or videos from digital spaces if they so choose. It first emerged in the jurisprudence of the Court of Justice of the European Union (CJEU) as an aspect of the right to privacy of data subjects in the context of personal data processing.[47]

---

[42] United Nations Development Programme. (2024). From access to empowerment: Digital inclusion in a dynamic world (p. 6). United Nations. https://www.undp.org/sites/g/files/zskgke326/files/2024-05/undp_digital_inclusion_in_a_dynamic_world.pdf

[43] *Commission Communication on the State of Digital Decade 2024*, COM(2024) 260 final (July 2, 2024). The Annex 4 dedicated to the monitoring of the European Digital Rights and Principles is published separately. *See*, *Commission Communication on the State of Digital Decade 2024*, annex 4, COM(2024) 260 final (July 2, 2024), https://ec.europa.eu/newsroom/dae/redirection/document/106722

[44] Cyberbullying — bullying that occurs through digital devices such as mobile phones, computers, and tablets.

[45] Doxxing — the act of publicly disclosing personally identifiable information about an individual or organization, usually via the Internet and without their consent.

[46] Zamfir, I., & Murphy, C. (2024). Cyberviolence against women in the EU (European Parliamentary Research Service Briefing, No. PE 767.146). European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPRS_BRI%282024%29767146_EN.pdf

[47] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) & González, ECLI:EU:C:2014:317 (May 13, 2014). See the section above dedicated to this decision.

Today, this right is framed and protected under the General Data Protection Regulation (GDPR), which mentions the "right to erasure" in the Article 17, balancing it with the right to freedom of expression and information, and the protection of personal data.[48]

Right to Algorithmic Transparency

Adopted by the European Union in March 2024, the AI Act is the world's first comprehensive legal framework regulating the development and use of artificial intelligence.[49] Its core objective is to ensure that AI systems operate in alignment with European values, fundamental rights, and human dignity. The Act introduces a risk-based approach, categorizing AI systems as unacceptable, high, limited, or minimal risk. Applications such as government social scoring, manipulative algorithms, and biometric surveillance in public spaces are strictly prohibited.[50]

For high-risk AI systems including those used in healthcare, education, recruitment, and law enforcement developers must comply with stringent obligations regarding transparency, human oversight, data quality, and accountability.[51] The Act also reinforces individuals' right not to be subjected to decisions made solely by automated systems without human intervention,[52] echoing Article 22 of the GDPR.[53] This Act therefore establishes a new digital right to algorithmic transparency, fairness, and human oversight in AI governance.

Right to Disconnect

The right to disconnect (also known as the "right to be offline") protects workers from the expectation of constant digital availability outside working hours. Formally recognized by the European Parliament Resolution of January 21, 2021, this right allows employees to disengage from emails, calls, and other work-related digital tools beyond their contractual working time.[54] Its purpose is to safeguard mental health, privacy, and work–life balance in an era defined by remote work and digital communication.

France was the first country to introduce this right through the El Khomri Law (Law No. 2016-1088)[55], followed by Spain (Royal Decree-Law 28/2020 on Remote Work)[56] and Italy (Law 81/2017)[57].

---

48 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) 43–44.

49 Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) 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) 2016/798 of the European Parliament and of the Council, 2024 O.J. (L 202) 1.

50 *Id.*, art. 5, 2024 O.J. (L 202) 51–53.

51 *Id.*, art. 6, 2024 O.J. (L 202) 51–54.

52 *Id.*, art. 8-9, art. 14, 2024 O.J. (L 202) 55–57, 60–61.

53 General Data Protection Regulation, 2016 O.J. (L 119) 39–40.

54 Resolution on the Right to Disconnect, Eur. Parl. Doc. 2019/2181(INL)) (2021).

55 Loi 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels [Law No. 2016-1088 of August 8, 2016 on Work, the Modernization of Social Dialogue and the Safeguarding of Career Paths], J.O., Aug. 9, 2016, p. 1 (Fr).

56 Remote Work Law (B.O.E. 2020, 77064) (Spain).

57 Legge, Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato [Law on Measures for the Protection of Self-Employed Work and to Encourage Flexible Work Arrangements], n. 81, 22 May 2017 (It.).

These laws require employers to establish clear internal policies on digital disconnection and to ensure that employees are not penalized for exercising this right. By recognizing the right to disconnect, European legislation has created a new form of digital labor right—one that ensures humane working conditions in the digital age and protects individuals' rights to rest, privacy, and psychological well-being.

Emergent Threats to Human Rights in Digital Spaces

Alongside the rapid advancement of digital technologies, new threats to digital human rights have emerged. While the Internet offers vast opportunities for the exercise of human rights, it also possesses features that make it a significant source of risks and threats to those very rights.[58]

Cyber Attacks

One of the most significant threats to digital human rights is cyber-attacks, which involve the exposure of personal data and user information. A cyber-attack represents a violation of privacy, in which hackers steal financial, medical, or personal details about users.

Attackers can range from individual hackers and activists to petty criminals, corporations, and even national governments.[59] To counter such threats, strong cybersecurity measures are essential.

Indeed, the term cybersecurity itself is defined by the European Union as "safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure.[60]"

Challenges to Digital Human Rights

Unfortunately, these new digital rights still face numerous challenges and threats that shape the ways in which users exercise their freedoms. In this context, challenges refer to systemic obstacles that require technological, regulatory, or societal solutions, while threats encompass the risks directed against the exercise of those very rights. There is a broad range of threats and challenges associated with the ongoing digitalization of traditional spheres of state and social life and the integration of smart technologies such as artificial intelligence and neural networks (Volodenkov & Fedorchenko, 2022, pp. 283-291).

Balance Between Digital and Real-Life Privacy

In today's hyperconnected environment, maintaining a balanced relationship between digital life and real-life privacy has become increasingly challenging. Constant engagement with digital platforms not only exposes individuals to information overload and continuous connectivity demands but also intensifies the production of personal data, which places additional pressure on the protection of digital rights and well-being (Turkle, 2015, pp. 3–28).

[58] Pajuste, T. (Ed.). (2022). Specific threats to human rights protection from the digital reality. Tallinn University. https://graphite.page/GDHRNet-threats-to-human-rights-protection/assets/documents/GDHRNet-ThreatsReport-EditedVolume.pdf

[59] Rossini, C., & Green, N. (2015). Cybersecurity and human rights. In *Webinar series training summaries*. Global Partners Digital. https://bestbits.net/wp-content/uploads/2015/04/Cybersecurity-and-Human-Rights-GCCS2015-Webinar.pdf

[60] European Commission. (2013, February 7). EU cybersecurity plan to protect an open Internet and online freedom and opportunity — cyber security strategy of the European Union: An open, safe and secure cyberspace [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_13_94

This continuous interaction with digital technologies inevitably generates a digital footprint comprising all traces of data that individuals leave behind through browsing, posting, location sharing, and platform interaction. This footprint, once accumulated and processed in the context of big data, can circulate across multiple domains such as commercial advertising, algorithmic profiling, and public or private databases, raising concerns about privacy, autonomy, and long-term control over personal information (Lin et al., 2022, pp. 1–2, 6–7).

Thus, the challenge of balancing digital and real-life privacy is inseparable from the issue of digital footprints: the more individuals depend on digital environments, the more personal data they generate, amplifying both the opportunities and risks inherent to contemporary digital ecosystems.

Digital Divide

The concept of the digital divide is generally defined as the gap between people who have access to information and communication technologies and those who do not (van Dijk, 2017, p. 1). It refers to limited access to the Internet, digital tools, and essential online services such as education, healthcare, and employment opportunities.

The digital divide became particularly evident during the COVID-19 pandemic, when Internet access became a necessity for education, work, and social interaction, millions of students and individuals were left without reliable Internet connections and access to online services.[61]

Gap Between Digital Laws and Real-World Realities

Despite significant legal progress—such as the EU's Artificial Intelligence Act[62], Digital Services Act[63], and Digital Markets Act[64]—a major challenge persists in the discrepancy between the legal framework and its practical enforcement. Many digital rights remain largely symbolic, as citizens often lack the digital literacy, institutional support, or procedural mechanisms necessary to exercise them effectively.

For instance, while users are legally entitled to transparency regarding algorithmic decision-making, few possess the technical capacity or access required to verify how these algorithms function in practice. Moreover, enforcement authorities (such as data protection agencies and digital regulators) frequently face limited resources and insufficient technological expertise, undermining their ability to monitor compliance or impose sanctions for violations. This has created an expanding gap between the normative promise of digital rights and their lived implementation.

The Growing Power and Responsibility of Private Actors

Perhaps the most complex challenge lies in the concentration of digital power in the hands of private corporations. Global technology platforms such as *Meta**, *Google*, *X* (*Twitter*), and *TikTok* have

[61] UNESCO. (2020, April 21). Startling digital divides in distance learning emerge [Press release]. https://www.unesco.org/en/articles/startling-digital-divides-distance-learning-emerge

[62] Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) 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) 2016/798 of the European Parliament and of the Council, 2024 O.J. (L 202) 1.

[63] 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.

[64] 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.

* 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.

become de facto regulators of online spaces, controlling access to information, moderating content, and shaping public discourse.

Their algorithms determine visibility, engagement, and even the contours of democratic participation—often without adequate transparency or accountability. Although recent laws, such as the Digital Services Act, attempt to rebalance this power by imposing stricter obligations on very large online platforms, the enforcement of these obligations remains uncertain.[65]

Moreover, the privatization of rights enforcement where companies decide what constitutes "harmful content" or "free expression" raises serious ethical and legal concerns about legitimacy and democratic control.[66] The key challenge today is to redefine a governance model that ensures private accountability within a framework of public responsibility, reinforcing the principle that digital rights are not corporate privileges but universal human rights.

Strengthening Digital Rights: Present Solutions and Strategies for Protecting the Digital Sphere

Within this general regulatory context, the law recognizes that individuals possess a fundamental right to information and communication. In today's world, the media, digital platforms, and regulation represent three interdependent domains.

The media require legal frameworks to regulate the circulation of information in order to safeguard public opinion and collective rights. Digital platforms, in turn, need a strict regulatory structure to protect users from fake news and deepfakes, to govern a new category of information disseminators (influencers and content creators) to regulate communication among users, to uphold freedom of expression, to ensure the accountability of emerging technologies, and to protect copyright and intellectual property on social networks.

Finally, it is through regulation and law that the media can play a fundamental role in facilitating access to legal information and raising public awareness of rights and responsibility. The law, in turn, requires a fair, transparent, and responsible media ecosystem and well-regulated platforms to popularize legislation, inform individuals of their duties, and disseminate newly adopted rules effectively.

Legal and Framework Solutions

The European Declaration on Digital Rights and Principles as a Foundational Pillar for Analysis

The rapid advancement of technology has necessitated the continuous adaptation of various laws and regulatory approaches. Legislators, for their part, often struggle to keep pace with users' growing agency and acts of digital appropriation, sometimes overlooking or diminishing legitimate user claims to control how their data and digital interactions are used. Consequently, a range of legal frameworks have been updated to strengthen the protection of digital human

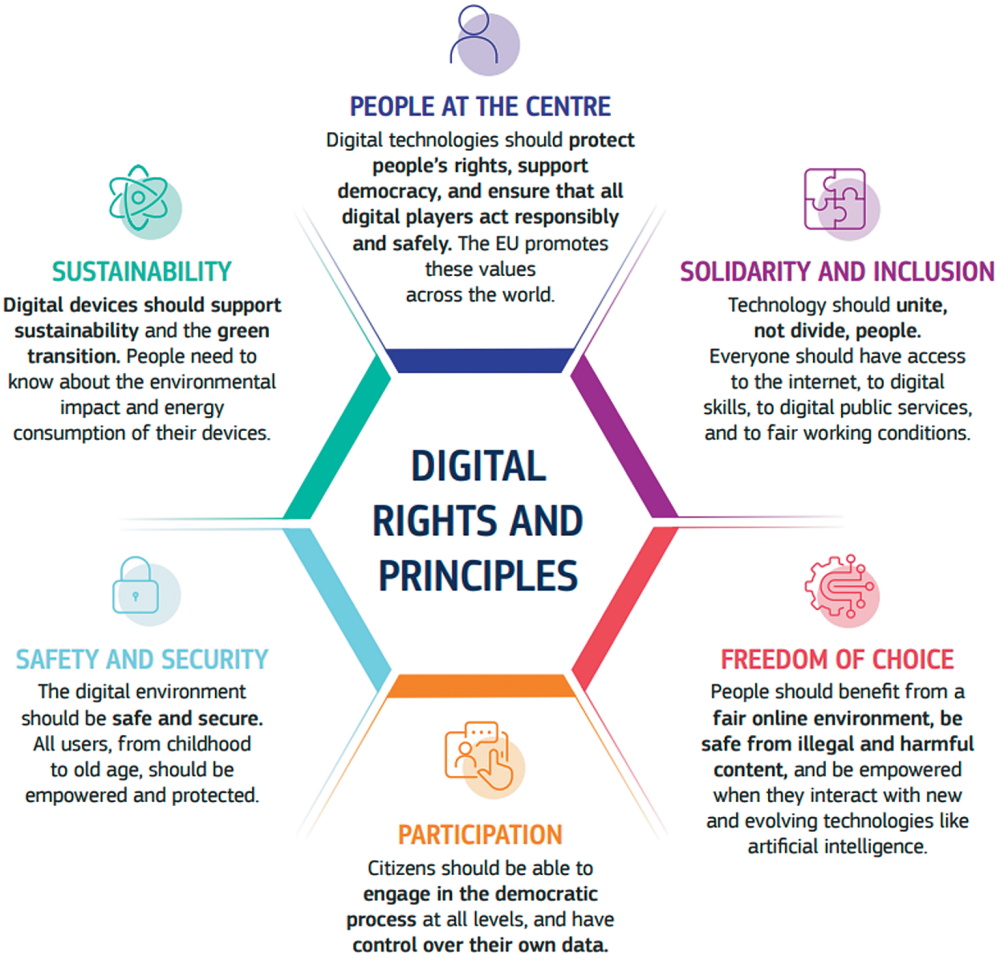
[65] Regulation 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), art. 33, 38, 40, 42, 2022 O.J. (L 277) 63–64, 69, 70–72, 73–74.

[66] Ortutay, B. (2025, January 9). *Meta* eases some restrictions on speech targeting transgender people, immigrants, and other groups after review tied to elections*. Associated Press. https://apnews.com/article/meta-facebook-hate-speech-trump-immigrant-transgender-41191638cd7c720b950c05f9395a2b49

* 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.

Figure 1

The six Chapters of the European Declaration on Digital Rights and Principles for the Digital Decade



Note. Reproduced from the European Commission's study to support monitoring of the Declaration on Digital Rights and Principles.[67]

rights, among which the European Declaration on Digital Rights stands out as one of the most significant.[68]

Adopted in 2022, the European Declaration on Digital Rights represents a landmark policy instrument that embodies the EU's vision of a human-centric digital transformation. It reaffirms the EU's commitment to ensuring that the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union[69] and in international human rights instruments are effectively upheld in the digital realm.

[67] European Commission. (2025). *Study to support the monitoring of the Declaration on Digital Rights and Principles : Final Report* (2nd ed., p. 28). European Union. https://doi.org/10.2759/0915515

[68] European Declaration on Digital Rights and Principles for the Digital Decade, 2023 O.J. (C 23) 1.

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

The Declaration is built around six core principles: placing people at the center of the digital transformation; promoting solidarity and inclusion; ensuring freedom of choice; fostering participation in the digital public sphere; enhancing safety, security, and empowerment; and advancing sustainability in the digital age.

Following the adoption of the European Declaration on Digital Rights and Principles, scholars and institutions across Europe welcomed it as a significant milestone in embedding human-centric values within the digital transformation. Experts in digital constitutionalism, such as Cristina Cocito and Paul De Hert, praised its transformative vision and its potential to shape governance in the digital domain (Cocito & De Hert, 2023). Policy analyst Anna Pingen viewed it as a strategic framework designed to inspire legislation and policymaking throughout the EU.[70]

While the European Economic and Social Committee (EESC) acknowledged the Declaration's value,[71] it also pointed to challenges in implementation and public awareness. Critical commentators cautioned against placing excessive responsibility on individuals without providing sufficient institutional safeguards. Overall, the Declaration has been positively received for articulating a shared vision of Europe's digital future, while underscoring the need for stronger enforcement mechanisms and inclusive implementation.

Sporadic Constitutional Recognition of Digital Rights

The constitutional recognition of digital rights by a few European jurisdictions represents a fundamental advancement in safeguarding human rights in the digital era.

For instance, the Portuguese Constitution protects the right to privacy under Article 26, which prohibits arbitrary interference with personal data.[72] Moreover, under Law No. 58/2019, Portugal has enshrined the rights to data protection and access to digital information, providing citizens with strong legal remedies against excessive surveillance or misuse of personal data.[73]

In Spain, Organic Law 3/2018, following the constitution, establishes key digital rights, including the rights to privacy, security in digital interactions, digital identity, and the right to disconnect.[74] These rights are closely linked to constitutional protections, creating a robust legal framework for their enforcement.

---

[70] Pingen, A. (2022, February 22). Commission proposes Declaration on European Digital Rights and Principles. Eucrim. https://eucrim.eu/news/commission-proposes-declaration-on-european-digital-rights-and-principles/

[71] Opinion of the European Economic and Social Committee on (a) 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — Establishing a European Declaration on Digital rights and principles for the Digital Decade' and on (b) 'Digital rights and principles'. O.J. (C 365) 13.

[72] Constitution of the Portuguese Republic art. 26 (Rev. 2005), English translation available at https://www.parlamento.pt/sites/EN/Parliament/Documents/Constitution7th.pdf

[73] Law No. 58/2019, of August 8, on the implementation in the national legal order of Regulation (EU) 2016/679 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, Diário da República [D.R.] No. 152/2019 — Série I of 8 Aug. 2019 (Portugal). Available at https://diariodarepublica.pt/dr/en/detail/act/58-2019-123815982

[74] Constitución Española, art. 18.4, B.O.E. n. 311, Dec. 29, 1978 (Spain). See about interpretation of Article 18.4 as a basis for data protection law: GDPR Hub. (n.d.). *Data protection in Spain*. Retrieved July 7, 2025 from https://gdprhub.eu/Data_Protection_in_Spain. This provision should be read in conjunction with Organic Law 3/2018, see: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales [Organic Law on on Personal Data Protection and Guarantee of Digital Rights], (B.O.E. 2018, 294) (Spain).

Similarly, the Constitution of the Republic of Estonia, in Article 43, guarantees access to the internet and secure digital identity as integral components of its constitutional and digital governance framework.[75]

The constitutional codification of digital rights ensures legal stability, enforceability, and resilience in the face of technological evolution, providing a solid foundation upon which legislative measures, regulatory frameworks, and educational initiatives can build to protect citizens effectively in the rapidly evolving digital landscape.

Educational Safeguard for Digital Human Rights: Media and Information Literacy Solutions

In an era where digitalization marks a new stage of human evolution, media and information literacy serves as a crucial tool for protecting digital human rights. It empowers users to understand and critically assess information circulating in digital spaces, to distinguish between reliable and false content, and to recognize their responsibilities within the online environment.

Many scholars emphasize that Media and Information Literacy movement functions not only as an educational instrument but also as a form of empowerment, enabling citizens to recognize and resist disinformation, online manipulation, and violations of privacy[76]. Within the framework of digital human rights, MIL should be a preventive social mechanism that complements legal and regulatory measures by fostering informed, autonomous, and resilient digital citizens capable of asserting their rights within complex online ecosystems.

The protection of digital human rights requires the joint operation of law and MIL. Law provides the formal rights and standards, while MIL equips individuals with the competencies to understand, exercise, and defend these rights online. Without Media and Information Literacy, legal protections remain abstract; without law, literacy alone cannot ensure enforcement. Together, they establish a holistic framework that empowers citizens and safeguards human rights in the digital environment.

Conclusion

As the digital world continues to evolve and assumes a central role in the dissemination of information and the fulfilment of everyday needs, it simultaneously presents major challenges for fundamental rights. On the one hand, it enables unprecedented forms of expression, civic participation, and access to information; on the other hand, it has become a space marked by troubling phenomena such as disinformation, hate speech, and violations of users' privacy.

To safeguard these digital rights, legal protections must be effectively enforced, including robust data protection, the security of digital transactions, laws imposing stricter age restrictions to limit minors' exposure to harmful content on social media platforms, and the promotion of social justice.

Furthermore, high levels of education in media and information literacy enhance users' ability to critically assess media content, while awareness-raising campaigns can strengthen public understanding of global challenges and foster a more informed and resilient digital society.

---

[75] Constitution of the Republic of Estonia art. 43 (1992, as amended 2015), available at https://www.riigiteataja.ee/en/eli/521052015001/consolide

[76] For instance, Kostas Karpouzis argues that MIL is essential for individuals to critically engage with information, navigate the digital environment safely, and counter both disinformation and hate speech. Karpouzis, K. (2024). *Media and information literacy as a fundamental human right*. Preprints. https://doi.org/10.20944/preprints202408.2242.v1

References

1. Balkin, J. M. (2004). Digital speech and democratic culture: A theory of freedom of expression for the information society. New York University Law Review, 79(1), 1–55. https://nyulawreview.org/issues/volume-79-number-1/digital-speech-and-democratic-culture/
2. Bygrave, L. A. (2002). Data protection law: Approaching its rationale, logic and limits. Kluwer Law International.
3. Cocito, C., & De Hert, P. (2023). The transformative nature of the EU Declaration on Digital Rights and Principles: Replacing the old paradigm (normative equivalency of rights). *Computer Law & Security Review, 50*, Article 105846. https://doi.org/10.1016/j.clsr.2023.105846
4. De Gregorio, G. (2022). *Digital constitutionalism in Europe: Reframing rights and powers in the algorithmic society*. Cambridge University Press. https://doi.org/10.1017/9781009071215
5. Domaradzki, S., Khvostova, M., & Pupovac, D. (2019). Karel Vasak's generations of rights and the contemporary human rights discourse. *Human Rights Review, 20*(4), 423–443. https://doi.org/10.1007/s12142-019-00565-x
6. Dowd, R. (2022). *The birth of digital human rights: Digitized data governance as a human rights issue in the EU*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-82969-8
7. Fernández Rodríguez, J. J., & Argüello Lemus, J. (2019). Digital media and the challenges for fundamental rights. In A. Berea (Ed.), *A Complex Systems Perspective of Communication from Cells to Societies* (pp. 1–14). IntechOpen. https://doi.org/10.5772/intechopen.82435
8. Floridi, L. (2013). *The ethics of information*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199641321.001.0001
9. Floridi, L. (2016). *The fourth revolution: How the infosphere is reshaping human reality*. Oxford University Press.
10. Hildebrandt, M. (2015). Smart Technologies and the End(s) of Law. Edward Elgar Publishing. https://doi.org/10.4337/9781849808774
11. Hildebrandt, M. (2020). *Law for computer scientists and other folk*. Oxford University Press. https://doi.org/10.1093/oso/9780198860877.001.0001
12. Jevtić, R. (2020). Digital violence and the role of different factors in its prevention. *Zbornik radova Pedagoškog fakulteta, Užice, 23*(22), 195–212. https://doi.org/10.5937/ZRPFU2022195J
13. Katyal, S. K. (2005). Privacy vs. piracy. *Yale Journal of Law & Technology, 7*, 222–345.
14. Lin, X., Ju, F., Zhao, C., Feng, X., & Luo, D. (2022). The wave of the digital economy: The conflict and balance between data sharing and personal privacy. *SHS Web of Conferences, 148*, Article 03055. https://doi.org/10.1051/shsconf/202214803055
15. Livingstone, S., & Bulger, M. (2014). A global agenda for children's rights in the digital age. *Journal of Children and Media, 8*(4), 317–335. https://doi.org/10.1080/17482798.2014.961496
16. Livingstone, S., Mascheroni, G., & Staksrud, E. (2017). European research on children's internet use: Assessing the past and anticipating the future. *New Media & Society, 20*(3), 1103-1122. https://doi.org/10.1177/1461444816685930
17. Maietta, A. (2020). The right to be forgotten. *Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito*, *12*(2), 207–226. https://doi.org/10.4013/rechtd.2020.122.03
18. Pérez Tornero, J. M., Orozco, G., & Hamburger, E. (Eds.). (2020). Media and information literacy in critical times: Re-imagining learning and information environments. Autonomous University of Barcelona; The Arab Academy for Science.

19. Pérez-Tornero, J. M., & Martire, A. (Eds.). (2017). Educación y nuevos entornos mediáticos. [Education and new media environments]. Editorial UOC.
20. Potter, W. J. (2013). *Media literacy* (6th ed.). Sage Publications.
21. Razmetaeva, Y., Barabash, Y., & Lukianov, D. (2022). The concept of human rights in the digital era: Changes and consequences for judicial practice. *Access to Justice in Eastern Europe, 3*(15), 41–56. https://doi.org/10.33327/AJEE-18-5.3-a000327
22. Schwartz, P. M. (2025). Spiros Simitis as Data Protection Pioneer. *George Washington Journal of Law & Technology*, *1*(1), 102–118.
23. Simitis, S. (1999). Reconsidering the premises of labour law: Prolegomena to an EU regulation on the protection of employees' personal data. *European Law Journal, 5*(1), 45–62. https://doi.org/10.1111/1468-0386.00065
24. Siraba, A. (2019). Cyberbullying and online harassment among Facebook users in Papua New Guinea. *Contemporary PNG Studies, 30*, 42–50.
25. Turkle, S. (2015). Reclaiming conversation: The power of talk in a digital age. Penguin Press.
26. Tumber, H. & Waisbord, S. (2017). Media and human rights: Mapping the field. In H Tumber, & S. Waisbord, (Eds.), *The Routledge companion to media and human rights* (pp. 1–14). Routledge.
27. van Dijk, J. A. G. M. (2017). Digital divide: Impact of access. In The International Encyclopedia of Media Effects. Willey. https://doi.org/10.1002/9781118783764.wbieme0043
28. Volodenkov, S., & Fedorchenko, S. (2022). Digital human rights: Risks, challenges, and threats of global socio-political transformations. *Cuestiones Constitucionales*, *1*(46), 279–316. https://doi.org/10.22201/iij.24484881e.2022.46.17057
29. Wuermeling, U. (1998). The first national multimedia law — How Germany regulates online services and the internet. *Computer Law & Security Report, 14*(1), 41–44. https://doi.org/10.1016/S0267-3649(97)88076-4

Information about the author:

Nour Nfissi — L.L.B, LL.M. of Business and Digital Law (Faculty of Law, University Sidi Mohamed Ben Abdelah, Morocco), Ph.D. student, Department of Journalism and Communication Sciences, Faculty of Communication Studies, Autonomous University of Barcelona (Barcelona, Spain), with an international co-supervision with the Faculty of Law, Sidi Mohamed Ben Abdelah, Fez, Morocco.
nournfissi41@gmail.com
ORCID: https://orcid.org/0009-0003-0731-5718

Сведения об авторе:

Нфисси Н. — бакалавр права, магистр бизнес-права и цифрового права (юридический факультет, Университет Сиди Мохаммед бен Абделлах, Марокко), аспирант, кафедра журналистики и коммуникационных наук, факультет коммуникационных исследований, Автономный университет Барселоны (Барселона, Испания) в рамках международного научного руководства совместно с юридическим факультетом Университета Сиди Мохаммеда бен Абделлаха, Фес, Марокко.
nournfissi41@gmail.com
ORCID: https://orcid.org/0009-0003-0731-5718

https://doi.org/10.38044/2686-9136-2025-6-13

ЭССЕ

ЦИФРОВОЕ РОДИТЕЛЬСТВО: ТЕХНОЛОГИИ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В МЕХАНИЗМЕ РЕАЛИЗАЦИИ ПРАВА РОДИТЕЛЕЙ НА ОБЩЕНИЕ С РЕБЕНКОМ

Е. В. Ерохина

Оренбургский государственный университет
460018, Россия, Оренбург, пр. Победы, 13

Аннотация

Цифровые технологии и искусственный интеллект находят все более широкое применение в различных сферах жизни и могут быть использованы не только для решения текущих утилитарных и ныне уже общеизвестных задач, которые обуславливают написание компьютерного кода, но и в качестве технических гарантий реализации прав детей и родителя, проживающих раздельно, на общение. Цель исследования сводится к тому, чтобы описать концептуальные рамки известной за рубежом модели «виртуального родительства» как дополнительного способа общения ребенка с родителем, проживающим отдельно, и обосновать возможность применения данного способа построения семейных отношений и их соответствующей регламентации в конфликтной стадии в рамках российского правового поля. Для достижения данной цели с применением формально-юридической методологии автором представлен сравнительно-правовой обзор использования современных зарубежных приложений (компьютерных программ), позволяющих обеспечить нейтральную цифровую среду для такого общения. В ходе исследования также в необходимой мере были проанализированы труды из иных областей, прежде всего психологии и социологии, что обусловлено необходимостью «тонкой настройки» межличностных отношений в рамках изучаемого сложнейшего социального института. В эссе анализируется и обосновывается необходимость создания и внедрения приложения, которое могло бы иметь условное название «Территория семейного общения и доверия» как государственной онлайн-платформы с искусственным интеллектом, позволяющей осуществлять виртуальное общение ребенка и родителя. Изучение правоприменительной практики демонстрирует, что, несмотря на предоставление современными правопорядками родителю, проживающему отдельно, права на общение и участие в воспитании ребенка, реализация этого права при сопротивлении второго родителя затруднительна, а в ряде случаев и невозможна. В работе отстаивается точка зрения о том, что доступ к платформе в некоторых случаях должен предоставляться государственным органам (например, судебным приставам), а цифровые отчеты должны получать юридическую силу доказательств. Автор приходит к выводу, что в цифровую эпоху необходимо использовать возможности технологий и искусственного интеллекта для институциональной поддержки семьи и общества, в том числе при реализации права на семейное общение и для профилактики потенциальных злоупотреблений со стороны одного из родителей.

Ключевые слова

цифровые технологии, искусственный интеллект, семейное право, развод, наилучшие интересы ребенка, право родителя на общение и воспитание

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.
Для цитирования	Ерохина, Е. В. (2025). Цифровое родительство: технологии и искусственный интеллект в механизме реализации права родителей на общение с ребенком. *Цифровое право, 6*(3), 34–66. https://doi.org/10.38044/2686-9136-2025-6-13

Поступило: 01.07.2025; принято в печать: 21.08.2025, опубликовано: 30.09.2025

ESSAYS

DIGITAL PARENTING: TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE IN THE REALIZATION OF PARENTS' RIGHTS TO COMMUNICATE WITH THE CHILD

Elena V. Erokhina

Orenburg State University
13, Pobedy Ave., Orenburg, Russia, 460018

Abstract

Digital technologies and artificial intelligence, which are increasingly used to address general tasks across all areas of society, may also serve as technical means for enforcing the rights of children and separately-living parents to maintain contact with one another. Delineating the internationally recognized conceptual model of "virtual parenting" as an additional means of communication between a child and a parent residing separately, the study substantiates the possibility of applying such a model to the construction of family relationships and corresponding regulation at the conflict stage within the Russian legal framework. Using a formal legal methodology, the author provides a comparative legal review of the application of contemporary foreign applications (software programs) designed to ensure a neutral digital environment for such communication. Due to the need for "fine-tuning" interpersonal relationships within the framework of the family, representing one of the most complex social institutions, works from other disciplines—primarily psychology and sociology—were also analyzed. The need to develop and implement a state-run online platform—provisionally entitled "The Territory of Family Communication and Trust"—powered by artificial intelligence for enabling virtual communication between a child and a parent is outlined. An examination of law enforcement and judicial practice demonstrates that, despite modern legal systems formally granting a separately residing parent the right to communicate with—and participate

in the upbringing of—a child, in cases of resistance by the other parent, the practical realization of this right becomes difficult and, in some cases, impossible. It is argued that, in certain cases, access to such a platform should be granted to state authorities (for example, bailiffs), and that digital reports generated by the platform should be endowed with evidentiary legal force. It is concluded that, in the digital era, it is necessary to leverage the capabilities of technologies and artificial intelligence to support family and society institutionally through a more flexible mechanism for enforcing the right to family communication and preventing potential abuses by one of the parents.

Keywords

digital technologies, artificial intelligence, family law, divorce, best interests of the child, right to communication and upbringing

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Erokhina, E. V. (2025). Digital parenting: Technologies and artificial intelligence in the realization of parents' rights to communicate with the child. *Digital Law Journal, 6*(3), 34–66. https://doi.org/10.38044/2686-9136-2025-6-13

Submitted: 1 July 2025, accepted: 21 Aug. 2025, published: 30 Sep. 2025

Постановка проблемы

Цифровые технологии уже создали новый мир социальных коммуникаций, особенно для молодежи, активно использующей текстовые сообщения, электронную почту, социальные мессенджеры и иные инструменты цифрового общения. Поскольку технологии все больше интегрируются в повседневную жизнь и сферу коммуникации, то важно изучить возможности, которые они предоставляют членам семьи, в том числе для сохранения родственных отношений с ребенком после расторжения брака.

Сохранение эмоциональных родственных отношений между родителями и детьми после расторжения брака является достаточно сложной и многогранной проблемой как с точки зрения психологии, социологии, так и с точки зрения права. Одной из значимых проблем, стоящих перед семейным правом, является эффективное поддержание возможности общения ребенка с родителем, проживающим отдельно.

В контексте развития цифровых технологий наше исследование фокусируется на способность современного законодательства обеспечить права несовершеннолетнего и отдельно проживающего родителя на общение в краткосрочный период и поддержании семейно-родственных связей в долгосрочной перспективе за счет имплементации известной зарубежным правопорядкам модели «виртуального родительства» в российское правовое пространство. В связи с отсутствием в российском законодательстве прямых запретов на установление в судебном порядке графика онлайн-общения в работе обосновывается целесообразность разработки государственной цифровой платформы для реализации закрепленного в отечественном законодательстве принципа паритета родительских прав и права ребенка на полноценное общение с обоими родителями.

Цель исследования заключается в обосновании возможности использования модели «виртуального родительства» при должной адаптации к правовой системе России через регламентацию отношений по имплементации цифровых технологий для соблюдения прав членов семьи после расторжения брака.

Исследование базируется на методологическом принципе междисциплинарности, что отражает современную тенденцию интеграции различных областей научного знания. В работе рассматриваются юридические, социологические, психологические и технологические аспекты проблемы. Данный подход позволяет избежать односторонности и создать многомерную модель анализа проблематики реализации родительских прав разведенных родителей в цифровую эпоху. Применяются формально-юридический и сравнительно-правовой методы для выявления общих и специфических черт правового регулирования «виртуального родительства» в различных правовых системах. Особую методологическую ценность представляет компаративистский анализ судебной практики, позволяющий идентифицировать правоприменительные паттерны и юридические коллизии в исследуемой сфере. В работе используется технологический детерминизм как методологическая установка, предполагающая существенное влияние технологий на трансформацию социальных институтов и правовых механизмов. Благодаря такому подходу можно экстраполировать существующие тенденции и формулировать обоснованные прогнозы относительно будущих изменений в сфере реализации семейных прав.

Расторжение брака и реализация права на общение ребенка с родителем, проживающим отдельно

Первое предположение: трансформация, а не прекращение, соответствует современному взгляду на последствия расторжения брака для семейной системы

С теоретической точки зрения расторжение брака долгое время рассматривалось как исключительно негативное событие, которое приводит к дезорганизации членов семьи и разрушает семейную жизнь. Исследуя парадигму кризиса семьи, ученые отмечают, что он приводит к фрустрации привычных способов функционирования семьи и к невозможности справиться с новой ситуацией, используя старые модели поведения (Olifirovich, 2015, p. 25). Гипотеза нестабильности предполагает, что развод является стрессом для родителей и детей, и может негативно повлиять на развитие ребенка. Действительно, лица, находящиеся в процессе развода, часто испытывают эмоциональное напряжение и трудности в поддержании позитивных отношений другом с другом и с детьми. Многочисленные исследования устанавливали взаимосвязь факта развода родителей с ухудшением эмоционального и психологического благополучия детей, проблемами с поведением, более низкими образовательными достижениями, ухудшением родительского ухода, а также сокращением экономических ресурсов и снижением уровня жизни (Ermilova, 2015; Härkönen et al., 2017; Perkins, 2019; Raley & Sweeney, 2020).

Впрочем, необходимо признать: в современном обществе стремление индивидов к достижению баланса между личной автономией и поиском долгосрочных межличностных отношений привело к нормализации развода как сложной взаимосвязи аксиологических ориентиров. Исследования в России подтверждают увеличение социальной приемлемости разводов (Sinelnikov, 2023, p. 75). В современной научной парадигме применительно к полной семье развод — это изменение, а не распад системы семейных отношений. В семье

взрослые выполняют одновременно и супружеские (жены или мужа), и родительские (матери или отца) роли; в ситуации развода происходит модификация набора ролей субъектов семейных отношений: супружеские роли формально исчезают, а родительские сохраняются (Kletsina, 2015, p. 35). Исходя из данной трактовки, можно сделать вывод о том, что развод приводит не к дезорганизации, а к трансформации семейных отношений, в которых членам семьи приходится приспосабливаться к новой ситуации. Исследования показывают, что не сам факт расторжения брака наносит вред развитию несовершеннолетних, а постоянная враждебность между бывшими супругами: «дети разведенных родителей, которые прекратили ссориться, были так же хорошо приспособлены, как и те, кого воспитывали родители в успешных браках» (Hetherington & Stanley-Hagan, 2002, p. 296). Хотя развод родителей создает определенные трудности, дети, получающие стабильную эмоциональную поддержку от родителей, как правило, легче адаптируются к этим изменениям и развивают здоровое чувство уверенности и независимости. В целом, крайне важно, чтобы родители продолжали уделять своим детям все свое внимание после развода, поддерживали хорошее общение и создавали благоприятную среду, чтобы дети могли развиваться, несмотря на трудности, с которыми они сталкиваются (Safira & Rozatul, 2025, p. 92).

В этом ключе гипотеза нестабильности семьи сфокусировалась на сохранении семейных уз между бывшими ее членами. Действительно, одной из серьезных проблем, с которой сталкиваются родители и дети после расторжения брака, является создание условий, позволяющих нормализировать взаимодействие между бывшими супругами для воспитания ребенка и сохранить родственные отношения между детьми и родителем, проживающим отдельно.

Мы не можем предотвратить разводы, которые в современном обществе пусть и не считаются нормой, но и не выходят за рамки обыденной жизни. Однако одна из задач государства и общества — минимизация негативных последствий расторжения брака, и прежде всего для ребенка.

Второе предположение: сохранение родительской вовлеченности в воспитание и общение с ребенком позволяет обеспечить его наилучшие интересы

Принцип обеспечения наилучших интересов ребенка входит в число общих принципов Конвенции ООН о правах ребенка[1], однако «его четкого определения не существует» (Pavlenko, 2021, p. 77). Конвенция в том числе закрепляет право ребенка знать своих родителей и право на их заботу (п. 1 ст. 7); право детей, разлученных с одним или обоими родителями, поддерживать личные отношения и прямые контакты с обоими родителями на регулярной основе, если это не противоречит наилучшим интересам ребенка (п. 3 ст. 9); общую и одинаковую ответственность за воспитание детей обоих родителей (ст. 18)[2]. Презумпция родительского участия признает важность поддержания отношений между детьми и обоими родителями, независимо от их семейного статуса, и основана на понимании того, что если не доказано иное, в наилучших интересах ребенка поддерживать отношения с обоими родителями.

В России расторжение брака супругами, независимо от процентного соотношения гендерного распределения решений суда об определении места жительства ребенка, приводит к тому, что один из родителей приобретает статус родителя, проживающего *отдельно от ребенка*, а другой — статус родителя, *проживающего с ребенком*.

[1] Конвенция о правах ребенка (одобрена Генеральной Ассамблеей ООН 20 ноября 1989 г.; вступила в силу для СССР 15 сентября 1990 г.). Ведомости Съезда народных депутатов СССР и Верховного Совета СССР, 1990, № 45.

[2] Там же.

Отметим, что за последние десятилетия правовая структура родительских ролей существенно изменилась: права отцов стали защищаться, подчеркивается роль отца в общем развитии детей, выдвигается на первый план его взаимодействие с ребенком: все больше детей общаются со своими отцами, и все больше детей поддерживают хорошие отношения со своими отцами (Van Spijker, 2022, p. 446), отмечается увеличение вовлеченности отцов в воспитание детей (Haux & Platt, 2021, p. 152), что число отцов, воспитывающих детей, увеличилось (Cancian et al., 2014, p. 1384), а в России «вектор судебной практики, возможно, постепенно меняется в сторону отцов» (Pyankova, 2025, p. 62).

Во многих странах защита наилучших интересов ребенка как ведущий юридический принцип влияет на решение вопросов обеспечения общения ребенка с отдельно проживающим родителем, даже в случаях если отношения между родителями характеризуются конфликтами (Zartler, 2021, p. 306).

В зарубежных исследованиях продемонстрирована прямая зависимость формирования родственных отношений во взрослом периоде жизни ребенка от степени и количества участия родителя, проживающего отдельно, в воспитании детей: низкий уровень участия разведенных отцов в жизни детей приводит к уменьшению частоты их общения во взрослой жизни (Arditti & Keith, 1993, p. 670), дети, которые в юности были вовлечены в межличностный конфликт между родителями высокого уровня, во взрослом возрасте были менее близки со своими отцами (Spaan et al., 2022, p. 1204), конфликт между родителями отрицательно влияет на родительское сотрудничество (Toews & McKenry, 2001, p. 71), что может сказаться на общении родителя, не проживающего в семье с детьми. Маттейс Калмейн утверждает, что одной из причин неравенства родителей после развода являются конфликт лояльности и эффект компенсации (Kalmijn, 2013, p. 896). Исследование, проведенное сотрудниками Университета Миколаса Ромериса, подтверждает, что родитель, проживающий с ребенком после развода, действует вопреки наилучшим интересам ребенка, отрицая его неотъемлемое право на воспитание и общение с обоими родителями (Kairiene et al., 2022). Таким образом, благополучие ребенка во многом зависит от участия родителя, проживающего отдельно, в его воспитании и общении с ним и после расторжения брака.

Наиболее заметным способом обеспечения участия обоих родителей в воспитании ребенка и его общения с ними обоими стало введение в некоторых зарубежных странах института совместной («физической») родительской опеки (*joint physical custody*), которая была известна в странах общего права довольно давно, а с недавних пор устанавливается в качестве дефолтного режима опеки отдельными штатами в США. Данное обстоятельство не могло не способствовать росту интереса правоведов к изучению данного института. Так, можно выделить проведенное комплексное исследование способов правового закрепления в 36 западных странах данной формы опеки в контексте реализации права ребенка на общение (Bjarnason & Amarsson, 2011, pp. 483–488), исследование в 37 юрисдикциях Северной Америки и Европы на предмет соответствия данной формы опеки наилучшим интересам ребенка (Steinbach et al., 2021, pp. 151–154) и сравнительное исследование совместной опеки, которую осуществил в диссертационном исследовании Марк Поли[3]. Отметим, что термин, означающий совокупность родительских прав и обязанностей, как и его содержание зависит от установленного правопорядка, основанного на исторических и национальных традициях

[3] Комплексный анализ способов закрепления форм совместной опеки в Бельгии, Англии и Уэльсе, а также в Италии проведен в докторской диссертации Марко Поли «Влияние наилучших интересов ребенка на совместное воспитание детей и совместную опеку» (Poli, 2023).

стран[4]. В контексте нашей темы интересно такое право родителей, как "*rights of custody*" (дословно «право опеки», что соответствует официальному переводу Конвенции о гражданско-правовых аспектах международного похищения детей 1980 г.)[5]. Данная конвенция впервые закрепила понятие и определение прав родительской опеки и прав доступа как составляющих понятия родительских прав и обязанностей. Разработчики Конвенции прямо указали на автономный по отношению к национальным законодательствам характер толкования указанных дефиниций «для целей Конвенции», отметив, что «ключевые концепции, определяющие сферу действия Конвенции, не зависят от их толкования в какой-либо отдельной правовой системе»[6].

В Англии, провозвестнике современного режима совместной «физической» опеки, принято считать, что концепция «естественной опеки» ("*natural guardianship*"), известная английскому общему праву[7], восходит к концепции естественного права[8] юриспруденции Древнего Рима, а в настоящее время используется в правопорядках стран как романо-германской, так и англосаксонской семей права. Родительская опека подразделяется на совместную (с равным объемом прав обоих родителей) и единоличную (только один родитель наделен всей совокупностью правомочий, составляющих содержание родительских прав, а другой, который, как правило, проживает отдельно и обладает ограниченным перечнем родительских правомочий[9].

Также англосаксонская традиция подразделяет родительскую опеку над ребенком на юридическую (*legal*) и физическую (*physical*) опеку. Юридическая опека дает родителю, осуществляющему опеку, право принимать решения в интересах ребенка по следующим наиболее важным

[4] Например, применяются такие термины, как: *obsorge* (Австрия), *parental authority* (Франция, Португалия, Чехия), guardianship (Великобритания) и т. д. Регламент ЕС, посвященный проблеме определения юрисдикции, а также признанию и приведению в исполнение решений по вопросам семьи и опеки, использует термин "parental responsibility", под которым подразумевает все права и обязанности в отношении лица или имущества ребенка, которыми физическое или юридическое лицо наделено судебным решением, указанием законодательного акта или имеющим юридическую силу соглашением., включая права опеки и права доступа См.: Art. 2(2)(7) Council Regulation 2019/1111 of June 25, 2019 on Jurisdiction, the Recognition and Enforcement of Decisions in Matrimonial Matters and the Matters of Parental Responsibility, and on International Child Abduction (recast), O.J. (L 178), 18.

[5] Конвенция о гражданско-правовых аспектах международного похищения детей (Гаага, 25 октября 1980 г. (вступила в силу для Российской Федерации 1 октября 2011 г., На основании федерального закона «О присоединении Российской Федерации к Конвенции о гражданско-правовых аспектах международного похищения детей» от 31 мая 2011 г. № 102-ФЗ, Собрание законодательства РФ, 2011, № 23, Ст. 3242.

[6] Hague Conference on Private International Law, Report of the Second Special Commission Meeting to Review the Operation of the Hague Convention on the Civil Aspects of International Child Abduction at p. 4 (January 18–21, 1993), https://assets.hcch.net/upload/abdrpt93e.pdf

[7] Law Comm'n (Eng.), Family Law: Review of Child Law—Guardianship & Custody, Report No. 172 ¶ 2.2, at p. 5 (July 25, 1998), https://www.gov.uk/government/publications/family-law-review-of-child-law-guardianship-and-custody-1988

[8] «Естественное право есть то, которое природа внушила всем живым существам. Право это свойственно не только человеческому роду, но вообще всем существам, которые рождаются или в воздушном пространстве, или на земле, или в море. Отсюда происходит союз мужчины с женщиной, который мы называем браком; отсюда рождение и воспитание детей; далее мы видим, что и прочие живые существа руководствуются знанием этого права» (Приведено по изданию Institutsii Iustiniana, ca. 533 C. E./1998, I.2). Заметим, что институт родительской опеки в римском праве существовал только в виде законной (Institutsii Iustiniana, I.8) и фидуциарной опеки (Institutsii Iustiniana, I.19). Во всех иных случаях говорится о родительской власти. «Под нашею властью находятся наши дети, прижитые в законном браке» (Institutsii Iustiniana, I.9).

[9] Не смешивать с российским институтом ограничения родительских прав.

вопросам его жизни: медицинское обслуживание, образование и другие аспекты его жизни (Meyer et al., 2025, p. 27). Совместная юридическая опека позволяет обоим родителям принимать решения совместно, в то время как единоличная юридическая опека предоставляет только одному родителю право принимать все решения.

Зарубежный институт совместной физической опеки родителей предполагает совместное осуществление ухода за ребенком при его проживании в чередующемся режиме (регулярных и попеременно сменяющихся периодов, определяемых часами, днями, неделями или месяцами) у каждого из родителей (Hakovirta, 2023; Murru & Merla, 2025; Merla et al, 2025). Хотя официального определения этого термина нет, критическим фактором для признания физической опеки совместной предлагается считать ситуацию, когда дети после развода проживают не менее 30% своего времени с каждым из родителей (Augustijn, 2022, p. 496). Определение временного отрезка, проводимого с каждым из родителей, различается в разных странах, приблизительно от четверти до половины общего времени с каждым из родителей (Berman & Daneback, 2022, p. 1448).

Институт совместной физической опеки родителей становится все более распространенным в зарубежных странах (Augustijn et al., 2025, p. 508). Так, влияние правовой реформы в Испании в 2010 г. и установление совместной родительской опеки привели к интенсивному росту ее назначения за последние несколько лет (Flaquer, 2020, p. 382). В 2024 г. парламент Японии внедрил данный институт в национальное законодательство[10].

Обращаем внимание на то, что в национальном российском законодательстве отсутствует термин «совместная физическая родительская опека». Л. Ю. Михеева, рассматривая пересечение понятий «семья» и «опека», отмечает, что их сходство «не дает оснований к отождествлению этих явлений, а юридический характер опеки не позволяет рассматривать ее и как одну из разновидностей семьи» (Mikheeva, 2004, pp. 66–67). Согласно ст. 126 Семейного кодекса Российской Федерации установлено, что опека или попечительство устанавливаются над детьми, оставшимися без попечения родителей (по основаниям, указанным в пункте 1 статьи 121 СК РФ), в целях их содержания, воспитания и образования, а также для защиты их прав и интересов[11]. Федеральный закон «О дополнительных гарантиях по социальной поддержке детей-сирот и детей, оставшихся без попечения родителей» регламентирует опеку и попечительство как форму устройства детей-сирот и детей, оставшихся без попечения родителей, в целях их содержания, воспитания и образования, а также для защиты их прав и интересов[12]. Таким образом, в России под принятием ребенка под опеку понимается принятие чужого (не родного по первой нисходящей кровной линии родства) ребенка в семью.

В Российской Федерации при раздельном проживании родителей либо соглашением родителей, а при его отсутствии судом определяется место жительство ребенка, а не форма родительской опеки.

Косвенно из анализа Конвенции 1980 г. и Конвенции о юрисдикции, применимом праве, признании, исполнении и сотрудничестве в отношении родительской ответственности и мер

---

[10] あたらし法律事務所. (2024, 25 мая). 共同親権とは | 法改正はいつ？メリットとデメリット [Что такое совместная родительская опека? Когда состоится реформа законодательства? Преимущества и недостатки]. https://www.atarashi-law.com/column/2422

[11] Семейный кодекс Российской Федерации от 29 декабря 1995 г. № 223-ФЗ, Собрание законодательства РФ, 1996, № 1, Ст. 16.

[12] Федеральный закон «О дополнительных гарантиях по социальной поддержке детей-сирот и детей, оставшихся без попечения родителей» от 21 декабря 1996 г. № 159-ФЗ, Собрание законодательства РФ, 1996, № 52, Ст. 5880.

по защите детей[13] можно утверждать, что право на опеку и право на доступ как права родителей все же известны российскому праву и применимы при незаконном перемещении или удержании ребенка одним из родителей в родительских правоотношениях с иностранным элементом. В свою очередь, в России 4 августа 2025 г. группой депутатов Государственной Думы ФС РФ был внесен на рассмотрение проект № 983464-8 федерального закона о внесении изменений в СК РФ, которым предлагается введение института совместного воспитания и проживания в чередующемся режиме[14]. В пояснительной записке к законопроекту авторы обращают внимание на наличие у членов современного общества дефицита отцовского воспитания[15].

Несмотря на растущую популяризацию данного института, есть и его противники. Так, А. Маршалл пишет о том, что для детей постоянное перемещение между двумя местами проживания означает, что они живут двойной жизнью ("*in double-looped situation*") и должны быть внимательны к различным распорядкам, ожиданиям, требованиям и стилям воспитания каждого из родителей (Marschall, 2017, p. 343). Кроме того, необходимость решать практические вопросы — такие как наличие необходимой одежды, оборудования, школьных принадлежностей и прочих вещей в нужном домохозяйстве в нужное время, выстраивание устойчивых механизмов координации и коммуникации между этими домохозяйствами может существенно усложнять повседневную жизнь как родителей, так и детей (Zartler, 2021 p. 305). Кроме того, А. Ф. Пьянкова отмечает, что отсутствие детской привязанности к домашней обстановке, которая воздействует на подсознательные аспекты психики, телесные ощущения и эмоции приведет к появлению у детей чувства тревожности, неспособности понять и принять свою идентичность (Pyankova, 2025, p. 65).

Некоторые ученые пришли к заключению о недоказанности выводов эмпирических исследований о положительном влиянии на благополучие родителей и детей института совместной («физической») опеки родителей, поскольку их методология и заложенная в основу концепция опеки неоднородны и не учитывают множество факторов, а законодательство не регламентирует отдельные важнейшие спорные вопросы его реализации (Steinbach, 2019, p. 365, Ortega-Gaspar et al., 2021, p. 113).

В России еще 29 января 2019 г. Верховный Суд РФ указал на недопустимость утверждения графика общения и проживания ребенка в формате «любых четырех дней по выбору каждую неделю с 9 часов до 21 часа с правом посещения места жительства отца, общественных мест в отсутствие матери», поскольку он «ведет к формированию амбивалентного (двойственного) восприятия ребенком реальности, к двойным стандартам, к формированию навыков манипулирования у детей, лишает ребенка чувства "настоящего дома"»[16].

Учитывая рамки настоящего исследования, следует отметить, что вне зависимости от итогов рассмотрения законопроекта институт совместного воспитания хоть и способен обеспечить

[13] Конвенция о юрисдикции, применимом праве, признании, исполнении и сотрудничестве в отношении родительской ответственности и мер по защите детей от 19 октября 1996 г. (вступила в силу для Российской Федерации 1 июня 2013 г., Российская Федерация присоединилась к Конвенции на основании Федерального закона от 5 июня 2012 г. № 62-ФЗ), Собрание законодательства РФ, 2012, № 24, ст. 3079.

[14] Законопроект № 983464-8 «О внесении изменений в Семейный кодекс Российской Федерации (в части определения условий установления и осуществления порядка совместного воспитания детей родителями, расторгающими брак)», https://sozd.duma.gov.ru/bill/983464-8

[15] См. пояснительную записку по ссылке, указанной выше в предшествующей сноске.

[16] Определение Судебной коллегии по гражданским делам Верховного Суда РФ от 29 января 2019 г. № 18-КГ18-223.

соблюдение прав всех участников семейных отношений на общение друг с другом, но не является идеальным.

В этом аспекте интересна позиция судов стран, где данный институт внедрен и действует, относительно возможности устанавливать совместную физическую опеку. Так, 30 октября 2014 г. в Испании гражданская палата Верховного суда указала, что «конфликтная ситуация между родителями наносит ущерб интересам ребенка, что препятствует назначению совместной родительской опеки. Предпосылка назначения совместной опеки заключается в том, что между родителями должны существовать отношения взаимного уважения, позволяющие им принимать такие решения, которые приносят пользу ребенку и не нарушают его эмоционального развития, и вести себя соответствующим образом»[17]. Результаты исследований немецких ученых показывают, что совместная родительская опека над детьми может быть «хорошим решением для родителей, которым удается избежать родительских конфликтов и достичь мирного соглашения об уходе за детьми после развода» (Helms et al., 2023). Согласно шведским ученым, именно «качество совместного воспитания является ключевым фактором, определяющим психическое здоровье детей дошкольного возраста» (Bergström et al., 2021, p. 5). Родители, выбравшие совместное проживание на момент развода или расставания, отличались от других родителей тем, что они — и особенно матери — как правило, имели высокое образование и сообщали о более низком уровне родительских конфликтов до расставания и о небольшом количестве родительских проблем (Poortman & van Gaalen, 2017, p. 540).

Полагаем, что даже если будет принят законопроект о введении в Российской Федерации института совместного воспитания, аналога зарубежной «совместной физической родительской опеки», он будет неосуществим в тех случаях, когда родители не способны поддерживать между собой взаимное уважение и выстроить семейную систему ценностей, способствующую гармоничному развитию ребенка. То есть при наличии конфликтов между родителями – бывшими супругами такой институт не будет способствовать наилучшим интересам ребенка, а лишь приведет к эскалации конфликта, в центре которого будет ребенок.

Исследования подтверждают важность и качества отношений, и вовлеченности родителя в процесс воспитания ребенка (Palkovitz, 2019, p. 581). Совместное воспитание как институт, направленный на соблюдение прав всех участников родительских правоотношений, должно осуществляться только в соответствии с наилучшими интересами ребенка и невозможно при наличии конфликтных ситуаций между родителями. Обеспечение регулярного и безопасного общения между ребенком и родителем, не проживающим с ним, становится приоритетной задачей для предотвращения негативных последствий для психического и эмоционального развития ребенка.

Третье предположение: «виртуальное родительство» — эффективное дополнительное средство общения ребенка с родителем, проживающим отдельно

Одной из самых больших проблем, с которыми сталкиваются дети во время развода, является потеря связи с одним из родителей. Хотя электронная почта и телефонные разговоры могут использоваться и используются для общения, упомянутые способы связи обладают существенными недостатками. Так, с одной стороны, телефонный разговор можно применять

[17] Tribunal Supremo [TS], Sentencia 619/2014, de 30 de octubre de 2014, ECLI:ES:TS:2014:4342. См. описание этого решения, к примеру, на сайте одной из юридических фирм Мадрида: Muñoz Gómez, M. (2015, April 17). *Supreme Court pronouncement on joint custody.* G. Elías y Muñoz Abogados. https://www.eliasymunozabogados.com/en/blog/supreme-court-pronouncement-joint-custody

для мгновенного решения срочных вопросов и переговоров, однако, во-первых, отсутствие визуального контакта, а во-вторых, достаточная дороговизна телефонной связи (по сравнению с интернет-соединением) свидетельствуют о неудовлетворительности подобного способа общения. Электронная почта в качестве основного виртуального средства общения с ребенком в принципе некомфортна: огромное количество электронных писем и папок, возможная неверная интерпретация интонации письма затрудняют использование электронной для общения с ребенком.

Научные исследования в России и в целом в мире подтверждают тот факт, что молодежь почти в каждой стране использует социальные сети для поддержания постоянного контакта с друзьями (Steinsbekk et al., 2024; Dunas, 2020, p. 31, Mikhalev, 2025, p. 22).

Простота использования и распространенность социальных сетей и мессенджеров в обыденной жизни несовершеннолетних привели к тому, что в дополнение к традиционным формам непрямого общения (письма, телефонные звонки, сообщения на электронную почту) виртуальное общение родителей и детей стало включать расширяющийся спектр новых цифровых средств: программное обеспечение для видеоконференций, например *Zoom, Skype*; платформы социальных сетей, таких как «ВКонтакте»; мессенджеры *WhatsApp* и *Telegram* как особый вид программного обеспечения для обмена текстами, изображениями, видео, позволяющие осуществлять аудио- и видеосвязь.

Использование новых (сравнительно недорогих) способов поддержания связи родителями с детьми после расторжения брака с помощью цифровых инструментов обозначается в зарубежной доктрине различными терминами: "*virtual parenting*"[18], "*parenting online*" (Saini et al., 2013, p. 124). Для российского правового дискурса предлагается перевод данных терминов, как виртуальное родительство — как наиболее лаконичный, фокусирующий внимание на отношениях родителя и ребенка в их воспитательном и коммуникативном измерении.

Несомненно, технологии позволяют участвовать в воспитании ребенка после расторжения брака в ситуациях, в которых это, казалось бы, невозможно: например, при проживании родителя в другом городе или стране или осуществлении родителем, проживающим отдельно, трудовых функций вахтовым методом, а также при наличии конфликтов между родителями. Так, в решении суда г. Альберты по делу *BRH v. RPS* указано, что благодаря технологиям отдельно проживающему родителю предоставляется возможность общаться с ребенком, который проводит каникулы за границей: «Всякий раз, когда Б. Х. может приехать в Эдмонтон, бóльшую часть времени она должна проводить с А. С. Необходимо организовать широкий доступ к телефону и *Skype*»[19].

Одно из первых исследований в области международных показателей онлайн-активности детей и использования цифровых технологий для поддержки родительских правоотношений после расторжения брака провел Р. Бирнбаум[20]. Его результаты позволили выделить как поло-

[18] Birnbaum, R. (2019, November 12). *"Virtual Parenting" after Separation and Divorce.* The Vanier Institute of the Family. Vanier Institute of the Family. https://vanierinstitute.sharepoint.com/sites/PublicWebResources/Documents/Public%20Files/AR_2019-11-12_Birnbaum-Virtual-Parenting.pdf?ga=1https://vanierinstitute.ca/resource/virtual-parenting-after-separation-and-divorce/

[19] BRH v. RPS (2016), 40 Alta LR 6th 78 (Can. Alta. Q.B.), https://canlii.ca/t/gs8lt

[20] Birnbaum, R. (2019, November 12). *"Virtual Parenting" after Separation and Divorce.* The Vanier Institute of the Family. Vanier Institute of the Family. https://vanierinstitute.sharepoint.com/sites/PublicWebResources/Documents/Public%20Files/AR_2019-11-12_Birnbaum-Virtual-Parenting.pdf?ga=1https://vanierinstitute.ca/resource/virtual-parenting-after-separation-and-divorce/

жительные, так и отрицательные стороны «виртуального родительства». К отрицательным можно отнести проблемы конфиденциальности разговора (другой родитель подслушивал разговор), несение ответственности за доступ ребенка к цифровым технологиям в указанное время, вторжение в личную жизнь в результате использования технологий (беспрепятственный виртуальный доступ к дому родителя, проживающего с ребенком) и ощущение слежки (как за родителем, проживающим с ребенком, так и за родителем, проживающим отдельно). Наибольшее преимущество, отмеченное каждым из родителей, заключается в том, что ребенок имеет возможность поддерживать общение с родителем, проживающим отдельно, без контакта с бывшим супругом.

Хотя концепция «виртуальное родительство» является относительно новой, в ряде стран уже приняты специальные законы, регламентирующие договорный и судебный порядок установления графика онлайн-общения. Так, среди стран, в которых официально одобрили и рекомендовали включать график онлайн-общения в судебные решения, можно выделить США, Новую Зеландию и Австралию. Первый в США Закон о виртуальном общении был принят в 2004 г. в штате Юта[21]. В Колорадо, напротив, нет специальных законов, регулирующих виртуальное общение[22], однако судьи, рассматривающие семейные споры, могут в целях наилучших интересов ребенка включить его в официальный график общения «План родительского воспитания»[23]. Другим примером является Закон о заботе о детях Новой Зеландии 2004 г.[24], в соответствии с которым предусматривается в рамках «виртуального родительства» общение при помощи телефонных звонков или электронной почты, однако новые цифровые виды коммуникации не указаны. В свою очередь, проведенное М. Голлоп исследование позволило установить, что 70 опубликованных и доступных решений судов Новой Зеландии (53) и Верховного суда Австралии (17) за семилетний период (2017–2023 гг.) содержат разрешение на виртуальное общение: телефонная и видеосвязь указаны в 95% решений, общение через приложения и социальные сети — в 79%, в онлайн-играх — в 28% и т. д.[25]

Анализ нормативно-правовых актов и судебной практики позволяет выделить общие черты режима «виртуального родительства». Во-первых, в решении судов обычно описывают частоту, продолжительность и предпочтительные методы виртуального общения. Во-вторых, регламентируется соблюдение принципа сбалансированности физического и виртуального общения. Личное (физическое) общение признается приоритетным, а виртуальное должно дополнять, а не заменять, личный физический контакт. На суды возлагается обязанность следить за тем, чтобы виртуальное родительство не ставило одного из родителей в невыгодное положение и не сокращало его физическое время с ребенком, если только это не отвечает наилучшим интересам последнего. В-третьих, определяется возложение бремени предоставления соответствующих технологий и доступа к ним. Суд может рассмотреть способность каждого родителя предоставить необходимые технологии для «виртуального родительства».

[21] H.B. 82, 55th Leg., Gen. Sess. (Utah 2004), codified at Utah Code Ann. §§ 30-3-33, 30-3-35.

[22] Colo. Rev. Stat. § 14-10-124 (2014).

[23] См. мнение практикующих в Колорадо американских юристов: Robinson & Henry. (2024, March 13). What is virtual visitation in Colorado? https://www.robinsonandhenry.com/blog/family-law/virtual-visitation/7. Форма бланка «Плана воспитания», который заполняют в штате Колорадо родители и все заинтересованные в воспитании ребенка стороны, доступна для ознакомления по адресу https://www.coloradojudicial.gov/sites/default/files/2023-07/JDF1113.pdf

[24] Care of Children Act 2004, 2004 No 90 (N.Z.).

[25] Gollop, M. (2024). *Post-separation parent-child virtual contact: Opportunities and challenges.* University of Otago. https://www.borrinfoundation.nz/wp-content/uploads/2024/09/Post-separation-Virtual-Contact-Research-Summary.pdf

Бремя обеспечения ребенку доступа к цифровым технологиям возлагается на родителя, проживающего с ним: устройство должно иметь необходимый уровень зарядки и быть подключено к интернету; необходимо отслеживать, чтобы у ребенка было свободное время в его расписании, предпринимать другие действия, чтобы родитель в назначенное время мог виртуально общаться с ним. И наконец, в-четвертых, устанавливается запрет на изменение плана воспитания без разрешения суда.

Важно отметить, что фиксирование в судебном решении графика онлайн-встреч не означает, что необходимо разрешение суда, чтобы позвонить ребенку по телефону, но для того, чтобы виртуальное родительское время имело юридическую силу, оно должно быть одобрено судом.

Четвертое предположение: российское законодательство позволяет обеспечить равенство прав разведенных родителей на воспитание ребенка

Обратимся к нормативно-правовой базе, регламентирующей права мужчины и женщины в статусе родителей.

1. Конституция РФ закрепляет равенство прав мужчины и женщины, в том числе и при воспитании ребенка (ст. 19 и ч. 2 ст. 38)[26].
2. Согласно п. 1 ст. 61 СК РФ родители имеют равные права и несут равные обязанности в отношении своих детей.
3. В ст. 63 СК РФ закреплено преимущественное право родителей на воспитание своего ребенка.
4. В соответствии со ст. 55 СК РФ расторжение брака не влияет на право ребенка общаться с родителем и иными родственниками.
5. Государство в ст. 66 СК РФ предоставляет родителю, проживающему отдельно от ребенка, права на общение с ребенком, участие в его воспитании и решении вопросов получения ребенком образования, медицинской помощи и т. д.

Анализ ст. 66 СК РФ позволяет выделить следующие правовые гарантии реализации права такого родителя на общение:

1) судебный порядок утверждения графика общения ребенка и родителя, проживающего отдельно;
2) неправомерное препятствование общению ребенка и родителя квалифицируется как правонарушение, за которое статьей 5.35 КоАП РФ предусмотрена административная ответственность, варьирующаяся от штрафа до изменения места жительства ребенка (при злостном неисполнении решения суда)[27].

Исполнение требования исполнительного документа о порядке общения с ребенком включает в себя обеспечение судебным приставом-исполнителем беспрепятственного общения взыскателя с ребенком в соответствии с порядком, установленным судом[28]. Факт нарушения порядка фиксируется в административном протоколе, в который вносятся объяснения сторон, показания свидетелей и оценка сложившейся ситуации должностным лицом. При этом исполнительное производство считается оконченным, как только судебный пристав-исполнитель

[26] Конституция Российской Федерации. Принята всенародным голосованием 12.12.1993 г. (с изменениями, одобренными в ходе общероссийского голосования 01.07.2020), http://pravo.gov.ru/constitution/ (дата обращения: 01.07.2025).

[27] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001, № 195-ФЗ, Собрание законодательства РФ, 2002, № 1 (ч. 1), Ст. 1.

[28] Ст. 109.3 Федерального закона «Об исполнительном производстве» от 02.10.2007 № 229-ФЗ, Собрание законодательства РФ, 2007, № 41, ст. 4851.

установит факт непрепятствия должника общению взыскателя с ребенком (Filippova & Titarenko, 2022, p. 32).

Все вышесказанное позволяет сделать вывод о том, что с точки зрения закона защита прав родителя, проживающего отдельно от ребенка, и права ребенка на общение с родителями и иными родственниками полностью гарантированы.

Обратимся к правоприменительной практике.

1. Конституционный Суд РФ подтвердил конституционность положений действующего семейного законодательства, регулирующих порядок общения с ребенком[29]. Существующая нормативная база признана полностью соответствующей конституционным принципам и обеспечивающей необходимый баланс интересов всех участников семейных правоотношений.

2. Анализ решений судов Российской Федерации показывает, что при определении графика общения с ребенком в большинстве случаев суд указывает:

- первую и третью субботу месяца, второе и четвертое воскресенье месяца, дополнительно может быть установлено время, например, с 16:00 до 20:00;
- проведение отпуска в количестве *n* календарных дней. Даты проведения отпуска согласовываются между родителями заблаговременно, за два месяца до выезда[30].

В судебном решении в обязательном порядке уточняется присутствие или отсутствие второго родителя при общении и место проведения встречи. Например, «без присутствия матери в общественных местах либо по месту жительства отца с учетом режима дня, погодных условий и состояния здоровья ребенка»[31].

В Обзоре практики Верховного Суда РФ № 1 за 2024 г. подчеркнуто, что решение суда должно быть соотнесено с «закрепленным семейным законодательством принципом равенства родительских прав и обязанностей раздельно проживающих родителей (пункт 1 статьи 61 СК РФ)»[32]. Ввиду отсутствия опыта использования цифровых технологий в данной сфере такая практика пока фактически отсутствует, однако ранее Верховный Суд РФ указал, что расторжение брака «не исключает возможности другого родителя полноценно общаться с ребенком, а также принимать участие в его воспитании без каких-либо ограничений»[33]. Общение при помощи цифровых технологий осуществляется и в случаях, когда родители не разведены, причем как в обыденной жизни (общение по телефону), так и при длительном или кратковременном отсутствии, например при длительной командировке одного из них, выполнении трудовой функции в сменном графике или вахтовым методом работы, обучении при прохождении срочной службы и т. д. Такое цифровое общение в принципе предполагается и не осуждается обществом как дополнительный вид взаимодействия родителей и ребенка. В настоящее время законодательство РФ не содержит запрета на онлайн-общение родителя и ребенка, соответственно, с учетом аналогии права, приемлемости такого формата общения для современных детей и направленности правоприменительной практики на соблюдение наилучших интересов ребенка и максимальное сохранение семейно-родственных

[29] Определение Конституционного Суда РФ «Об отказе в принятии к рассмотрению жалобы гражданки Г. на нарушение конституционных прав ее несовершеннолетнего сына статьей 57 Семейного кодекса Российской Федерации» от 30 мая 2024 г. № 1267-О.

[30] Определение Судебной коллегии по гражданским делам Верховного Суда РФ от 4 октября 2022 г. № 4-КГ22-40-К1.

[31] Решение Заводского районного суда г. Саратова от 10 марта 2021 г. по делу № 2-779/2021.

[32] Обзор судебной практики Верховного Суда Российской Федерации № 1 (утв. Президиумом Верховного Суда РФ 29 мая 2024 г.), Бюллетень Верховного Суда РФ, 2024, № 7 (ред. от 27.11.2024 г.).

[33] Там же.

отношений полагаем возможным устанавливать график онлайн-общения в решениях суда по спорам об определении места жительства ребенка.

3. Российское законодательство устанавливает ответственность за нарушение порядка общения в виде штрафа и административного ареста (ч. 2 ст. 5.35 КоАП РФ). При злостном невыполнении судебного решения суд вправе вынести решение о передаче родителю, проживающему отдельно, ребенка, исходя из интересов ребенка и с учетом его мнения. В настоящее время достаточно сложно сделать вывод о статистических показателях по количеству рассмотренных дел в порядке привлечения по ч. 2 и 3 ст. 5.35 КоАП РФ. На интернет-странице Судебного департамента при Верховном Суде РФ[34] и сайте «Судебная статистика РФ»[35] есть данные по ст. 5.35.1 КоАП РФ, не релевантные для нашего исследования, а также по «*иным правонарушениям, посягающим на права граждан (иные статьи главы 5 КоАП РФ)*», среди которых и «скрывается» информация об интересующих нас составах административных правонарушений[36]. Согласно указанной статистике, на 2024 г. было рассмотрено 3183 дела, однако не представляется возможным определить, сколько из них затрагивало именно ч. 2 или 3 ст. 5.35 КоАП РФ. Имеются данные о том, что на 2024 г. Поступило заявлений об осуществлении родительских прав родителем, проживающим отдельно от ребенка (п. 2 ст. 66 СК РФ) — 16570, об устранении препятствий к общению с ребенком его близких родственников (п. 3 ст. 67 СК РФ) — 3210, а о возврате родителям ребенка, удерживаемого не на основании закона или судебного решения (п. 1 ст. 68 СК РФ) — 42 заявления[37]. Однако поскольку участники процесса (родители или иные родственники) неизвестны, однозначного вывода об эффективности предусмотренных мер ответственности, исходя из данных статистики, сделать нельзя.

В практике встречаются примеры, когда родители могут злоупотреблять родительским правами, препятствуя общению второго родителя с ребенком. Например, Челябинский областной суд отменил решение Озерского городского суда Челябинской области от 16 января 2023 г., вынесенное по делу об административном правонарушении, предусмотренном частью 2 ст. 5.35 КоАП РФ, в связи с истечением сроков давности привлечения к административной ответственности[38]. Анализ текста судебного решения показывает, что ответчица документов об уважительности причин непредоставления детей для общения с отцом не представила, а на судебном заседании суда первой инстанции сама признала, что не предоставляет отцу детей для общения из-за сложившихся между бывшими супругами неприязненных отношений. Иначе говоря, правонарушение имело место, а привлечение к ответственности стало невозможным, поскольку суд первой инстанции неверно трактовал нормы права и, пока шли процессы, истек срок давности. Согласимся с мнением ученых о том, что штрафные санкции не в полной мере достигают цели воспитательного воздействия. Родитель, проживающий отдельно, нередко встречает препятствия при привлечении родителя-нарушителя к ответственности. Так, дело

[34] Судебный департамент при Верховном Суде РФ. (б.д.). *Данные судебной статистики.* Верховный Суд РФ. По обращению 01.07.2025 к https://cdep.ru/?id=79

[35] Агентство правовой информации. (б.д.). *Судебная статистика РФ.* По обращению 01.07.2025 к https://stat.xn----7sbqk8achja.xn--p1ai/

[36] Агентство правовой информации. (б.д.). *Судебная статистика РФ. Административные правонарушения. Показатели по отдельным правонарушениям.* По обращению 15.10.2025 к https://stat.xn----7sbqk8achja.xn--p1ai/stats/adm/t/31/s/1

[37] Судебный департамент при Верховном Суде РФ. (2024). *Отчет о работе судов общей юрисдикции о рассмотрении гражданских, административных дел по первой инстанции.* https://cdep.ru/userimages/Statistika_2024/F3-svod-vse_sudy-2024.xls

[38] Решение Челябинского областного суда. г. Челябинск от 20 февраля 2023 г. по делу № № 7-142/2023.

об оспаривании бездействия сотрудников ОМВД, выразившееся в нерассмотрении заявлений отца о привлечении матери к административной ответственности за неисполнение решения суда об установлении порядка общения с сыном, дошло до Верховного Суда РФ. И только на этом этапе определение судьи Измайловского районного суда г. Москвы от 11 июня 2021 г., апелляционное определение судьи судебной коллегии по административным делам Московского городского суда от 10 сентября 2021 г. и кассационное определение судьи судебной коллегии по административным делам Второго кассационного суда общей юрисдикции от 9 декабря 2021 г. были отменены и дело было направлено в Измайловский районный суд г. Москвы на рассмотрение со стадии принятия к производству суда административного искового заявления[39].

Итак, нормы российского права закрепляют равные права родителей на воспитание ребенка, право ребенка и родителя, проживающего отдельно, на общение, санкции за создание препятствий общению родителя и ребенка. Основная проблема заключается в реализации прав на общение ребенка и родителя, проживающего отдельно, в реальной жизни. Штрафные санкции практически не применяются либо их применение затруднительно и растянуто во времени (фиксация препятствий, возбуждение производства по делу и т. д.). Несмотря на то что создание препятствий детско-родительскому общению, на наш взгляд, должно отрицательно оцениваться судом с точки зрения соответствия ответственному и компетентному родительству, мы не нашли ни одного судебного решения, которое бы изменило место жительства ребенка на основании ч. 3 ст. 5.35 КоАП РФ. Отметим, что в настоящее время в ряде стран используется термин «толерантность привязанности», который означает, что разведенные родители способны уважать связь и отношения ребенка со вторым родителем (Temizyürek, 2018, p. 303)[40]. Исследователи из Германии подчеркивают необходимость того, чтобы оба родителя обладали компетенцией «заботы о привязанности»[41], т. е. ценили сложившиеся отношения ребенка с другим родителем и активно содействовали их поддержанию. К сожалению, мы не можем утверждать, что судебная система нашей страны отдает предпочтение тому родителю, который способен максимально помочь несовершеннолетнему адаптироваться в условиях распада семьи и сохранить родственные отношения с другим родителем. В реальности де-факто существующая система непривлечения к ответственности приводит к тому, что ребенок может превратиться в оружие противостояния между бывшими супругами.

Анализ российского законодательства позволяет сделать вывод о том, что, исходя из буквы закона, отсутствуют нормы, препятствующие включению в решение суда графика общения ребенка с родителем по телефонной или интернет-связи как дополнительного средства общения с ребенком. Верховный Суд РФ неоднократно указывал на то, что определение места жительства ребенка с одним из родителей не исключает возможности другого родителя полноценно с ним общаться. Несомненно, ребенок и родитель, проживающий отдельно, могут общаться с использованием цифровых технологий и без решения суда, однако в ситуации конфликта между родителями, психологическое давление родителя, с которым проживает ребенок (обида родителя, скандалы, обвинения, настраивание против другого родителя и т. д.), общение будет, скорее всего, осуществляться тайно и формировать чувство вины у ребенка вне зависимости от того, чью сторону он выберет.

---

[39] Кассационное определение Верховного Суда РФ от 28 июля 2022 г. № 5-КАД22-36-К2.

[40] Сам термин возник благодаря психологу Уве Тевесу в 1992 году.

[41] Lux, U., & Zimmermann J. (2024, January 31). Familienbeziehungen und Loyalitätskonflikte [Семейные отношения и конфликты лояльности]. Universität Ulm. https://www.stark-familie.info/de/eltern/erziehen/trennungskinder/bindungsfuersorge/

Пятое предположение: цифровые технологии возможно использовать как средство реализации права на общение

В настоящее время такие услуги, представленные на рынке, можно разделить на две группы.

К первой группе можно причислить организации, которые используют общераспространенные цифровые инструменты и предоставляют услуги скорее организационного и (или) сопроводительного характера. В качестве примера приведем компанию *Brayden Supervision Services*, оказывающую услуги по организации контролируемого виртуального родительского общения через систему *Zoom* на территории Онтарио и Новой Шотландии (https://www.braydensupervision.com). Компания берет на себя обязательство запрашивать визуальный осмотр обоих физических пространств как в начале проведения виртуальной встречи, так и в любой момент виртуального общения. Проживающий с ребенком родитель несет ответственность за подготовку комнаты. Если ребенок старше пяти лет, то его оставляют одного, если младше, то в комнате находится инспектор — служащий компании. Компания заверяет родителей, что все сотрудники прошли проверку в полиции и имеют высшее или специальное среднее профессиональное образование по психологии, работе с детьми и молодежью или в смежной области.

Вторая группа характеризуется использованием специального программного обеспечения для общения родителей и ребенка. Веб-ориентированное программное обеспечение — это программное обеспечение, предназначенное для объединения людей путем упрощения и автоматизации общения, обмена информацией и идеями, планирования расписаний и т. д. На международном рынке уже существуют успешные решения, помогающие разведенным родителям координировать графики общения и фиксировать договоренности. Среди популярных продуктов можно выделить *Our Family Wizard, TalkingParents, 2houses, Alimentor, Custody X Change* и др. Среди общих характеристик данных онлайн-платформ можно выделить:

- функциональность — большинство приложений включают функции для планирования встреч, обмена сообщениями, мониторинга выплаты алиментов и дополнительных расходов на несовершеннолетних и фиксации нарушений;
- ориентацию на удобство — дружелюбный пользовательский интерфейс (компании, предлагающие приложения на рынке, предлагают и обучение, и даже услуги присутствия специалиста на онлайн-встречах);
- условную юридическую значимость в качестве доказательств при рассмотрении споров.

По приблизительным оценкам аналитических агентств, мировой рынок приложений для родителей в последние годы стремительно растет. Ожидается, что он увеличится с 1,53 млрд долл. США в 2024 г. до 1,72 млрд долл. США в 2025 г. при среднегодовом темпе роста (*compound annual growth rate*) 12,3%[42]. В мае 2023 г. *AppClose,* ведущая платформа для совместного воспитания детей, преодолела отметку в 500 000 загрузок в *Google Play*[43]. Компании стараются приобрести конкурентное преимущество, предлагая дополнительные возможности. Так, например, *TalkingParents* позиционируется как приложение без возможности удаления сообщений и записей и с совместным сохранением документов (https://talkingparents.com), а *Alimentor* не только имеет календарь встреч, но и позволяет создавать подробные отчеты о времени, которое каждый родитель проводит с детьми, фиксируя случаи нарушения графика, а также оповещает о том, что запланированное время общения с детьми совпадает с праздниками

[42] См. отчеты компании, осуществляющей бизнес-исследования. Business Research Company. (2025). *Parenting apps global market report*. https://www.thebusinessresearchcompany.com/report/parenting-apps-global-market-report

[43] См. о рынке приложений для родителей в докладе: Patel, D. (2025). *Parenting apps market*. Data Intelo. https://dataintelo.com/report/global-parenting-apps-market

или другими событиями в календаре родителя (https://alimentor.org). Интересна в контексте настоящей работы платформа *Custody X Change* — австралийское онлайн-приложение, которое позволяет разведенным родителям составить план-график общения с ребенком для суда (https://www.custodyxchange.com).

Если рассматривать государственное внедрение таких онлайн-платформ, то в качестве примера можно привести приложение *Anthea* для смартфонов и планшетов, включающее в себя виртуальную коммуникационную платформу, с помощью которой разведенные родители могут обмениваться информацией, документами и общаться с детьми. В Италии суд г. Модены, рассматривая вопрос о соблюдении разведенными родителями подписанного ими пакта о родительской лояльности в целях содействия решению проблем, которые могут касаться воспитания их детей и общения с ними, обязал использовать исключительно приложение *Anthea.* Суд подчеркнул, что родители должны осознавать, что все сообщения, которыми они обмениваются на цифровой платформе, могут быть предметом судебного рассмотрения и представляют собой неоспоримое доказательство[44].

Проведенное в Австралии и Новой Зеландии исследование, основанное на онлайн-опросе юристов, специализирующихся на семейном праве, показало, что три четверти из них рекомендуют приложения своим клиентам, однако и юристам по семейному праву, и разведенным родителям необходимо всестороннее и более тонкое понимание преимуществ и рисков таких приложений (Payne et al., 2022. p. 13).

Приложение «Территория общения и доверия» как цифровая технология, позволяющая обеспечить право на общение в России

На наш взгляд, для наиболее эффективной реализации прав родителей, отдельно проживающих от ребенка, и соблюдения наилучших интересов ребенка, который оказывается в фокусе сложных отношений разводящихся или разведенных родителей, необходимо разработать и внедрить государственное приложение с рабочим названием «Территория общения и доверия».

[44] Tribunale di Modena [Суд Модены], 28 декабря 2017, n. 2259 (It.), https://news.avvocatoandreani.it/allegati/sentenze/Tribunale-Modena-sentenza-2259-2017.pdf (дата обращения: 01.07.25). См. также реакцию юридического бизнеса на данное приложение: Studio Legale Forani. (б.д.). *App per genitori separati: La tecnologia salva conflitti* [Приложения для раздельно проживающих родителей: технологии помогают предотвращать конфликты]. По обращению 01.07.25 к https://studiolegaleforani.it/separazione-e-divorzio/app-per-genitori-separati-basta-conflitti-grazie-alla-tecnologia/; Zazzarini, S. (б. д.). *La tecnologia al servizio della famiglia: Arriva l'app per genitori separati o divorziati che li aiuta a gestire i figli* [Технологии на службе семьи: появляется приложение для раздельно проживающих или разведенных родителей, которое помогает им управлять вопросами, связанными с детьми]. Busetto Studio Legale. По обращению 01.07.2025 к https://www.studiolegalebusetto.it/arriva-lapp-genitori-separati-divorziati-aiuta-gestire-figli/; Ordine degli Avvocati di Sondrio. (2018). *Trib. Modena 28 dicembre 2017 n. 2259. Accordi di divorzio: sì all'app. per gestire insieme i figli* [Суд г. Модены, 28 декабря 2017 г., № 2259. Соглашения о разводе: да — приложению для совместного управления вопросами, связанными с детьми]. https://www.ordineavvocatisondrio.it/formazione-continua/famiglia-successioni-mediazione/2018/marzo/famiglia-app-per-la-gestione-figli.pdf#:~:text=che%20%E2%80%9Cil%20mancato%20uso%20dell'applicazione%20non%20potr%C3%A0,di%20insorta%20conflittualit%C3%A0%20tra%20i%20genitori%20successivamente%E2%80%9D; Diritto di famiglia. (2018, 25 февраля). *Una app per gestire la conflittualità genitoriale dopo il divorzio* [Приложение для управления родительскими конфликтами после развода]. StudiLegali. https://www.studilegali.com/articoli/una-app-per-gestire-la-conflittualita-genitoriale-dopo-il-divorzio; Micolucci, F. (2018, 19 января). *Divorzio: Al via il progetto Anthea per gestire i figli* [Развод: стартует проект Anthea для управления вопросами, связанными с детьми]. Salvis Juribus. https://www.salvisjuribus.it/divorzio-al-via-il-progetto-anthea-per-gestire-i-figli/

Данное приложение должно, по нашему мнению, быть государственным по ряду причин.

1. Разработчики коммерческих мобильных приложений поощряют пользователей вводить персональные данные и регулярно делятся собранными данными с третьими лицами для улучшения пользовательского опыта или коммерциализации приложения. Мировое сообщество и Россия, понимая и признавая особую уязвимость детей, принимают нормативные акты, направленные на защиту конфиденциальности информации, связанной с ними[45]. Тем не менее ряд исследований свидетельствует о том, что большинство приложений, содержащих данные несовершеннолетних, являются одними из худших с точки зрения количества сторонних трекеров (Campbell, 2020), политика конфиденциальности в таких приложениях не всегда присутствует, а если и присутствует, то значительно различается по удобочитаемости (Das et al., 2018). Среди распространенных проблем — частый обмен данными или недостаточные меры безопасности, включая запросы разрешений и передачу данных третьим лицам.
2. Манипулятивная и прямая реклама в приложениях широко распространена. Даже если отвлечься от того, что содержание рекламы должно соответствовать определенной зрелости несовершеннолетних и может быть потенциально опасным для здоровья ребенка, наличие рекламы в работе таких приложений для общения выглядит неэтичным. Особенно если пострazводная ситуация конфликтная и эмоционально нестабильная.
3. Ряд функций в коммерческих приложениях для «виртуального родительства», которые распространены на рынке, возможно активировать только платно[46]. Поскольку право ребенка и родителей на общение особое, наполнено эмоциональным содержанием и является необходимой основой для сохранения кровнородственных отношений и ощущения семьи, то полагаем, что его обеспечение не должно ставиться в прямую зависимость от наличия или отсутствия у родителей денежных средств.

[45] См., к примеру, Общий регламент по защите данных (*General Data Protection Regulation, GDPR*): 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 O.J. (L 119) 1. См. также Закон США о защите конфиденциальности детей в Интернете вместе с подзаконным актом, принятым ФТК США во исполнение закона (*Children's Online Privacy Protection Rule, COPPA*): Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6505 (2018); 16 C.F.R. pt. 312 (2024), https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[46] Анализ приложений показывает, что бесплатные функции, в основном сводятся к следующим опциям: доступ к вебсайту с поддержкой рекламы, создание родительских аккаунтов (нередко ведение личного дневника), звонки внутри приложения (в частности, звонки в определенное судом время), защищенный обмен сообщениями, общий календарь. По платным подпискам в зависимости от тарифов можно выделить следующие функции: определенное или неограниченное количество записанных телефонных и видеозвонков, ограниченное или неограниченное количество PDF-записей, размер хранилища файлов, информационный банк данных о ребенке (хранение официальных документов ребенка, его медицинские данные, данные об образовательных учреждениях, дополнительных учреждениях и т. д.), уведомления о времени и дате общения или совместных мероприятий, формирования отчетов для суда, оплата расходов на ребенка, включая перевод алиментов. Отметим, что, например, в приложении *OurFamilyWizard* все функции платные, тариф зависит от выбираемых функций, наиболее интересные: формирование отчета с указанием даты и времени отправки, получения и первого прочтения сообщения (текст сообщений нельзя изменить или удалить), фиксирование запросов на изменение и перераспределение времени с ребенком, фиксирование нахождения родителя на месте встреч (до 500 футов точность), надежное хранение всех записей и стенограмм в течение 365 дней, запись звонков. Приложение *Custody X Change* (полностью платное), среди интересных функций содержит 140 типовых планов совместного воспитания ребенка, которые можно редактировать; калькулятор времени, проведенного с ребенком, за любой период, прошлый или будущий.

4. Одним из ключевых преимуществ приложения для воспитания детей после расторжения брака является возможность загрузки отчетов о переписке или событиях в качестве доказательств для суда[47]. Некоторым родителям эта функция может понадобиться, например, когда наблюдается продолжающийся межродительский конфликт, для представления доказательств фактов, угрожающих общению, или нарушения судебных постановлений.

Данное предложение должно быть ориентировано на использование современных технологий, интеграцию с государственными структурами и реализацию инновационных функций, таких как применение искусственного интеллекта (ИИ) для фиксирования спорных ситуаций, возникающих в процессе общения разведенных родителей между собой по вопросам воспитания детей.

Приложение должно включать следующий ***функционал***:

1) календарь совместного планирования:
   - родители могут составлять и согласовывать графики встреч, школьных мероприятий, медицинских приемов и других событий;
   - возможность настройки уведомлений о предстоящих событиях;
   - функция фиксации изменений с обязательным уведомлением обеих сторон;
2) обмен сообщениями:
   - отдельные встроенные текстовые мессенджеры: один для общения между родителями, второй — для ребенка и родителя, проживающего отдельно. Все сообщения автоматически архивируются, не подлежат удалению или изменению;
   - встроенный мессенджер (с функциями отправки видео- и аудиосообщений) для общения ребенка и родителя, проживающего отдельно;
3) базу документов, в которую родители смогут загружать важные документы и обмениваться ими (медицинские записи, школьные отчеты, судебные решения, чеки и справки о дополнительных расходах на ребенка и т. д.). Необходимо предусмотреть защищенный доступ к файлам, чтобы избежать их потери или несанкционированного удаления;
4) доступ для третьих лиц:
   - право доступа к личному кабинету должно быть предоставлено судебному приставу-исполнителю;
   - возможность предоставления доступа к аккаунту иным сотрудникам государственных учреждений, например органов опеки и попечительства, для мониторинга взаимодействий;
5) функционал гарантий:
   - система тонального и филологического анализа искусственным интеллектом сообщений и передача отчета о потенциально агрессивных формулировках судебному-приставу исполнителю; использование технологий обработки естественного языка (*Natural Language Processing, NLP*) для анализа сообщений; интеграция с модулями машинного обучения для обучения модели на анонимизированных примерах общения; постоянное обновление алгоритмов на основе обратной связи от пользователей;
   - генерация отчетов о взаимодействиях и нарушениях, которые могут быть предоставлены адвокатам или судьям;

[47] Такие инструменты есть, в частности, в *OurFamilyWizard* (платная функция по заказу неограниченного количества нотариально заверенных документов в печатном виде и с их доставкой по почте пользователю или его юристу) (См.: OurFamilyWizard. (n.d.). *Plans & pricing.* https://www.ourfamilywizard.com/plans-and-pricing) и в *AppClose* (платные функции по ведению коммуникации и документации, и их заверению (см.: https://appclose.com).

- отчеты о взаимодействиях и нарушениях, представленные приложением «Территория общения и доверия» и подтвержденные судебным приставом-исполнителем, получают юридическую силу доказательств при рассмотрении дел по ст. 5.35 КоАП РФ.

Процедура использования приложения «Территория общения и доверия» может иметь следующий вид.

1. В рамках рассмотрения споров об определении места жительства ребенка либо порядка общения с ним судья в решение включает график не только очных, но и виртуальных встреч. В решении суда должно быть установлено обязательное время, в течение которого ребенок и родитель, проживающий отдельно, могут гарантированно общаться посредством приложения. Родительские правоотношения трехсубъектные, и ребенок — полноправный субъект, однако, исходя из анализа ст. 57 СК РФ, его мнение должно быть выслушано, но оно не является обязательным при разрешении данного спора. Более того, как мы указывали ранее, Конституционный Суд РФ не счел неконституционными нормы, позволяющие не учитывать демонстративное нежелание ребенка контактировать с одним из родителей при рассмотрении судами споров о порядке общения с ребенком[48]. Существующая нормативная база признана полностью соответствующей конституционным принципам и обеспечивающей необходимый баланс интересов всех участников семейных правоотношений.

В ситуациях, когда несовершеннолетний полностью отказывается от виртуального общения с родителем, проживающим отдельно, суду, на наш взгляд, необходимо выяснить причины и мотивы такого решения. При этом согласно постановлению Пленума Верховного Суда РФ от 27 мая 1998 г. № 10[49] и п. 1 ст. 65 СК РФ суд только в исключительных случаях вправе отказать этому родителю в удовлетворении иска об определении порядка его участия в воспитании ребенка. Особенно если второй родитель изменил или планирует изменить место жительства, у него вахтовый метод работы и т. д. При этом важно учитывать позицию Верховного Суда РФ, который обращает внимание на то, что непосредственное исполнение решений о порядке общения с ребенком не может превращаться в средство давления на ребенка и родителя, если это угрожает психике самого несовершеннолетнего[50].

Финансовая обязанность обеспечить несовершеннолетнего соответствующими средствами связи (ноутбук, телефон, компьютер, веб-камера в зависимости от возраста и (или) финансовых возможностей) возлагается на обоих родителей в равных долях. В случае если ребенок младше семи лет, то родитель, с которым определено его место жительства, может по своему желанию предоставлять свои средства коммуникации.

2. Информация о новых участниках передается в службу судебных приставов, которые подключают несовершеннолетних детей (старше трех лет) и родителей к приложению «Территория общения и доверия».

При добросовестном и ответственном родительстве, когда оба родителя осознают, что расторжение брака прекращает супружеские правоотношения, но никак не родительские и понимают значимость и необходимость общения с обоими родителями, виртуальное общение

[48] Определение Конституционного Суда РФ «Об отказе в принятии к рассмотрению жалобы гражданки Г. на нарушение конституционных прав ее несовершеннолетнего сына статьей 57 Семейного кодекса Российской Федерации» от 30 мая 2024 г. № 1267-О.

[49] Постановление Пленума Верховного Суда РФ «О применении судами законодательства при разрешении споров, связанных с воспитанием детей» от 27 мая 1998 г. № 10, Бюллетень Верховного Суда РФ, 1998, № 7.

[50] Обзор судебной практики Верховного Суда РФ № 4 (утв. Президиумом Верховного Суда РФ 26.12.2018 г.), Бюллетень Верховного Суда РФ, 2019, № 8.

в приложении осуществляется на базе подсистемы ИИ на основе мультимодальных моделей, которые не будут сохранять анализируемые данные. Основная задача приложения при добросовестном и ответственном поведении родителей — обеспечение безопасного и конфиденциального виртуального общения. Обработка и хранение информации с использованием ИИ осуществляется в *экстраординарном порядке и только по решению суда.*

Так, в случае подачи жалобы от одного из родителей на нарушения решения суда: несоблюдение графика встреч, агрессивное поведение одного из родителей, которые влияют на психическое состояние ребенка, возбуждается исполнительное производство и активируется следующий ***алгоритм работы в приложении***:

1. Судебный пристав-исполнитель обращается в суд с ходатайством об установлении надзора (мониторинга) над виртуальным общением в приложении «Территория общения и доверия».
2. Родители и ребенок в обязательном порядке предупреждаются, что их общение находится под мониторингом судебного пристава-исполнителя.

3. Искусственный интеллект автоматически фиксирует нарушения договоренностей (например, несоблюдение расписания встреч) и только по дополнительному запросу от судебного пристава-исполнителя анализирует переписку между родителями, определяя эмоциональную тональность, выявляя потенциально конфликтные или агрессивные формулировки. Несомненно, существуют резонные опасения о правомерности передачи ИИ составления заключения относительно наличия или отсутствия факта неисполнения судебного решения. Думается, что и на современном этапе, и в даже в далеком будущем нельзя будет предоставлять ИИ возможность принимать решение относительно столь тонких и деликатных отношений, которые существуют между ребенком и его родителями, без учета индивидуальных особенностей каждого ребенка и родителя, истории и специфики их взаимоотношений, не говоря уже об отношениях проживающих отдельно родителей (да и вообще человеческих отношениях в целом). Именно поэтому ИИ должен предоставлять отчет судебному приставу, который и определяет необходимость точечной и (или) полной проверки, после проведения которой он формирует заключение. Судебный пристав-исполнитель вправе отслеживать выход в сеть, запрашивать информацию по отсутствию ребенка или родителя в сети в назначенное время. Показания судебного пристава исполнителя также являются доказательством недобросовестности одного из родителей.

4. По итогам проверки с учетом заключения судебного пристава-исполнителя ИИ формирует отчет для суда и родителей. Формат отчета, в котором он будет представляться, должен содержать дату, время, суть нарушения, подтверждающие материалы (скриншоты сообщений, записи изменений в расписании). Судебный пристав-исполнитель проверяет отчет и в зависимости от собственного усмотрения утверждает или редактирует.

Отметим, что, во-первых, в зарубежных странах уже более двух десятилетий используется режим контролируемых посещений, или, иначе сказать, общение под надзором, которые предлагают структурированный контакт между родителем и ребенком в присутствии третьего лица, ответственного за наблюдение и безопасность участников[51]. Использование нейтральной третьей стороны для контроля такого общения необходимо при наличии в материалах дела

[51] Ср. соответствующие положения Флоридского статута о надзоре за посещениями (Fla. Stat. § 753.01 (2025), http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0700-0799/0753/Sections/0753.01.html), положения восьмой книги Социального кодекса Германии (Sozialgesetzbuch [SGB] Achtes Buch [VIII] § 18(3) (Ger.)) и Французского гражданского кодекса (Code civil art. 373-2-9 (Fr.)).

фактов жестокого обращения с детьми, фактов, свидетельствующих о повышенном конфликте между родителями, о злоупотреблении родителями психоактивными веществами, о проблемах с психическим здоровьем (Oehme et al., 2021, p. 131). Во-вторых, как показывает опыт отдельных юрисдикций, распространение требований режима «контролируемых посещений» возможно и на виртуальное общение[52]. Как минимум такой опыт имел место в период распространения COVID–19 (Oehme et al., 2021, p. 134).

Соответственно, использование судебного пристава-исполнителя с целью соблюдения прав ребенка и родителя, проживающего отдельно, не противоречит сложившемуся мировому опыту в данной сфере, и, более того, признано достаточно эффективным механизмом.

Полагаем возможным задуматься над тем, чтобы мониторинг виртуального общения при наличии конфликтных ситуаций назначался не на стадии исполнительного производства, как мы предлагаем, а решением суда при подаче заявления по ст. 5.35 КоАП РФ. Это будет, с одной стороны, соответствовать международной практике и основным началам семейного законодательства, с другой — усложнять и увеличивать по времени весь процесс обеспечения исполнения решения суда. Предположим кейс: есть решение суда об определении порядка общения ребенка с родителем, проживающим отдельно, которое не исполняется, соответственно, необходимо возбудить исполнительное производство. Если мы используем предложенный алгоритм, то у нас будут зафиксированные доказательства для суда. Если мониторинг виртуального общения будет назначаться решением суда после отдельного разбирательства, то какие доказательства сторона сможет представить? Считаем, что данный вопрос нуждается в дополнительном рассмотрении, и исследуем его в ближайшем будущем.

Полагаем, что осведомленность участников о мониторинге виртуального общения не имеет принципиального значения. Корректировка поведения под влиянием такого контроля сама по себе означает достижение искомой цели — обеспечение надлежащего общения ребенка с отдельно проживающим родителем. Напротив, неспособность или нежелание участника адаптировать свое поведение косвенно свидетельствует о его родительской недобросовестности, независимо от того, исходит ли это от матери или отца. Данные мониторинга могут впоследствии использоваться как доказательства в иных судебных процессах: об уклонении от исполнения родительских обязанностей, о злостном неисполнении судебного решения с возможной передачей ребенка другому родителю и т. д. При этом ключевая функция приложения «Территория общения и доверия» — именно *обеспечение коммуникации*, а решение об использовании отчетов судебного пристава-исполнителя остается прерогативой заинтересованных родителей и ребенка, достигшего четырнадцатилетнего возраста. Предлагаемая модель разрешения проблемы поддержания общения родителей с ребенком, на наш взгляд, соответствует конституционному принципу неприкосновенности частной жизни (ст. 23 Конституции РФ) и основным началам семейного законодательства, в частности недопустимости произвольного вмешательства кого-либо в дела семьи (ст. 1 СК РФ), а также правам ребенка, закрепленным в СК РФ и Конвенции о правах ребенка[53]. В контексте особой конституционной и правовой ценности детства баланс прав на неприкосновенность частной жизни и родительских прав не может быть нарушен, поскольку использование такой модели направлено на заботу о нравственности, физической и психической безопасности ребен-

[52] К такому выводу пришел, к примеру, финский законодатель. См.: Laki lapsen huollosta ja tapaamisoikeudesta annetun lain muuttamisesta (Act Amending the Child Custody and Visitation Rights Act) (Fin.), 190/2019, 9 b § (8 Feb. 2019), https://www.finlex.fi/api/media/statute/696127/mainPdf/main.pdf?timestamp=2019-02-07T22%3A00%3A00.000Z

[53] Конвенция о правах ребенка, принята 20 ноября 1989 г., Сборник договоров ООН, т. 1577, с. 3.

ка, имеет целью обеспечение его наилучших интересов в контексте сохранения родственных отношений и преемственности поколений как традиционной семейной ценности. По аналогии можно использовать постановление Конституционного Суда РФ, который не нашел подтверждения нарушения Конституции РФ при использовании одним из разведенных родителей программных средств родительского контроля, даже если при этом станут известны какие-либо факты семейной жизни другого родителя: «...родитель в ситуации, которую он субъективно оценивает как представляющую реальную угрозу для интересов его ребенка, достаточно ограничен в выборе способов установления и подтверждения ненадлежащего характера поведения по отношению к ребенку других лиц для последующего принятия своевременных и необходимых мер... если ситуация, повлекшая собирание сведений с использованием соответствующего программного средства, рассматривается родителем как представляющая угрозу для физической неприкосновенности ребенка или его формирующейся психики с достаточной степенью обоснованности (не исключая и указанного добросовестного заблуждения), это не может не учитываться при уголовно-правовой оценке соответствующего деяния. Иное не согласовывалось бы с целями конституционно-правового закрепления приоритетности детей в государственной политике России, а также с критериями соразмерности ограничения прав»[54]. Полагаем, что все вышесказанное может быть применимо и к использованию приложения «Территория общения и доверия», поскольку при отсутствии конфликта и жалобы данные, как уже было сказано, не будут сохраняться, а при их возникновении можно говорить об угрозе наилучшим интересам ребенка, его психике и семейным ценностям и, соответственно, участие судебных приставов-исполнителей обоснованно.

В идеале приложение «Территория общения и доверия» должно быть интегрировано с Федеральной государственной информационной системой «Единый портал государственных и муниципальных услуг (функций)» и ГАС «Правосудие» для автоматической передачи данных. Важно создать интерфейс (*Application Programming Interface, API)* для обмена данными с государственными системами в режиме реального времени, применять зашифрованные каналы связи для защиты данных. Возможна адаптация интерфейса приложения для подготовки отчетов в формате, принятом судебными органами.

Использование такого типа цифрового инструмента обладает следующими значимыми преимуществами.

- Обеспечение нейтральной среды, позволяющей исключить ребенка из центра конфликта и ограничить его участие в напряженных, а подчас и токсичных, отношениях между родителями, делая невозможным или затруднительным возложение на него роли передатчика информации.
- Обеспечение кибербезопасной среды, позволяющей предотвратить взломы аккаунтов несовершеннолетних.
- Устранение чувства вины и тревожности у несовершеннолетних, использующих современные средства связи втайне от родителя, проживающего с ними. Дети не должны быть вынуждены выбирать между родителями, если те расторгли брак.

Данное цифровое приложение позволит:

- в сжатые сроки уведомить соответствующие государственные органы о нарушениях в отношении права ребенка и родителя, проживающего отдельно, на общение или иных нарушениях прав ребенка;

[54] Постановление Конституционного Суда РФ «По делу о проверке конституционности части первой статьи 137 Уголовного кодекса Российской Федерации в связи с жалобой гражданина П. О. Вильке» от 18 января 2024 г. № 2-П.

- предоставлять объективные данные для правоохранительных и иных органов при подаче заявления о возбуждении дела по ч. 2 и (или) 3 ст. 5.35 КоАП РФ и для судебных разбирательств;
- адаптировать документацию и отчеты для российских судов и правоохранительных органов.

Наше предложение полностью соответствует современному законодательству, не противоречит сложившейся судебной практике и отвечает перспективам цифровизации[55] и национальным целям развития Российской Федерации[56].

Риски внедрения и использования приложения «Территория общения и доверия»

Среди основных рисков эффективного использования приложения «Территория общения и доверия» как инструмента, обеспечивающего дополнительный вид общения разведенного родителя и ребенка, необходимо выделить вмешательство родителя, с которым проживает ребенок. Вмешательство может происходить различными способами, но наименее контролируемыми и, следовательно, наиболее опасными для сохранения теплых родственных отношений являются непредоставление ребенку тихого и уединенного пространства для общения (Saini et al., 2013, p. 132), намеренное создание шумового фона, активное и агрессивное вмешательство в онлайн-общение, подслушивание разговора и т. д.

К примеру, § 153.015(c) Семейного кодекса Техаса закрепляет обязанность родителей обеспечивать «электронное общение с ребенком с соблюдением той же конфиденциальности, уважения и достоинства, которые предоставляются всем другим формам доступа» во время разговора с другим родителем[57].

В свою очередь, § 3100 Семейного кодекса Калифорнии[58] содержит строгий запрет (под угрозой уголовного наказания) на умышленное и без согласия всех сторон конфиденциальной коммуникации использование электронного устройства для усиления или записи звука с целью подслушивания или записи конфиденциальной коммуникации, независимо от того, осуществляется ли коммуникация между сторонами в их присутствии или с помощью телеграфа, телефона или другого устройства (§ 632 Уголовного кодекса Калифорнии[59]).

Полагаем, что уголовное наказание не отвечает целям сохранения родственных отношений и является чрезмерным. Предлагаем квалифицировать такие действия родителей по ч. 2 и 3 ст. 5.35 КоАП РФ, используя в качестве доказательств данные, полученные благодаря использованию приложения «Территория общения и доверия». Соответственно, текстовые сообщения или видеозаписи, сохраненные после возбуждения исполнительного производства и свидетельствующие о пренебрежении или ненадлежащих ситуациях, потенциально могут быть использованы в делах об изменении условий определения места жительства ребенка при соблюдении правил доказывания и конфиденциальности.

---

55 Указ Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.», от 9 мая 2017 г. № 203, Собрание законодательства РФ 2017, № 20, Ст. 2901.

56 Указ Президента РФ «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» от 07.05.2024 № 309. Собрание законодательства РФ. 2024, № 20, Ст. 2584.

57 Tex. Fam. Code Ann. § 153.015 (2025), https://statutes.capitol.texas.gov/Docs/FA/htm/FA.153.htm#153.015

58 Cal. Fam. Code § 3100 (2024), https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=FAM&sectionNum=3100

59 Cal. Penal Code § 632 (2024), https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=632&lawCode=PEN

Разработка процедуры комплаенса защиты персональных данных (*privacy compliance*) для такой платформы является критичным аспектом, поскольку при использовании данной платформы будет непрерывно осуществляться передача данных о личной и семейной жизни физических лиц, их косвенная и прямая обработка и хранение.

Основная цель данной процедуры приложения «Территория общения и доверия» может заключаться в обеспечении защиты персональных данных пользователей (родителей, детей), минимизации рисков нарушения конфиденциальности и соответствии национальным и международным законам.

Отметим, что многие государства фокусируются на принятии законодательных актов о защите персональных данных. Так, в 2018 г. вступил в силу европейский Общий регламент о защите персональных данных (*GDPR*)[60], в 2020 г. — Закон Бразилии «О защите персональных данных» (*Lei Geral de Proteção de Dados Pessoais*)[61]. В 2023 г. был принят Закон Индии о защите цифровых персональных данных (*Digital Personal Data Protection Act*)[62]. Большинство нормативно-правовых актов о защите персональных данных требуют от компаний создания систем со встроенной защитой персональных данных (*privacy by design*) и систем конфиденциальности по умолчанию (*privacy by default*).

В России аналогом таких актов является Федеральный закон «О персональных данных»[63]. Этот закон с учетом национальных особенностей регулирует сбор, обработку, хранение и защиту персональных данных граждан:

1) согласия субъектов данных на обработку их информации;

2) обеспечения безопасности данных и соблюдения прав пользователей, таких как доступ и удаление данных.

В последние годы ужесточаются требования к компаниям по локализации данных и увеличиваются штрафы за нарушения в области цифровой безопасности[64].

Одним из явных рисков для физических лиц в связи с использованием платформы будет ограниченный контроль над персональными данными. По сути, у пользователей нет абсолютного права на данные (видеозаписи, аудиозаписи, текстовые сообщения), которые находятся в личном кабинете или в архивах приложения. Ни один из пользователей платформы не может что-либо удалить или отредактировать. Однако, хотя структура такого приложения ограничивает возможности пользователей по управлению личной и семейной информацией, заархивированные данные должны хранится в базах, поскольку могут являться доказательствами в спорах о воспитании детей. Соответственно, возникает оправданное беспокойство по поводу таких опасностей, как взлом баз приложения, возможные действия недобросовестных сотрудников, обеспечивающих работу платформы.

Возможное решение нам видится в следующих аспектах обращения с данными пользователей.

---

60 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 O.J. (L 119) 1.

61 Lei No. 13.709, de 14 de Agosto de 2018, as amended by Lei No. 13.853, de 8 de Julho de 2019, Diário Oficial da União de 8 Setembro 2019 (Braz.).

62 Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).

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

64 С 30 мая 2025 года увеличены размеры штрафов по общему составу нарушения в области персональных данных, ведены новые составы (Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» от 30.11.2024 № 420-ФЗ, http://publication.pravo.gov.ru/document/0001202411300011).

1. Обработка данных физических лиц

Согласие на обработку персональных данных несовершеннолетних по общему правилу предоставляется законными представителями[65]. Однако, поскольку ранее нами продвигался тезис об установлении решением суда графика виртуального общения ребенка с его родителем, данное требование вступает в системное противоречие с нормами семейного права. Отказ одного родителя предоставить согласие на виртуальное общение, при наличии вступившего в силу судебного акта о порядке общения, на наш взгляд, не имеет юридической силы (один из родителей не вправе самостоятельно запретить общаться ребенку с другим родителем) и может рассматриваться как нарушение права родителя и ребенка на общение, так и неисполнение судебного решения.

Однако мы понимаем, что, во-первых, необходимо обеспечить соблюдение Федерального закона «О персональных данных» и Федерального закона «Об информации, информационных технологиях и о защите информации»[66], а во-вторых, это предложение вызовет у ряда родителей недовольство. Но любое иное решение повлечет за собой возможность родителя, с которым определено место проживания ребенка, злоупотреблять своими родительскими правами, отказывая в предоставлении такого согласия. С другой стороны, можно соблюсти требования упомянутых федеральных законов, предоставив право давать согласие на обработку данных несовершеннолетнего родителю, проживающему отдельно. Ведь согласно российскому законодательству права родителей равны вне зависимости от того, с кем из них проживает ребенок. Либо можно квалифицировать отказ родителя, совместно проживающего с ребенком, предоставить согласие на обработку персональных данных как злоупотребление правом и форму фактического уклонения от исполнения, вступившего в законную силу судебного акта, определяющего порядок общения с ребенком (по логике ст. 10 ГК РФ и ст. 55, 66 СК РФ). В подобных случаях правовым основанием обработки данных целесообразно рассматривать необходимость исполнения обязанностей, вытекающих из судебного решения (абз. 3.1 ч. 1 ст. 6 и ч. 8. ст. 9 ФЗ «О персональных данных»). Еще одним вариантом решения этого вопроса могло бы быть (в известной мере условно) применение оговорки о личных и семейных нуждах (ч. 2 ст. 1 ФЗ «О персональных данных»), выводящая такую обработку из общего режима ФЗ «О персональных данных», поскольку она будет осуществляться исключительно для организации и поддержания общения (без избыточного распространения данных и при не нарушении прав ребенка).

В любом случае данный вопрос остается за рамками настоящей научной работы и подлежит дальнейшему изучению.

Должны соблюдаться стандарты для ИИ и обязательно национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 42001-2024 «Искусственным интеллект. Система менеджмента»[67], идентичный международному стандарту ISO/IEC 42001:2023[68]. В перспективе, при выходе платформы за пределы национального рынка потребуется соответствие требованиям европейского

[65] Ч. 6 ст. 9 Федерального закона «О персональных данных».

[66] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ. Собрание законодательства РФ, 2006, №31 (1 ч.), Ст. 3448.

[67] Национальный стандарт РФ ГОСТ Р ИСО/МЭК 42001-2024 «Искусственный интеллект. Система менеджмента», утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 28 октября 2024 г. № 1549-ст.

[68] International Organization for Standardization. (2023). *ISO/IEC 42001:2023: Information technology — Artificial intelligence — Management system.* https://www.iso.org/standard/42001

Общего регламента о защите персональных данных[69], Регламенту ЕС № 2024/1689 об установлении согласованных правил в отношении искусственного интеллекта[70] или аналогичным национальным законам иных стран о защите данных и ИИ, а также стандарту ISO/IEC 27701:2019 (расширяющий ISO/IEC 27001 и ISO/IEC 27002) в части управления режимом конфиденциальности данных и их трансграничной передачей[71].

2. Хранение данных

ИИ на данной платформе должен собирать данные, исходя из принципа минимизации[72]. Подсистема ИИ на основе мультимодальных моделей не будет сохранять анализируемые данные, за исключением случаев прямого указания пользователей или модераторов приложения (например, судебных приставов-исполнителей). Предлагается использовать отечественные мультимодальные модели на основе решений компаний «Яндекс» и «Сбер». При фиксировании конфликтных ситуаций, полагаем, нет необходимости устанавливать длительный срок хранения, достаточно одного года, а затем необходимо их анонимизировать.

3. Передача данных

Передача должна осуществляться только шифрованная, причем с шифрованием данных в покое и транзите (*Advanced Encryption Standard (AES)* 256 или выше). Нужно обеспечить прозрачность алгоритмов, осуществлять регулярные аудиты и пентесты (не реже одного раза в полгода и после значительных обновлений). Необходимо закрепить обязанность уведомлять пользователей в течении суток в случае взлома и утечки данных.

Стоимость разработки такой платформы может сильно варьироваться в зависимости от деталей: платформ (*iOS, Android,* веб-версия для ПК), уровня кастомизации нейросети, глубины интеграции с Госуслугами (требует *API*-доступа и соблюдения регуляций), функционала «виртуального родительства» (чат-боты, видео, аналитика).

Заключение

После расторжения брака возникает сложная ситуация, требующая государственного обеспечения взаимодействия всех трех субъектов родительского правоотношения, чтобы гарантировать благополучие ребенка и удовлетворить интересы обоих родителей.

---

[69] 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 O.J. (L 119) 1.

[70] Regulation 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), 2024 O.J. (L 1689) 1.

[71] International Organization for Standardization. (2023). *ISO/IEC 27001:2019: Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.* https://www.iso.org/ru/standard/71670.html

[72] Принцип минимализма в искусственном интеллекте основывается на требованиях ст. 5 Федерального закона «О персональных данных» (соответствие объема данных целям обработки и запрет на избыточность) и интерпретируется нами как пропорциональность: «собирай и обрабатывай ровно столько данных, сколько нужно для заявленных целей».

Всем детям приходится адаптироваться к жизни с одним родителем вместо двух, и этот процесс для большинства достаточно сложен. Одной из важнейших проблем является поддержание контакта и отношений с родителями, не проживающими с ними. Дети, которые не виделись с родителями, живущими отдельно, так часто, как им хотелось бы, или не имели контакта с родителями, не проживающими с ними, склонны сильнее переживать разлуку.

Постоянное и неоднократное создание препятствий, за исключением особых случаев, когда это вредит интересам ребенка, инструментализация детей, которая заключается не только в использовании несовершеннолетних для причинения вреда бывшему партнеру (возможно, путем лишения их возможности пользоваться правом на общение), но и в навязывании им ролей, которые не подходят ни для их возраста, ни для ситуации, в которой они находятся, ни для защищенного положения, которое должно быть им гарантировано в рамках семейной ячейки, являются недопустимыми.

«Виртуальное родительство», несмотря на то что является относительно новой концепцией, законодательно урегулировано в ряде стран. Более того, на мировом рынке в настоящее время достаточно много онлайн-приложений, позволяющих осуществлять онлайн-общение в рамках договоренностей разведенных родителей, а в отдельных государствах родителей обязуют использовать такой вид приложений.

Проведенное исследование показало, что российское законодательство не содержит норм, препятствующих включению в решение суда графика «виртуального родительства» как дополнительного средства общения с ребенком. На наш взгляд, рекомендации Верховного Суда РФ по обязательному включению периода «виртуального родительства» позволили бы сохранить эмоциональные и родственные отношения.

В исследовании предложены разработка, внедрение и варианты использования приложения с предлагаемым названием «Территория общения и доверия» с применением ИИ, интегрированного с государственными структурами, для предоставления цифрового коммуникативного пространства для общения разведенных родителей с ребенком и фиксации нарушений порядка общения.

Отметим, что, как и все остальное, программное обеспечение для совместной работы может быть использовано разведенными родителями недобросовестно, если они не готовы ставить интересы детей на первое место. Но, используя ее, все же можно снизить вероятность враждебного взаимодействия и исключить детей из взаимных эмоциональных разбирательств, а также помочь родителям сформировать нейтральные отношения ради благополучия своих детей. Благодаря доступным цифровым технологиям дети быстрее и легче адаптируются к периоду постразводных отношений, будучи уверены в том, что смогут поговорить с одним или обоими родителями в любое время при необходимости и не испытывать при этом чувство вины.

Список литературы / References

1. Arditti, J. A., & Keith, T. Z. (1993). Visitation frequency, child support payment, and the father–child relationship postdivorce. *Journal of Marriage and Family*, *55*(3), 699–712. https://doi.org/10.2307/353350
2. Augustijn, L., Claessens, E., Miettinen, A., Hakovirta, M., Mortelmans, D., Riser, Q., & Steinbach, A. (2025). Joint physical custody and mothers' life satisfaction in Belgium, Finland, and Germany. *Journal of Family Studies, 31*(3), 508–527. https://doi.org/10.1080/13229400.2025.2451192

3. Augustijn, L. (2022). The association between joint physical custody and children's mental health. Do children's experiences of parental loyalty conflicts moderate the relationship? *Children & Society*, *36*, 494–510. https://doi.org/10.1111/chso.12508
4. Berman, R., & Daneback, K. (2022). Children in dual-residence arrangements: A literature review. *Journal of Family Studies*, *28*(4), 1448–1465. https://doi.org/10.1080/13229400.2020.1838317
5. Bergström, M., Salari, R., Hjern, A, Hognäs, R., Bergqvist, K., & Fransson, E. (2021). Importance of living arrangements and coparenting quality for young children's mental health after parental divorce: A cross-sectional parental survey. *BMJ Paediatrics Open*, *5*(1), Article e000657. https://doi.org/10.1136/bmjpo-2020-000657
6. Bjarnason, T., & Amarsson, A. (2011). Joint physical custody and communication with parents: A cross-national study of children in 36 western countries. *Journal of Comparative Family Studies*, *42*(6), 871–890. https://doi.org/10.3138/jcfs.42.6.871
7. Campbell, A. J. (2020). Children's privacy laws must be strengthened and enforced. *JAMA Pediatrics, 174*(12), Article e203393. https://doi.org/10.1001/jamapediatrics.2020.3393
8. Cancian, M., Meyer, D. R., Brown, P. R., & Cook, S. T. (2014). Who gets custody now? Dramatic changes in children's living arrangements after divorce. *Demography, 51*(4), 1381–1396. https://doi.org/10.1007/s13524-014-0307-8
9. Das, G., Cheung, C., Nebeker, C., Bietz, M., & Bloss, C. (2018). Privacy policies for apps targeted toward youth: Descriptive analysis of readability. *JMIR Mhealth Uhealth, 6*(1), Article e3. https://doi.org/10.2196/mhealth.7626
10. Dunas, D. (2020). Sotsializatsiya i samorealizatsiya kak klyuchevyye motivy mediapotrebleniya [Socialization and self-realization as key motives of media consumption]. *Medi@lmanah*, (5), 25–34. https://doi.org/10.30547/mediaalmanah.5.2020.2534
11. Ermilova, A. V. (2015). Razvod glazami rebyonka: sotsiologicheskiy aspekt [Divorce through the eyes of a child: A sociological perspective]. *Vestnik Nizhegorodskogo Universiteta im. N.I. Lobachevskogo. Seriya: Sotsial'nyye Nauki,* (1), 115–120.
12. Filippova, T. A., & Titarenko, E. P. (2022) Ispolneniye soglasheniy v semeynom prave: probely pravovogo regulirovaniya [Performance of agreements in family law: Legal regulation gaps*]. Semeynoye i Zhilishchnoye Pravo*, (2), 29–32. https://doi.org/10.18572/1999-477X-2022-2-29-32
13. Flaquer, L. (2020). Shared parenting after separation and divorce in Europe in the context of the second demographic transition. In A-. M. Castrén, V. Česnuitytė, I. Crespi, J-. A. Gauthier, R. Gouveia, C. Martin, A. M. Mínguez, K. Suwada (Eds.), *The Palgrave handbook of family sociology in Europe* (pp. 377–398). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-73306-3_19
14. Hakovirta, M., Meyer, D. R., Salin, M., Lindroos, E., & Haapanen, M. (2023). Joint physical custody of children in Europe: A growing phenomenon. *Demographic Research, 49*, 479–492. https://doi.org/10.4054/DemRes.2023.49.18
15. Härkönen, J., Bernardi, F., & Boertien D. (2017). Family dynamics and child outcomes: An overview of research and open questions. *European Journal of Population, 33*(2), 163–184. https://doi.org/10.1007/s10680-017-9424-6
16. Haux, T., & Platt, L. (2021). Fathers' involvement with their children before and after separation. *European Journal of Population, 37*(1), 151–177. https://doi.org/10.1007/s10680-020-09563-z
17. Hetherington, E. M., & Stanley-Hagan, M. H. (2002). Parenting in divorced and remarried families. In M. H. Bornstein (Ed.), *Handbook of parenting: Being and becoming a parent* (2nd ed., pp. 287–315). Lawrence Erlbaum Associates Publishers.

18. Helms, T., Steinbach, A., & Augustijn, L. (2023). Joint physical custody in Germany: Legal framework and results of the Family Models in Germany (FAMOD) study. *International Journal of Law, Policy and the Family*, *37*(1), Article ebad010. https://doi.org/10.1093/lawfam/ebad010
19. Kairiene, B., Valackienė, A., & Blauzdžiūnaitė-Pavlovič, J. (2022). Ensuring the child's right to communication with both parents in the context of parental divorce: A Lithuanian case study. *Journal of Teacher Education for Sustainability, 24*(2), 67–82. https://doi.org/10.2478/jtes-2022-0017
20. Kalmijn, M. (2013). Long-term effects of divorce on parent – child relationships: Within-family comparisons of fathers and mothers. *European Sociological Review*, *29*(5), 888–898. https://doi.org/10.1093/esr/jcs066/
21. Kletsina, I. S. (2015). Situatsiya razvoda kak predmet otechestvennykh sotsiologicheskikh i sotsial'no-psikhologicheskikh issledovaniy semeynykh otnosheniy [Divorce in Russian sociological and social psychological research on family relationships]. *Social Psychology and Society*, *6*(3), 30-45. https://doi.org/10.17759/sps.2015060303
22. Marschall, A. (2017). When everyday life is double looped. Exploring children's (and parents') perspectives on post-divorce family life with two households. *Children and Society*, *31*(5), 342–352. https://doi.org/10.1111/chso.12202
23. Merla L., Dedonder J., & Baar M. (2025). Judicial treatment of applications for joint physical custody in Belgium: Criteria considered and underlying family normativities. *International Journal of Law, Policy and the Family*, *39*(1), Article ebaf015. https://doi.org/10.1093/lawfam/ebaf015
24. Murru, S., & Merla, L. (2025). Residential calendars in joint physical custody arrangements beyond the week on/week off model: Experiences of frequent alternating schedules and parental co-presence in Italy. *Child & Family Social Work. 30*(1), 1–14. https://doi.org/10.1111/CFS.70021
25. Meyer, D. R., Salin, M., Lindroos, E., & Hakovirta, M. (2025). Sharing responsibilities for children after separation: A European perspective. *Family Transitions*, *66*(1–2), 27–55. https://doi.org/10.1080/28375300.2024.2423432
26. Mikhalev, A. V. (2025) Vyyavleniye modeley povedeniya molodozhi v sotsial'nykh setyakh na osnove internet-analitiki [Identification of youth behavior patterns in social networks based on internet analytics]. *Prakticheskiy Marketing*, (7), 22–27. https://doi.org/10.24412/2071-3762-2025-7337-22-27
27. Mikheeva, L. Yu. (2004). *Opeka i popechitel'svo: teoriya i praktika* [Custody and guardianship: Theory and practice]. Wolters Kluwer.
28. Institutsii Iustiniana [The Institutes of Justinian] (D. Rassner, Trans.; L. L. Kofanov & V. A. Tomsinov, Eds.). (1998). Zertsalo. (Original work published ca. 533 C. E.).
29. Oehme, K., O'Rourke, K. S., & Bradley, L. (2021). Online virtual supervised visitation during the COVID-19 pandemic: One state's experience. *Family Court Review, 59*(1), 131–143. https://doi.org/10.1111/fcre.12555
30. Olifirovich, N., Zinkevich-Kuzemkina T. A., & Velenta T. F. (2006). *Psikhologiya semeynykh krizisov* [Psychology of family crises]. Rech.
31. Ortega-Gaspar, M., Moreno-Mínguez, A., & López-Narbona, A. (2021). Impact of joint physical custody and best interest of the child: Reflections from a critical review of empirical studies. *Journal of Divorce & Remarriage, 63*(2), 101–119. https://doi.org/10.1080/10502556.2021.1993014
32. Palkovitz, R. (2019). Expanding our focus from father involvement to father–child relationship quality. *Journal of Family Theory & Review*, *11*(4), 576–591. https://doi.org/10.1111/jftr.12352
33. Pavlenko, E. M. (2021). Obespecheniye nailuchshikh interesov i bezopasnosti detey: mezhdunarodnyye standarty i praktika v Rossii [Ensuring the best interests and safety of children: International standards and practice in Russia]. *Vestnik MGPU. Seriya: Yuridicheskiye Nauki,* 4(44), 75–84. https://doi.org/10.25688/2076-9113.2021.44.4.08

34. Payne, J. L., Smyth, B. M., Irving, M., Heard, G., & Althor, G. (2022). Family law professionals' views of post-separation parenting apps. *International Journal of Law, Policy and the Family, 36*(1), Article ebac029. https://doi.org/10.1093/lawfam/ebac029
35. Perkins, K. L. (2019). Changes in household composition and children's educational attainment. *Demography, 56*(2), 525–548. https://doi.org/10.1007/s13524-018-0757-5
36. Poli, M. (2023). *The impact of the best interests of the child on shared parenting and joint custody* [Doctoral dissertation, University of Turin & University of Antwerp]. University of Turin Campus Repository. https://iris.unito.it/retrieve/1f0c23ad-8f6e-40f1-9938-dfdf35b2107a/Marco%20Poli_JointPhD_The%20Impact%20of%20the%20Best%20Interests%20of%20the%20Child%20%20%20on%20Shared%20Parenting%20and%20Joint%20Custody%20%20.pdf
37. Poortman, A. R., & van Gaalen, R. (2017). Shared residence after separation: A review and new findings from the Netherlands. *Family Court Review*, *55*(4), 531–544. https://doi.org/10.1111/fcre.12302
38. Pyankova, A. F. (2025) Opredeleniye mesta zhitel'stva rebenka: v poiskakh balansa interesov [Determining the child's place of residence: In search of a balance of interests]. *Courier of Kutafin Moscow State Law University (MSAL)*, (7), 59–67. https://doi.org/10.17803/2311-5998.2025.131.7.059-067
39. Raley, R. K., & Sweeney, M. M. (2020). Divorce, repartnering, and stepfamilies: A decade in review. *Journal of Marriage and Family*, *82*(1), 81–99. https://doi.org/10.1111/jomf.12651
40. Safira, R., & Rozatul, J. (2025). The effects of parental divorce on children's self-confidence and independence. *Socrates: Journal of Education, Philosophy and Psychology*, *1*(4), 88–93. https://doi.org/10.63217/socrates.v1i4.168
41. Saini, M., Mishna, F., Barnes, J., & Polak, S. (2013). Parenting online: An exploration of virtual parenting time in the context of separation and divorce. *Journal of Child Custody*, *10*(2), 120–140. https://doi.org/10.1080/15379418.2013.796265
42. Sinelnikov, A. (2023). Sotsial'naya priyemlemost' ob'yektivnykh i sub'yektivnykh prichin dlya razvoda v sovremennoy Rossii [Social acceptability of objective and subjective reasons for divorce in modern Russia]. *Sotsiologicheskie Issledovaniya,* (4), 75–83. https://doi.org/10.31857/S013216250022703-6
43. Spaan, J., van Gaalen, R., & Kalmijn, M. (2022). Disentangling the long-term effects of divorce circumstances on father-child closeness in adulthood: A mediation analysis. *European Journal of Population*, *38*(5), 1183–1211. https://doi.org/10.1007/s10680-022-09636-1
44. Steinsbekk, S., Bjørklund, O., Valkenburg, P., Nesi, J., & Wichstrøm, L. (2024). The new social landscape: Relationships among social media use, social skills, and offline friendships from age 10–18 years. *Computers in Human Behavior*, *156*, Article 108235. https://doi.org/10.1016/j.chb.2024.108235
45. Steinbach, A., Augustijn, L., & Corkadi, G. (2021). Joint physical custody and adolescents' life satisfaction in 37 North American and European countries. *Family Process*, *60*(1), 145–158. https://doi.org/10.1111/famp.12536
46. Steinbach, A. (2019). Children's and parents' well-being in joint physical custody: A literature review. *Family Process*, *58*(2), 353–369. https://doi.org/10.1111/famp.12372
47. Temizyürek, K. (2018). Die richterliche Kindesanhörung: Bindungsfürsorge, Bindungstoleranz, Bindungsblockade [The judicial hearing of the child: Attachment caregiving, attachment tolerance, attachment blockade]. *Zeitschrift für Kindschaftsrecht und Jugendhilfe*, (8), 301–306. https://doi.org/10.5281/ZENODO.6126647
48. Toews, M. L., & McKenry, P. C. (2001). Court-related predictors of parental cooperation and conflict after divorce. *Journal of Divorce & Remarriage, 35*(1–2), 57–73. https://doi.org/10.1300/J087v35n01_03
49. Van Spijker, F., Kalmijn, M., & van Gaalen R. (2022). The long-term improvement in father–child relationships after divorce: Descriptive findings from the Netherlands. *Demographic Research, 46*(15), 441–452. https://doi.org/10.4054/DemRes.2022.46.15

50. Zartler, U. (2021). Children and parents after separation. In N. F. Schneider and M. Kreyenfeld (Eds.), *Research handbook on the sociology of the family* (pp. 300–313). Edward Elgar. https://doi.org/10.4337/9781788975544.00029

Сведения об авторе:

Ерохина Е. В. — кандидат юридических наук, доцент, доцент кафедры гражданского права и процесса, юридический факультет, Оренбургский государственный университет, Оренбург, Россия.
erohina.elena2020@gmail.com
ORCID: https://orcid.org/0000-0002-5793-2736

Information about the author:

Elena V. Erokhina — Ph.D. in Law, Associate Professor, Department of Civil Law and Procedure, Faculty of Law, Orenburg State University, Orenburg, Russia.
erohina.elena2020@gmail.com
ORCID: https://orcid.org/0000-0002-5793-2736

https://doi.org/10.38044/2686-9136-2025-6-3-67-93

СТАТЬИ

ПРАВОВОЙ РЕЖИМ УЧЕТНОЙ ЗАПИСИ: ЮРИДИЧЕСКИЕ ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ВИРТУАЛЬНОГО ОБЪЕКТА ПРАВА

В. О. Панин[1, 2]

[1]Институт государства и права Российской академии наук
119019, Россия, Москва, ул. Знаменка, 10

[2]Юридическая компания «К12»
125375, Россия, Москва, ул. Тверская, 14

Аннотация

Статья посвящена исследованию недостаточно разработанных в отечественной юридической науке вопросов о правовой природе учетной записи в информационной системе (на примере социальных сетей), а также о правовом статусе лица, имеющего законный интерес в защите принадлежащих ему учетных записей. На практике для обозначения субъекта, обладающего контролем над учетной записью, используются термины «пользователь», «обладатель», «участник», «правообладатель», «собственник» и пр. Цель исследования — сформулировать научно обоснованный вывод о правовой природе прав субъектов в отношении учетных записей как распространенного вида виртуальных объектов, а также рассмотреть особенности их правового режима. Автором рассмотрены существующие в науке подходы к определению правового режима учетной записи как объекта информационных и (или) гражданских правоотношений. С учетом анализа правоприменительной практики Соединенных Штатов Америки и Федеративной Республики Германия по вопросу принадлежности прав на учетную запись в социальной сети сделаны выводы о двойственной природе учетной записи как виртуального объекта. При проведении исследования использовались как общенаучные (анализ, синтез, аналогия), так и частнонаучные методы (сравнительно-правовой, формально-юридический методы). Принимая во внимание текущее состояние информационного и гражданского законодательства Российской Федерации, автор предлагает изменения в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», направленные на устранение существующего правового пробела и внесение определенности в общественные отношения, связанные с использованием учетных записей в социальных сетях. Делает вывод о том, что учетная запись является объектом информационных правоотношений — цифровыми данными, информационные правомочия в отношении которых (например, право обладания и право на предоставление доступа к учетной записи) в условиях экономики данных и цифровой экономики приобретают характеристику имущественных прав для целей участия в гражданском обороте. Полученные результаты могут быть использованы в законодательной и правоприменительной деятельности, в том числе при разрешении споров, связанных с принадлежностью учетных записей, а также при исследовании правовой природы иных разновидностей виртуальных объектов (цифровых валют, доменных имен и пр.).

Ключевые слова

виртуальные объекты, цифровые активы, цифровые данные, информация, учетная запись, обладатель информации, право собственности, цифровое право, социальные сети

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.
Для цитирования	Панин, В. О. Правовой режим учетной записи: юридические подходы к определению виртуального объекта права. *Цифровое право, 6*(3), 67–93. https://doi.org/10.38044/2686-9136-2025-6-3-67-93

Поступила: 19.07.2025, принята в печать: 28.08.2025, опубликована: 30.09.2025

ARTICLES

LEGAL REGIME OF ACCOUNT: APPROACHES TO DEFINING A VIRTUAL OBJECT OF LAW

Valerii O. Panin[1,2]

[1]The Institute of State and Law of The Russian Academy of Sciences
10, Znamenka St., Moscow, Russia, 119019

[2] K12 Law Firm
14, Tverskaya St., Moscow, Russia, 125375

Abstract

This article examines issues that have been insufficiently developed in Russian jurisprudence concerning the legal nature of accounts in information systems (on the example of social networks) and the legal status of persons who have a legitimate interest in protecting their accounts. In practice, various terms such as "user", "owner", "participant", "rights holder", "proprietor", etc. are used to refer to the entity that controls an account, which serves as a common type of virtual object. In setting out to formulate a scientifically sound conclusion about the legal rights of account subjects, we consider the features of their legal regime. Existing approaches to defining the legal regime of an account as an object of information and/or civil legal relations are analyzed in the light of law enforcement practice in the United States of America and the Federal Republic of Germany concerning social network account ownership to draw conclusions about the dual nature of accounts as virtual objects. The study is based on general (analysis, synthesis, analogy) and specific methods (comparative legal and formal legal approaches). Proposed amendments to Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies, and Information Protection" are aimed at eliminating the existing legal gap and bringing certainty to public relations related to the use of social media accounts. It is concluded that an account is an object of legal relations and digital data, the information rights to which (e.g., right of ownership and access to the account) acquire the characteristics of property rights in the context of the digital data economy for the purposes of participation in civil circulation. The results obtained can be used in legislative and law enforcement activities, including in the resolution of disputes related to the

ownership of accounts, as well as in the study of the legal nature of other types of virtual objects (digital currencies, domain names, etc.).

Keywords

virtual objects, digital assets, digital data, information, account, information holder, property right, digital right, social media

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Panin, V. O. Legal regime of account: Approaches to defining a virtual object of law. *Digital Law Journal, 6*(3), 67–93. https://doi.org/10.38044/2686-9136-2025-6-3-67-93

Submitted: 19 July 2025, accepted: 28 Aug. 2025, published: 30 Sep. 2025

Введение

Существующий опыт построения виртуальных игровых вселенных показывает, что между их пользователями чрезвычайно широко распространены отношения, связанные со сделками по отчуждению объектов виртуального мира. С точки зрения обычного пользователя функционал подобных виртуальных миров предоставляет ему возможность продать, купить либо подарить определенные объекты. В качестве примера можно привести торговую площадку виртуального мира *Second Life* (https://marketplace.secondlife.com/). Аналогичная ситуация и в иных многопользовательских виртуальных мирах[1].

Как указано в аналитическом отчете консалтинговой компании *Verified Market Research*[2], основные области, в которых осуществляется оборот виртуальных товаров — это социальные сети, виртуальные миры (например, *Second Life*) и многопользовательские игры (например, *Dota 2, League of Legends* и др.). К перечню виртуальных миров необходимо также отнести децентрализованные среды *Sandbox, Decentraland, PlanetIX* и т.п. При этом разграничение виртуальных миров и многопользовательских игр не совсем корректно, так как указанные категории соотносятся как общее и частное[3].

В литературе поднималась проблема, связанная с определением места, которое занимают в правовой системе права пользователей (участников) виртуальных сред в отношении создаваемых, используемых и отчуждаемых виртуальных ценностей. По нашему мнению, такие правомочия не относятся к сфере интеллектуальных прав, а применение лицензионной модели к отношениям сторон искусственно (Panin, 2022, p. 52).

---

1 Decentraland. Terms of Use ¶¶ 1–2, § 12.4. https://decentraland.org/terms/; Planet IX. Terms & Conditions. https://netempire.planetix.com/legal

2 Verified Market Research. (n.d.). *Virtual goods market: Size, forecast, and trends.* Retrieved 2026, February 2, from https://www.verifiedmarketresearch.com/product/virtual-goods-market/

3 Многопользовательские игры с оборотом виртуальных предметов, который в официальной плоскости осуществляется посредством торговой площадки, организованной правообладателем виртуального мира, представляют собой одну из разновидностей виртуальных миров. Другой разновидностью выступают виртуальные среды, называемые «песочницами» (*sandboxes*), к числу которых следует отнести виртуальный мир *Second Life*.

В настоящее время существует объективная потребность в научной разработке вопроса о правовом режиме виртуальных ценностей (объектов)[4]. С учетом их информационно-правовой природы целесообразно использовать инструментарий науки информационного права[5] для поиска подходящих правовых решений и развития научной дискуссии по данному вопросу. При этом необходимо учитывать текущее состояние информационного законодательства.

Специалистами в области информационного права неоднократно отмечалось, что в настоящее время информационное законодательство испытывает трудности, связанные с отсутствием взаимосвязанного нормативного понятийного аппарата, в рамках которого специальные категории берут начало в понятиях более общего порядка. В частности, В. Б. Наумов обоснованно указывает, что актуальная редакция Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[6] (далее — Закон об информации) использует различные категории в отношении информационной сферы: общее понятие «обладатель информации», которое должно быть системообразующим в рамках информационного законодательства, в нем фактически отсутствует, а в законодательных новеллах, напротив, употребляется термин «владелец» применительно к сайтам в сети Интернет, новостным агрегаторам и программам для электронно-вычислительных машин (Naumov, 2018, pp. 32–39).

Так, В. Б. Наумов подчеркивает, что одним из крупных достижений науки информационного права в начале 2000-х гг. был отказ от использования терминов «собственник» и «владелец» информации, которые существовали в Федеральном законе от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации»[7], посредством их замены на «обладателя информации» и «лицо, которому предоставлен доступ к информации». В настоящее время указанный результат фактически оказался утраченным (Naumov, 2018, pp. 33–34).

К сходным выводам об отсутствии терминологического единства в информационном законодательстве приходит Л. К. Терещенко, которая указывает на фундаментальное, с ее точки зрения, противоречие, заключающееся в следующем. В 2020 г. в Конституцию РФ было внесено понятие «оборот цифровых данных», содержание которого не было раскрыто на уровне отраслевого законодательства[8]. При этом термин «оборот» указывает прежде всего на экономическую составляющую операций с такими данными. С точки зрения Л. К. Терещенко, необходимо определить, включает ли смысловое множество «информация» в качестве составной

[4] Под виртуальным объектом в настоящей статье понимается совокупность данных, часть информационной системы, имеющая реальную экономическую ценность (например, учетная запись, доменное имя, виртуальная валюта, цифровая валюта, внутриигровые предметы и пр.).

[5] При проведении исследования автор руководствовался теоретическими положениями научной школы информационного права, сформированной в рамках Института государства и права РАН (основоположник — И.Л. Бачило). С позиций данной научной школы под информационным правом понимается комплексная отрасль российского права, регулирующая общественные отношения в области оборота информации (сбора, создания, хранения, распространения, использования и проч.) (далее — информационные правоотношения). В предмет информационно-правовых научных исследований включены вопросы правового режима информации, в том числе информационных объектов, вопросы правового статуса субъектов информационных отношений (например, пользователей социальных сетей), доступа к информации и др. См.: Bachilo et al., 2017; Polyakova & Troyan, 2025.

[6] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, Собрание законодательства РФ, № 31, 2006 г., ст. 3448 (часть I).

[7] Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ, Собрание Законодательства РФ, № 8, ст. 609.

[8] См. п. «м» ст. 71 Конституции Российской Федерации, принятой всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020, http://pravo.gov.ru/proxy/ips/?doc_itself=&nd=102027595#I0

части «цифровые данные» или в современных технологических реалиях они являются новой правовой категорией, отличной от «информации» (Tereshchenko, 2022, pp. 102–104).

К более решительным выводам приходят А. В. Минбалеев и Е. В. Холодная в разработанном ими проекте Концепции правового регулирования метавселенных, а именно, что цифровые данные являются ключевым активом в условиях экономики данных и метавселенной и требуют отдельного законодательного регулирования путем включения в нормативные акты определения цифровых данных и правовых режимов оборота разных типов данных[9]. Е. В. Холодная отдельно подчеркивает необходимость защиты «права собственности» на объекты, созданные с использованием метавселенных (Kholodnaya, 2024, p. 119).

Признание в научных исследованиях экономической составляющей данных и их квалификацию в качестве актива и товара следует поддержать. Подобный подход соответствует современным тенденциям развития сети Интернет, к числу которых относят ориентацию на данные, наделение пользователей элементами владения в отношении виртуальных ценностей, которые они создают и используют, предоставление им возможности управления данными (Krause, 2024, pp. 1–10).

Обозначим, что указанные вопросы находятся на пересечении информационного права и гражданского права, причем последнее в силу отраслевой принадлежности должно регулировать отношения, связанные с экономическим обменом, в том числе осложненным информационно-технологическим элементом. Однако цивилистической науке в отрыве от информационно-правовой составляющей не всегда удается однозначно разрешать возникающие правовые коллизии, что можно проследить на примере продолжающихся дискуссий о правовой природе бездокументарных ценных бумаг, цифровых финансовых активов, доменных имен и пр.

Анализ пользовательских соглашений и иных документов, заключаемых с пользователями (участниками) виртуальных сред, демонстрирует, что субъекты соответствующих отношений обозначаются терминами: «собственник», «владелец», «обладатель», «правообладатель», «пользователь», «участник»[10]. Кроме того, существуют различные виды виртуальных объектов: доменные имена, учетные записи в информационных системах (прежде всего социальных сетях), наименования учетных записей, цифровые валюты, виртуальные валюты, электронные денежные средства, внутриигровые предметы, иное виртуальное имущество, аватары и пр. Выявление общих черт регламентации соответствующих феноменов — одна из задач юридической науки в условиях развития экономики данных.

По утверждению П. У. Кузнецова, информация представляет собой фундаментальную правовую категорию, разновидности которой (именуемые исследователем отдельными элементами правовой структуры информации), например компьютерная информация, электронный документ, информационно-коммуникационная среда (ИКТ-среда) (как макрообъект[11]), имеют самостоятельное юридическое значение (Kuznetsov, 2005, p. 11).

---

[9] Минбалеев, А. В., & Холодная, Е. В. (2024, июль). *Проект концепции правового регулирования метавселенных*. МГЮА https://consortium.msal.ru/wp-content/uploads/2024/07/K_6-Koncepciya-regulirovaniya-metavselennyh.pdf

[10] Alien Worlds, *Terms of Use,* https://alienworlds.io/terms-of-use/; Decentraland. Terms of Use ¶¶ 1–2, § 12.4. https://decentraland.org/terms/; Planet IX. Terms & Conditions. https://netempire.planetix.com/legal

[11] Отдельные исследователи, например А. А. Стрельцов, подчеркивают, что ИКТ-среда как объект правового регулирования представляет собой юридическую фикцию, в соответствии с которой системе технических средств приписывают свойства суверенной территории для распространения на связанные с ней общественные отношения государственного суверенитета (Strel'tsov, 2019, p. 8).

С учетом широты исследуемой сферы, принимая во внимание вышеобозначенные противоречия в областях как информационного, так и частного права (и во избежание их усиления), с методологической точки зрения целесообразно последовательно рассмотреть вопросы регулирования отдельных разновидностей виртуальных объектов с целью получения достоверного научного знания об их правовой природе.

Настоящая статья посвящена анализу одного из распространенных виртуальных объектов — учетной записи в информационной системе (социальной сети, многопользовательской виртуальной среде и пр.), в отношении которой в отдельных юрисдикциях сформирована правоприменительная практика, анализ которой позволит сформулировать выводы относительно подходов к определению правового режима такого объекта, а также о наиболее подходящем термине для обозначения лица, которому принадлежит контроль над ним.

Кроме того, учетные записи как объект имеют не только самостоятельную ценность (применительно к социальным сетям), но и используются для учета иных виртуальных ценностей и обеспечения доступа к ним (например, к внутриигровым предметам, виртуальным и цифровым валютам и др.), в связи с чем полученные выводы могут иметь значение для научной разработки правового режима виртуальных объектов в целом.

Правовая природа учетной записи с точки зрения отечественной юридической науки

В науке гражданского права распространена точка зрения, в соответствии с которой учетная запись (аккаунт) не является объектом правовых отношений и объектом гражданских прав, представляя собой всего лишь часть функционала сайта социальной сети как сложного и составного объекта интеллектуальных прав[12]. Данная концепция ставит на первое место внутреннюю структуру объектов гражданских прав, фактически игнорируя международно-правовые тенденции обновления каталога прав человека применительно к ИКТ-среде, например право человека на цифровое (виртуальное) наследие, под которым понимается свободное определение судьбы данных и учетных записей, принадлежащих физическому лицу[13].

Иной точки зрения придерживается К. С. Митягин, рассматривающий учетную запись и страницу в социальной сети как результат интеллектуальной деятельности пользователя. Автор указывает, что для целей правовой охраны интересов создателя учетной записи возможна ее квалификация в качестве сложного объекта, составного произведения или базы данных (Mityagin, 2014). К. С. Митягин обоснованно отмечает, что в современных реалиях учетные записи в социальных сетях могут использоваться в коммерческих целях, являются «сетевыми местами скопления адресатов рекламы» (2014, pp. 74–77). При этом организации могут нести существенные затраты на ведение соответствующих социальных страниц, иметь необходимый штат сотрудников, в трудовые функции которых входит ведение таких страниц, в связи с чем они объективно заинтересованы в защите учетной записи как ценности, создаваемой в ходе подобной деятельности.

Е. С. Гринь указывает, что возможны различные трактовки правовой природы учетных записей в социальных сетях, например их рассмотрение как мультимедийного продукта, интернет-сайта (составного произведения), программы для ЭВМ, объекта *sui generis*. Оставляя

[12] Рожкова, М. А. (2024). *Можно ли рассматривать аккаунт как объект гражданских прав? Закон.ру.* https://zakon.ru/blog/2024/09/09/mozhno_li_rassmatrivat_akkaunt_kak_obekt_grazhdanskih_prav__can_an_account_be_considered_as_an_objec

[13] European Declaration on Digital Rights and Principles for the Digital Decade, 2023 O.J. (C 23) 1, pts. 1, 19, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOC_2023_023_R_0001

вопрос о правовой квалификации учетной записи открытым, Е. С. Гринь обращает внимание на то, что в условиях развития информационных технологий и коммерческой ценности учетных записей в социальных сетях *оставление их вне сферы правового регулирования не соответствует потребностям участников правоотношений*. Данный вывод автор делает в контексте анализа проблемы наследования учетных записей в социальных сетях, утвердительно отвечая на вопрос о возможности передачи по наследству учетной записи и права доступа к ней (Grin', 2022, pp. 130–134).

Кроме того, представляют интерес размышления Е. С. Гринь о необходимости разграничения передачи доступа к учетной записи и передачи всего комплекса прав на учетную запись (в том числе права на коммерческое использование) после смерти прежнего владельца. В действительности возможна ситуация, когда владелец учетной записи заинтересован в передаче исключительно сведений, содержащихся в учетной записи, например сообщений, фотографий, видеозаписей (информационный компонент), в случае своей смерти и не преследует цели передать иному лицу учетную запись как виртуальный актив (объект), который впоследствии может быть предметом коммерческих операций.

Возникает вопрос, допустима ли передача только права доступа к учетной записи в социальной сети без передачи иного комплекса прав (правовая природа которых на данном этапе исследования не определена), позволяющего свободно распоряжаться учетной записью в ИКТ-среде (например, опубликовывать новые сведения, использовать в целях извлечения прибыли и пр.). Думается, что это возможно при условии надлежащей технологической реализации со стороны правообладателя социальной сети.

Некоторые авторы признают информационно-правовую природу учетной записи в социальной сети, разграничивая ее состояния до определения содержания и после наполнения информацией (контентом), указывая, что в первом случае учетная запись является объектом информационного права, а во втором — объектом гражданских правоотношений (Fedorov, 2023, p. 152).

Часть исследователей, например А. Д. Крючкова, указывают на то, что нормы об интеллектуальной собственности не подходят для регламентации данных правоотношений и предлагают рассматривать учетную запись как иное имущество или цифровые права (Kryuchkova, 2021, p. 240).

В свою очередь, А. Д. Севергин, анализируя правовую природу метавселенной, указал, что фактически речь идет о данных как объекте информационных правоотношений. Кроме того, вопросы, связанные с виртуальной собственностью, отвечают признакам цифровых прав, предусмотренных гражданским законодательством (Severgin, 2023, pp. 40–43).

Таким образом, перечисленные позиции в отношении учетных записей в отечественной юридической науке целесообразно разделить на четыре основные группы:

1. концепции, отрицающие наличие у учетной записи в социальной сети атрибута объекта права (учетная запись не объект правовых отношений);
2. концепции, рассматривающие учетную запись через призму норм об интеллектуальной собственности и творческий вклад их создателей;
3. концепции, рассматривающие учетную запись как иное имущество или цифровое право;
4. концепции, признающие наличие у учетной записи двойственной природы: информационно-правовой до наполнения учетной записи информацией и появления определенного количества подписчиков и гражданско-правовой после возникновения указанных признаков.

Некоторые исследователи, не выбирая одну из вышеприведенных концепций (оставляя данный вопрос открытым), указывают на принципиальную возможность включения учетной

записи в социальных сетях в состав имущества, в том числе в состав общего имущества для целей последующего раздела в рамках бракоразводного процесса между супругами (Agaeva, 2023, pp. 5–7). Как видим, бóльшая часть концепций исходит из необходимости защиты прав обладателей учетных записей, однако из-за ограниченности отраслевыми рамками авторы применяют для решения этой задачи инструментарий только гражданского права, не задействуя терминологического потенциала науки информационного права, что не совсем верно.

Анализ зарубежной правоприменительной практики по вопросу принадлежности прав на учетные записи

Вышеприведенные обстоятельства свидетельствуют о необходимости разработки правового регулирования этой сферы, отвечающего потребностям участников правоотношений. В российском правовом поле отсутствуют судебные споры, связанные с юридической судьбой учетных записей в социальных сетях. Между тем иной результат демонстрирует изучение правоприменительной практики в иностранных юрисдикциях.

Опыт Соединенных Штатов Америки

В 2015 г. Суд по делам о банкротстве штата Техас (*U.S. Bankruptcy Court for the Southern District of Texas, Houston division*) рассматривал вопрос о признании аккаунтов в социальных сетях *Facebook*[14] и *Twitter*[15] имуществом организации, проходящей реабилитационную процедуру в рамках дела о несостоятельности (банкротстве)[16]. Спор был связан с учетными записями бенефициара, контролирующего должника, который от своего имени создал аккаунты в упомянутых социальных сетях, фактически посвященные деятельности организации (используемые для взаимодействия с клиентами, в рекламных и иных коммерческих целях).

Постановка вопроса о признании учетной записи имуществом и ее вхождении в конкурсную массу реорганизуемого должника была вызвана тем фактором, что для эффективного проведения реабилитационной процедуры был необходим доступ к учетным записям — основным маркетинговым и коммерческим инструментам, посредством которых осуществлялась экономическая деятельность общества. Его отсутствие ставило под угрозу исполнение реабилитационного плана. При этом ответчик по спору уклонялся от передачи доступа к учетным записям, аргументируя это нарушением его информационных прав, прежде всего права на тайну частной жизни, и личным характером учетной записи. Указанный факт существенным образом нарушал права кредиторов.

В результате суд на основе анализа сходных прецедентов в различных штатах разграничил личные и коммерческие учетные записи, включив последние в конкурсную массу должника — юридического лица для целей проведения процедур банкротства и расчетов с кредиторами. Для разграничения суд применил следующие критерии[17]:

[14] Правообладатель данной социальной сети — компания *Meta* — признан в Российской Федерации экстремистской организацией. Упоминание данных сведений носит исключительно научный характер и необходимо для целей исследования.

[15] Социальная сеть заблокирована в Российской Федерации на основании решения Генеральной прокуратуры РФ от 24 февраля 2022 г. в порядке ст. 15.3 Закона об информации.

[16] *Memorandum opinion on Jeremy Alcede's emergency motion objecting to proposed order regarding social media accounts*, No. 14-33564 (Bankr. S.D. Tex. Apr. 3, 2015), https://www.govinfo.gov/content/pkg/USCOURTS-txsb-4_14-bk-33564/pdf/USCOURTS-txsb-4_14-bk-33564-0.pdf

[17] Ibid., 9–19.

- анализ наименования аккаунта: наименование учетной записи, созданной бенефициаром, соответствовало названию общества;
- наличие иной связи с обществом: учетная запись отсылала к официальному сайту общества (в аккаунте была размещена ссылка на официальный сайт);
- содержание страницы и характер сообщений: абсолютное большинство сообщений преследовало коммерческие и рекламные цели, явно связанные с деятельностью общества.

Суд отклонил доводы ответчика о том, что он никому не передавал право администрирования учетной записи. Суд указал, что в данном случае фактически страница была создана в интересах общества и для ведения его деятельности. В подобной ситуации то обстоятельство, что технически администратором сообщества и создателем персональной страницы являлся ответчик, не имеет юридического значения[18], т. к. по материальному критерию (исходя из фактического содержания отношений по использованию учетной записи) фактически учетная запись принадлежит должнику.

Было также принято по внимание противоречивое поведение ответчика, который в предыдущих судебных разбирательствах по иным вопросам в ходе банкротного процесса (прежде всего по вопросу определения его собственного вознаграждения по трудовому договору за осуществление функций руководителя должника в предбанкротный период) указывал, что он ежедневно отвечает на тысячи сообщений с вышеупомянутых учетных записей в целях поддержания деловой репутации организации и взаимодействия с контрагентами, а в данном споре, напротив, обосновывал личный характер таких учетных записей[19].

Кроме того, судом был разрешен занимательный юридический вопрос, связанный с личным вкладом ответчика в развитие учетной записи. Отклоняя указанный довод, как не препятствующий передаче ответчиком доступа (логина и пароля) к учетной записи, суд констатировал следующее. Действительно, нельзя отрицать, что, несмотря на корпоративный характер учетной записи, контролирующее должника лицо внесло определенный вклад в ее развитие. Этот аспект предложено рассматривать в контексте деловой репутации организации и деловой репутации конкретного лица. Суд отметил, что в случае если значительный вклад в развитие учетной записи (например, количество активных подписчиков) внесен конкретным лицом, то объективно указанный фактор следует за деловой репутацией такого лица. Как следствие, при создании этим лицом новой или использовании иной учетной записи связанные с его личной деловой репутацией подписчики (иные пользователи), последуют за ним. Данный фактор, с позиции суда, не препятствует рассмотрению учетной записи в качестве имущества в контексте законодательства о банкротстве[20].

Суд также оценил возможность взыскания убытков за недобросовестные действия ответчика в отношении учетных записей. Ответчик, уклоняясь от передачи сведений, необходимых для доступа к учетным записям, совершил следующие действия, влияющие на их коммерческую ценность: изменил наименование учетных записей на собственные имя и фамилию и опубликовал сообщения (посты) диффамационного содержания. При этом правила использования одной из социальных сетей не предусматривали повторного изменения наименования учетной записи. Суд указал, что в случае если в результате досудебного или судебного взаимодействия с социальной сетью не удастся восстановить наименование учетной записи (например, посредством добавления в условия использования социальной сети возможности смены наименования в подобных ситуациях или создания дублирующей учетной записи с переносом всего

[18] Ibid., 18.
[19] Ibid., 15.
[20] Ibid., 20–22.

содержания и подписанных пользователей с исходной учетной записи), с бенефициарного владельца должника и технического администратора учетных записей могут быть взысканы убытки, причиненные совершенными им действиями[21]. При описании учетной записи как имущества должника суд использовал термин «имущественные интересы» (*property interests*)[22].

Таким образом, в рамках данной концепции суд исходит из юридического интереса организации как фактического обладателя учетной записи, в получении доступа к ней и защите соответствующих прав. Именно законный интерес выступает в качестве одного из элементов, формирующих ядро правового статуса пользователя в виртуальных средах. В данном примере для описания лица, имеющего права в отношении учетной записи, судом использован термин «собственник»[23], без определения конкретного вида собственности (объекта гражданских прав) с указанием на имущественные интересы. Суд также остановился на вопросе о правовой квалификации личных учетных записей, которые он связал с категорией *persona* (альтер эго), т. е. с интересом субъекта в использовании собственной идентичности, который может быть выражен в использовании имени, псевдонима или иного объекта (например, учетной записи) в личных целях или для выгоды иных лиц[24].

В контексте использования американским судом категории «имущественные интересы» для определения гражданско-правового режима учетных записей отметим, что указанный подход возможно применить и в Российской Федерации для юридического оформления операций в рамках экономики данных с учетом открытого перечня имущественных прав. При этом категория имущественных прав позволит решить задачу юридического оформления оборота виртуальных объектов, однако не даст ответа на вопрос об их правовой природе, так как имущественные права возникают в отношении какого-либо объекта. Например, имущественное право на использование имени имеет объектом имя как нематериальное благо (необходимо различать право на использование имени и право на имя, которое неотчуждаемо[25]). Аналогичным образом объектом исключительных (имущественных) прав на программы для ЭВМ, произведения, базы данных и пр. выступают конкретные результаты интеллектуальной деятельности.

Актуальность использования категории «имущественное право» для оформления оборота виртуальных объектов подчеркивается в научной литературе (Rozhkova, 2024, p. 118). Отдельные авторы применительно к уголовно-правовой квалификации деяний, направленных на хищение цифровых активов (на примере внутриигровых ценностей, осложненных использованием технологии распределенного реестра), считают возможным рассматривать конвертируемую виртуальную внутриигровую валюту в качестве имущества (и, как следствие, предмета

[21] *Memorandum opinion on Jeremy Alcede's emergency motion objecting to proposed order regarding social media accounts*, No. 14-33564 (Bankr. S.D. Tex. Apr. 3, 2015), pp. 25–26, https://www.govinfo.gov/content/pkg/USCOURTS-txsb-4_14-bk-33564/pdf/USCOURTS-txsb-4_14-bk-33564-0.pdf

[22] Ibid., 10–11.

[23] В данном контексте необходимо учитывать особенности англо-американского понимания концепта «собственность» (property), который по содержанию сконцентрирован на конкретных правомочиях лица в отношении определенных благ и современные трактовки которого не ограничены пониманием вещи как строго телесного объекта окружающего мира. См. статью А. М. Доева (Doiev, 2023).

Акцент на социальной природе юридической категории вещи (как объекта, воспринимаемого органами чувств) и на конкретных правомочиях субъекта в отношении такой вещи позволяет судам в США применять конструкцию «собственности» к отношениям, связанным с цифровыми (виртуальными) объектами, в данном случае — с учетными записями.

[24] *Memorandum opinion on Jeremy Alcede's emergency motion objecting to proposed order regarding social media accounts*, No. 14-33564 (Bankr. S.D. Tex. Apr. 3, 2015), https://www.govinfo.gov/content/pkg/USCOURTS-txsb-4_14-bk-33564/pdf/USCOURTS-txsb-4_14-bk-33564-0.pdf

[25] Пункт 2 Обзора судебной практики Верховного Суда РФ № 1 (2023), утв. Президиумом Верховного Суда РФ 26 апреля 2023 г.

хищения), а также считать имуществом отдельные виртуальные предметы в случае признания их цифровыми правами (Khromov & Zyablikov, 2024, pp. 46–67).

Обратим внимание на то, что пояснительная записка к законопроекту № 424632-7 (Федеральный закон от 18 марта 2019 г. № 34-ФЗ) непосредственно указывает, что категория «цифровое право» вводится в гражданское законодательство с целью регулирования рынка цифровых объектов, конкретный перечень которых впоследствии будет определяться законодателем посредством указания на их виды в федеральном законодательстве, исходя из степени влияния того или иного цифрового объекта на экономику страны (следовательно, указанный перечень может быть расширен)[26].

С учетом направленности воли законодателя на обновление понятийного аппарата гражданского законодательства выдвинем предположение, что в имущественных правоотношениях в цифровой среде целесообразно использовать термин «цифровое право» (понимая под ним имущественное, в том числе обязательственное, и иное право в отношении цифрового объекта). Аналогичный подход использован в проекте Цифрового кодекса Республики Казахстан, размещенном в открытом доступе на информационном ресурсе *Github* депутатом Мажилиса Парламента Республики Казахстан Е. В. Смышляевой[27].

С учетом изложенного вновь подчеркнем, что регламентация подобного рода отношений не ограничивается инструментарием интеллектуального права. Его применение в ситуациях, явно не рассчитанных на такое использование (например, правовой режим учетных записей и оборот иных виртуальных объектов), излишне (Fairfield, 2023, p. 20)[28].

Вернемся к анализу правоприменительной практики Соединенных Штатов Америки. В 2024 г. Апелляционный суд второго округа США вынес постановление по вопросу «права собственности» на учетные записи в социальных сетях *Instagram*[29] и *Pinterest* в рамках трудового спора между бывшим работником и работодателем, отменив судебный акт Окружного суда Южного округа Нью-Йорка и направив дело на новое рассмотрение[30].

Данное дело интересно тем, что в нем судом первой инстанции был применен многофакторный тест, сформулированный в 2015 г. Судом по делам о банкротстве штата Техас в деле, описанном выше. Однако суд апелляционной инстанции, указав на то, что судебное постановление, которым руководствовался окружной суд, вынесено в другом штате, сформулировал иной подход к определению «права собственности» на учетные записи.

Обстоятельства дела следующие. Ответчик по спору — Хейли Гутман, модельер, которая занимается разработкой дизайнов одежды. В 2011 г. между ней и организацией *JLM Couture*, специализирующейся на производстве премиальной свадебной одежды, был заключен трудовой договор, в соответствии с которым она как работник приняла на себя обязательства

[26] Пункты 2–3 Пояснительной записки к законопроекту «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» № 424632-7. https://sozd.duma.gov.ru/bill/424632-7

[27] См. п. 3 ст. 11 Проекта Цифрового кодекса Республики Казахстан, 2024. *GitHub*. https://github.com/Akylbay-Katira/digital-codex/blob/main/digital-Codex-2024-ru.md

[28] Например, в законодательстве и юридической литературе не предлагают для квалификации цифровых валют или электронных денежных средств использовать инструментарий интеллектуального права. Применение указанных правовых средств к иным видам виртуальных объектов (учетным записям, внутриигровым предметам в виртуальных средах, доменными именам и пр.) на данном этапе недостаточно обоснованно.

[29] Правообладатель данной социальной сети — компания *Meta* — признан в Российской Федерации экстремистской организацией. Упоминание данных сведений носит исключительно научный характер и необходимо для целей исследования.

[30] *JLM Couture, Inc. v. Gutman* 91 F.4th 91, No. 21-2535, 2024 WL 172609 (2d Cir. 2024).

по разработке дизайнов свадебной одежды. Трудовой договор также содержал условия о неконкуренции ответчика с *JLM Couture* и о передаче работодателю прав на использование имени и фамилии работника, в том числе для их регистрации в качестве товарного знака.

Кроме того, стороны предусмотрели, что исключительные права на результаты интеллектуальной деятельности, созданные, задуманные или разработанные Хейли Гутман в связи с ее работой в *JLM Couture*, принадлежат организации (служебное произведение)[31]. Через некоторое время после трудоустройства работником были созданы учетные записи в социальных сетях *Instagram*[32] и *Pinterest,* в которых впоследствии, помимо сообщений личного характера, также были опубликованы рекламные сообщения, связанные с деятельностью организации и дизайнами одежды, разрабатываемой работником. Кроме того, Хейли Гутман передала данные, необходимые для доступа к учетной записи, нескольким сотрудникам организации в целях публикации рекламных материалов. В 2019 г., не договорившись об изменении условий трудового договора, работник расторг его в одностороннем порядке и заблокировал доступ *JLM Couture* к учетным записям (было произведено изменение пароля). Работодатель обратился в суд с требованием о предоставлении доступа к учетным записям, а также заявил ходатайство о передаче организации управления учетными записями на период рассмотрения спора.

Окружной суд, удовлетворяя ходатайство и обязывая бывшего работника передать организации доступ к учетным записям, руководствовался критериями, сформулированными Судом по делам о банкротстве штата Техас.

Суд первой инстанции проверял следующие обстоятельства: отражает ли наименование учетных записей название организации или, напротив, персональные данные работника; каково содержание учетных записей; включают ли они ссылки на сайты в сети Интернет, принадлежащие организации; использовались ли учетные записи в рекламных целях, связанных с организацией; имели ли сотрудники или участники организации доступ к учетным записям и участвовали ли в управлении ими[33].

Установив, что содержание учетных записей включало в себя публикации рекламного характера, связанные с деятельностью работодателя, а также то обстоятельство, что несколько работников организации имели доступ к учетной записи и возможность публикации сообщений, суд удовлетворил ходатайство *JLM Couture.* Суд отклонил доводы ответчика об указании в наименовании учетной записи ее личных данных (имени и фамилии), а также о том, что работодателем не представлено доказательств, что учетные записи были созданы по его указанию и в рамках исполнения трудовых обязанностей. Суд также посчитал дополнительным аргументом в пользу вывода о том, что работодатель является правообладателем учетных записей, тот факт, что Хейли Гутман передала организации права на использование своего имени, в том числе в качестве товарного знака, а также согласилась на то, что все исключительные права в отношении результатов ее интеллектуальной деятельности в организации будут принадлежать последней[34].

---

31 JLM Couture, Inc., ¶¶ 4–5.

32 Правообладатель данной социальной сети — компания *Meta* — признан в Российской Федерации экстремистской организацией. Упоминание данных сведений носит исключительно научный характер и необходимо для целей исследования.

33 Barrett, S. J., & Rios, G. (2024, February 8). *"Handle" with care: Second Circuit clarifies ownership test for social media accounts.* Wilson Elser. https://www.wilsonelser.com/publications/handle-with-care-second-circuit-clarifies-ownership-test-for-social-media-accounts

34 Goldman, E. (2024, January 24). Courts still have no clue how to determine who owns social media accounts. *Technology & Marketing Law Blog.* https://blog.ericgoldman.org/archives/2024/01/courts-still-have-no-clue-how-to-determine-who-owns-social-media-accounts-jlm-v-gutman.htm

Отменяя судебный акт окружного суда, Апелляционный суд второго округа США указал следующее[35].

То обстоятельство, что определение «права собственности» на аккаунты в социальных сетях является новым для юридической сферы, не позволяет применять новые критерии (многофакторные тесты) в отрыве от уже существующей юридической методологии. Со спорными учетными записями следует обращаться как с любой другой разновидностью собственности[36].

На основании изложенного апелляционный суд сделал вывод о том, что если будет установлено, что Хейли Гутман использовала свою личную информацию и создала учетные записи для личного пользования (которое может в том числе иметь коммерческую направленность), т. е. совершила указанные действия не по поручению работодателя, а в своем интересе, в таком случае следует признать, что права на учетные записи принадлежали ей, вне зависимости от того, каким образом аккаунты могли быть использованы впоследствии[37].

Апелляционный суд отклонил ссылки *JLM Couture* на то, что ответчик передал обществу исключительные права на использование части результатов интеллектуальной деятельности, размещенных в учетных записях. Суд отметил, что данный довод свидетельствует только о передаче организации исключительных прав на результаты творческого труда *и не подтверждает передачу ответчиком права собственности на спорные учетные записи, которые не отнесены к сфере регулирования интеллектуального права*[38]. Указанный вывод является юридически значимым, так как также подтверждает ранее сформулированный тезис об искусственном характере применения норм об интеллектуальной собственности к отношениям, связанным с оборотом виртуальных объектов.

Таким образом, в Соединенных Штатах Америки формируется судебная практика, в соответствии с которой учетные записи в социальных сетях признаются объектом имущественных интересов и «права собственности». Показательно, что появление подобных судебных решений связано с достаточно конфликтными отраслями законодательства — сферой несостоятельности (банкротства) и трудовым правом. При этом следует сделать важное замечание: при внимательном анализе постановлений Суда по делам о банкротстве штата Техас и Апелляционного суда второго округа США можно установить, что данные права в силу их возникновения и существования в рамках информационной системы, с которой у «собственника» (обладателя) учетной записи заключено соглашение, имеют определенные ограничения. Как указано выше, Суд по делам о банкротстве штата Техас для описания указанных прав использует категорию «имущественный интерес», конкретно не определяя учетные записи в системе объектов права собственности. Апелляционный суд второго округа США отмечает, что конкретные правомочия «собственника», например право на передачу прав на учетную запись (т. е. оборотоспособность такой учетной записи), могут зависеть от содержания пользовательских соглашений с правообладателем социальной сети[39]. Подобный подход, с точки зрения англо-американского права, не противоречит содержанию понятия «собственность» (*property*), которое воспринимается

[35] JLM Couture, Inc. ¶¶ 16–17.

[36] Ibid. ¶ 17.

[37] Отметим, что экономическая составляющая указанного спора заключалась в том, что спорные учетные записи имели более 1 млн подписчиков, а стоимость одного рекламного сообщения составляла около 30 тыс. долл. США (Finguerra DuCharme, D., Kohn, F., & A. Belhachmi. (2024, March 22). *Social media account ownership: When a business relationship breaks down, who gets the accounts?* https://www.law.com/newyorklawjournal/2024/03/22/social-media-account-ownership-when-a-business-relationship-breaks-down-who-gets-the-social-media-accounts/).

[38] JLM Couture, Inc. ¶ 18.

[39] Ibid. ¶ 18.

как совокупность («пучок») различных правомочий, объем которых может различаться в зависимости от конкретной формы собственности (Doiev, 2023, pp. 11–13).

Иными словами, правоприменительная практика в Соединенных Штатах Америки приходит к двум ключевым выводам. Во-первых, юридический интерес пользователей в отношении учетных записей может иметь имущественное содержание и должен быть обеспечен судебной защитой. Во-вторых, конкретный набор правомочий обладателя учетной записи зависит от условий использования социальной сети. В контексте споров между третьими лицами, не являющимися правообладателями социальной сети, необходимо защищать интересы лица, которое создало учетную запись в собственных интересах (например, физическое лицо, которое одновременно является работником организации). В силу принципа свободы договора допустима передача как права использования учетной записи посредством предоставления права доступа к ней иным лицам, так и прав обладателя («собственника») учетной записи, если это не запрещено условиями использования социальной сети.

Отметим, что позиция Апелляционного суда второго округа США не противоречит выводам Суда по делам о банкротстве штата Техас, так как общий критерий определения первого владельца — создателя социальной страницы — не подлежит применению в ситуации с *мнимой собственностью*, когда субъект выступает исключительно номинальным держателем учетной записи, фактически используемой в интересах организации. Общее правило может быть применено в спорах между независимыми субъектами, не имеющими общих экономических интересов (например, бывший работник и работодатель). Исключение, связанное с более тщательной проверкой отношений сторон, необходимо в спорах между аффилированными лицами (участник общества и общество), особенно в ситуации несостоятельности организации, когда действиями участника нарушаются права сообщества кредиторов.

Расширенная проверка была применена судом также в деле *Teamsters Local 651 v. Philbeck,* в рамках спора о принадлежности учетной записи между профессиональным союзом и его бывшим председателем. Суд установил, что фактически учетная запись создавалась и использовалась в интересах профессионального союза, в связи с чем не принадлежит ответчику (адреса учетных записей были указаны на официальном сайте профессионального союза, использовались в его визитных карточках, фактическое управление учетными записями осуществляли работники профессионального союза). Суд расценил как недобросовестные действия председателя по изменению данных, необходимых для доступа в учетную запись, которые были совершены после проигрыша выборов на должность[40].

Опыт Федеративной Республики Германия

На данном этапе нами были выделены отдельные особенности рассмотрения споров в отношении учетных записей в США. Перейдем к анализу дела, рассмотренного в 2018 г. Федеральным верховным судом Германии[41].

Краткая фабула спора такова. Несовершеннолетняя девушка, имеющая гражданство Федеративной Республики Германия (ФРГ), зарегистрировала учетную запись в социальной сети *Facebook*[42] в 2011 г. В 2012 г. при невыясненных обстоятельствах она была сбита поездом

[40] Int'l Bhd. of Teamsters Local 651 v. Philbeck, 464 F. Supp. 3d 863 (E.D. Ky. June 3, 2020).

[41] Bundesgerichtshof [BGH] [Federal Court of Justice] Jul. 12, 2018, III ZR 183.

[42] Правообладатель данной социальной сети — компания Meta — признан в Российской Федерации экстремистской организацией. Упоминание данных сведений носит исключительно научный характер и необходимо для целей исследования.

в метрополитене на территории ФРГ. В целях установления обстоятельств гибели своей дочери ее родители, вступившие в наследство, предприняли попытку получить доступ к учетной записи девушки, так как им стали известны идентификационные данные (логин и пароль). Однако ввиду установления для ученой записи так называемого мемориального статуса со стороны правообладателя социальной сети наследники не смогли получить доступ к содержанию учетной записи (сообщениям, аудио- и видеозаписям и пр.). Администрация социальной сети в досудебном порядке отказалась предоставить доступ, мотивируя негативный ответ условиями использования социальной сети. Наследники обратились в суд с требованиями к социальной сети об обеспечении доступа к ученой записи[43].

Суд первой инстанции удовлетворил заявленные требования, однако суд апелляционной инстанции решение суда первой инстанции отменил и в удовлетворении исковых требований отказал, мотивируя это тем, что специальное информационное законодательство в области связи, исходя из его толкования, запрещает передачу сведений, хранящихся на серверах, используемых социальной сетью. Передача доступа к учетной записи повлечет за собой нарушение конфиденциальности содержащихся в ней сведений, в том числе связанных с иными лицами, с которыми наследодатель вступал в коммуникацию в рамках социальной сети.

Федеральный верховный суд Германии с выводами апелляционного суда и доводами представителя социальной сети не согласился, сформулировав следующие юридически значимые выводы.

1. Право на доступ к учетной записи вытекает из договорного обязательства, которое перешло к наследникам в порядке универсального правопреемства[44]. Суд отдельно отмечает, что указанное право не является имущественным[45], что полностью соответствует правовой природе права на доступ в российском законодательстве (иными словами, это информационное право, основанное на договоре). При этом Федеральный верховный суд Германии обращает внимание на то, что правовая природа договора о создании и использовании аккаунта остается неясной, однако в силу специфики конкретного дела данное обстоятельство было признано не имеющим решающего значения для разрешения спора[46]. Отметим, что даже в этой формулировке суд ведет речь о создании и использовании аккаунта как объекта, в отношении которого возникает право на доступ, а не о лицензионных правоотношениях, хоть и уходит от рассмотрения вопроса об обсуждении правовой природы связанного с учетными записями договора.

Суд указывает, что с момента вступления в наследство к наследникам перешли права и обязанности наследодателя по договору о создании и использовании аккаунта, в том числе право на доступ к учетной записи[47]. При этом иное могло быть предусмотрено соглашением сторон[48].

2. Запрет доступа к учетной записи наследникам наследодателя неуместно ущемляет права и законные интересы таких наследников, подрывает их правовое положение, что противоречит

[43] BGH, III ZR 183/17, Rn. 2–5.

[44] Ibid., 8.

[45] Ibid., 29.

[46] Ibid., 8.

[47] Ibid., 9.

[48] Интересно, что суд приходит к выводу, что согласно общим принципам регулирования соответствующих отношений наследование указанных прав могло быть исключено на уровне соглашения сторон, однако из пользовательского соглашения подобного не усматривается. С нашей позиции, указанный вопрос должен быть включен в сферу публично-правового регулирования, в котором следует предусмотреть нормы, гарантирующие переход прав по договору в порядке наследования, связанных с участием в многопользовательских социальных сетях со значительным охватом участников.

немецкому законодательству[49]. Ни тайна связи, ни право на конфиденциальность данных и неприкосновенность частной жизни иных субъектов, с которыми состоял в переписке наследодатель, не могут служить основанием для отказа в предоставлении доступа к учетной записи[50]. Напротив, суд приходит к выводу, что при предоставлении наследникам доступа к учетной записи тайна связи с юридической точки зрения не нарушается[51], так как происходит замена уполномоченного лица в отношении учетной записи, т. е. одной из сторон в уже существующем правоотношении, без возникновения новых правоотношений с иным лицом[52]. С учетом того что право доступа имеет информационно-правовую природу, данный вопрос интересен в контексте разработки института правопреемства в информационном праве, который в настоящее время фактически не исследуется[53].

3. Суд *obiter dictum* отмечает, что, вероятнее всего, дальнейшее активное использование аккаунта не охватывается правом наследования (это применимо в большей степени к личным учетным записям). Однако суд оставил данный вопрос без дальнейшего обсуждения с учетом предмета заявленных требований и обстоятельств спора. Он указал, что в ситуации, когда истцам необходим доступ к учетной записи в том состоянии, в котором она была на момент открытия наследства, отсутствуют какие-либо причины отказывать в реализации подобного права[54].

4. Суд указывает, что с учетом реального положения дел не выдерживают критики аргументы *Facebook*[55] о том, что их обязательство по передаче сообщений между пользователями связано с конкретным лицом (лицами). Федеральный верховный суд Германии отмечает: в связи с тем, что достоверно определить, владелец учетной записи или иное лицо использует аккаунт в конкретный момент, невозможно и определенная степень анонимности имманентно присуща подобного рода коммуникации, следует признать, что *соответствующие обязательства связаны с учетными записями, а не с лицами*[56]. Аккаунты выступают идентификационными признаками адресата и адресанта, продолжают существовать после их смерти[57]. Отметим, что именно поэтому в большинстве социальных сетей запрещено создание фальшивых аккаунтов с учетом указанного риска из сферы идентификации. При этом обладатель учетной записи несет всю ответственность за любые действия, совершенные третьим лицом в результате неправомерного доступа к учетной записи.

5. Участники коммуникации в социальных сетях должны разумно ожидать и учитывать, что доступ к переписке может быть получен наследниками их собеседников в порядке универсального правопреемства[58]. Федеральный верховный суд Германии также констатиру-

[49] BGH, III ZR 183/17, Rn. 12.

[50] Ibid., 7.

[51] Ibid., 27.

[52] Предоставление доступа к учетной записи иному лицу происходит не в рамках нового правоотношения, а в пределах уже существующего.

[53] Поисковой запрос «правопреемство в информационном праве» в электронном каталоге Российской государственной библиотеки не выявил никаких подходящих исследований (https://search.rsl.ru/ru/search).

[54] Изложенное подтверждает обозначенную Е. С. Гринь дискуссию о необходимости разграничения передачи доступа к учетной записи и передачи всего комплекса прав на учетную запись (Grin', 2022, pp. 133–134).

[55] Правообладатель данной социальной сети — компания *Meta* — признан в Российской Федерации экстремистской организацией. Упоминание данных сведений носит исключительно научный характер и необходимо для целей исследования.

[56] BGH, III ZR 183/17, Rn. 17, 34.

[57] Ibid.

[58] Ibid. Rn. 20.

ет, что если бы переписка была распечатана наследодателем или выгружена на хранилище персонального компьютера, наследники не имели бы никаких препятствий к доступу и ознакомлению с соответствующими сведениями[59]. Установление неравенства в двух сущностно сходных ситуациях несправедливо[60].

Не усмотрел суд противоречий и с Общим регламентом по защите данных (*General Data Protection Regulation, GDPR*[61]), указав, что наследник в таком случае становится оператором персональных данных в отношении сведений партнеров по переписке наследодателя и обязан обеспечивать конфиденциальность таких данных. На защиту персональных данных умерших лиц *GDPR* не распространяется[62].

Завершая рассуждения, Федеральный верховный суд Германии разграничивает право доступа к учетной записи и к содержащимся в ней имущественным[63] и личным материалам как к двум разным категориям[64], что в очередной раз свидетельствует о том, что учетная запись — это объект, в отношении которого могут возникать информационные права и обязанности и который в связи с этим подлежит правовому регулированию. При этом содержание учетной записи также может быть предметом правового регулирования. Фактически в зависимости от сферы применения аккаунты могут использоваться для учета иных ценностей: цифровых валют, цифровых активов, виртуальных внутриигровых предметов, виртуальных валют (в широком смысле) и др.

Таким образом, правоприменительная практика в ФРГ[65] и США разграничивает личные и корпоративные учетные записи, правовой режим которых может различаться (например, дальнейшее использование личной учетной записи при правопреемстве в порядке наследования может не допускаться; само правомочие на создание и управление личной учетной записью в США связывают с реализацией права на использование собственной идентичности (*a persona*) в ИКТ-среде)[66]. В США права субъектов в отношении учетных записей рассматриваются через призму теории собственности, причем к пользователю применяется термин «собственник». При этом с учетом того, что суды не могут игнорировать объективные особенности взаимодействия с социальной сетью, к учетным записям применяется термин «имущественный

---

[59] Интересно, что подобные сведения, наряду с дневниками и письмами, Федеральный верховный суд Германии называет термином «аналоговые документы» (*analoge dokumente*), впоследствии указывая, что нет оснований по-разному регламентировать отношения, связанные с аналоговым и цифровым контентом (*analoge und digitale Inhalten*).

[60] BGH, III ZR 183/17, Rn. 20, 28.

[61] 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 o.J. (l 119) 1.

[62] Ibid. Rn. 31.

[63] Суд косвенно признает, что определенный содержательный аспект учетной записи может иметь имущественный характер (например, к учетной записи может быть привязано определенное количество виртуальной валюты, иных ценностей). Развивая данную логику, к имущественной составляющей учетной записи следует отнести право на использование доменного имени и наименования учетной записи, которые в отдельных случаях могут выступать объектами экономического оборота.

[64] BGH, III ZR 183/17, Rn. 35–36.

[65] Корпоративные аккаунты отдельно не упоминались в рассмотренном решении Федерального верховного суда Германии, однако их выделение допустимо, исходя из общего анализа судебного акта, определившего правовой режим *личной* учетной записи в ситуации наследования.

[66] По аналогичным причинам, как правило, в пользовательских соглашениях запрещено отчуждение личных учетных записей.

интерес» и указывается, что конкретное содержание прав пользователя («собственника»), а также их оборотоспособность во многом определяются соглашением с правообладателем социальной сети.

В ФРГ, напротив, отношения с правообладателем социальной сети рассматриваются через информационно-правовой аспект (в контексте права доступа)[67], через призму обязательственных отношений сторон, с акцентом на то, что право доступа к учетной записи является самостоятельным, хоть и тесно связано с правом доступа к содержащимся в учетной записи сведениям. Федеральный верховный суд Германии также признает, что содержание учетной записи может иметь имущественный характер, что может быть использовано при анализе правовой природы прав пользователя на виртуальную валюту, внутриигровые ценности, наименование учетной записи, на использование поддоменного имени и др. Важно, что фактически суды в обеих юрисдикциях признают, что учетные записи — это объекты правового регулирования и правового интереса.

Подводя итог рассмотрению германского и американского опыта, отметим, что правовой режим учетных записей в своей основе является сходным: например, у любой учетной записи (в том числе в системе электронной почты) есть обладатель, определяющий юридическую судьбу учетной записи и порядок ее использования, в том числе предоставление доступа к ней иным лицам. Учетные записи — это объекты правового регулирования, прежде всего информационно-правового, которые могут участвовать в различных правоотношениях: трудовых (например, создание и ведение учетной записи в интересах и по заданию работодателя), личных (создание личной учетной записи, в том числе в коммерческих целях), семейных (совместное ведение учетной записи супругами и ее включение в состав общего имущества, в том числе для целей последующего раздела), предпринимательских (например, создание и ведение учетной записи в ходе исполнения договора о совместной деятельности) и др. Как следствие, особенности правового режима учетных записей могут быть предусмотрены в отраслевом законодательстве (корпоративном, семейном, трудовом, законодательстве о государственной и муниципальной службе и пр.), а также зависеть от правил использования конкретной информационной системы.

При этом особенности использования отдельных видов учетных записей могут быть определены отраслевыми особенностями той сферы общественных отношений, в которой они применяются, даже в отсутствие конкретных правовых норм, посвященных данному вопросу. Например, принципы трудового права определяют общий смысл и структуру деятельности работника под контролем и на основании поручений (заданий) работодателя в рамках выполнения трудовой функции, из которых можно вывести правило, что обладателем учетной записи, созданной работником по заданию и в интересах работодателя, при отсутствии соглашения сторон об ином[68] является работодатель. При этом недопустим уход работодателя

[67] Регламентация доступа к информации (в том числе в контексте социальных сетей) — один из институтов информационного права, который, с учетом комплексного характера данной отрасли права и отрасли науки, охватывает, как публично-правовое, так и гражданско-правовое регулирование. Информационное право, в связи с комплексным предметом и методами регулирования, рассматривается в науке в качестве «базовой отрасли для развития правового регулирования новых информационных отношений, информационных (цифровых пространств)» (Polyakova et al., 2025).

[68] Речь идет о ситуации, когда работник создает учетную запись в интересах и по заданию работодателя, однако стороны приходят к соглашению, что учетная запись также может быть использована в личных целях работника, не связанных с выполнением трудовой функции у конкретного работодателя, в связи с чем стороны признают, что обладателем учетной записи является работник.

от ответственности, когда фактически учетная запись используется в интересах работодателя, однако ответственность за потенциальный вред и (или) нарушения прав иных лиц будет нести работник как формальный обладатель учетной записи. В данном случае необходимо применять концепцию мнимого обладателя («собственника»), разработанную в США[69].

Концепция двойственной правовой природы учетной записи

На основе изученного материала предлагается следующее ви́дение правового режима учетных записей как разновидности виртуальных объектов.

I. Учетная запись, как виртуальный объект, обладает двойственной правовой природой: информационно-правовой и иной отраслевой (гражданско-правовой, трудоправовой и пр.). Особенности использования (правового режима) учетных записей могут быть предусмотрены в отраслевом законодательстве и в правилах информационной системы, а также выведены судами при разрешении конкретных споров посредством применения механизмов аналогии и толкования права.

Информационно-правовая природа первична для учетных записей, которые необязательно выступают объектами экономических отношений (например, учетная запись в системе электронной почты). Однако для целей настоящего исследования акцент сделан прежде всего на тех учетных записях, которые становятся ценностью и товаром в условиях экономики данных.

Виртуальные объекты, в том числе учетные записи, существуют в рамках информационных систем, в связи с чем правомочия в отношении таких объектов всегда будут частично основаны на договорных отношениях с правообладателем виртуального мира, в отсутствие которых невозможны ни создание учетной записи, ни получение доступа к виртуальной среде посредством использования такой записи, ни приобретение иных виртуальных ценностей (объектов). Однако данное обстоятельство не умаляет значение восприятия учетных записей и иных виртуальных ценностей в качестве объектов, в отношении которых возможны правовые отношения, т. е. возникновение прав и обязанностей. Выводы исследователей об ином следует признать ошибочными.

Стратегический ориентир Российской Федерации на построение экономики данных[70] (по аналогии с Европейским союзом)[71] диктует необходимость обновления законодательства, связанного с оборотом цифровых данных, разработки качественно новых правовых подходов к опосредованию отношений, связанных с данными, которые в текущих технологических реалиях

[69] См. вышеупомянутые решения Суда по делам о банкротстве штата Техас (*Memorandum opinion on Jeremy Alcede's emergency motion objecting to proposed order regarding social media accounts*, No. 14-33564 (Bankr. S.D. Tex. Apr. 3, 2015), https://www.govinfo.gov/content/pkg/USCOURTS-txsb-4_14-bk-33564/pdf/USCOURTS-txsb-4_14-bk-33564-0.pdf), Окружного суда США округа Кентукки (Int'l Bhd. of Teamsters Local 651 v. Philbeck, 464 F. Supp. 3d 863 (E.D. Ky. June 3, 2020)).

[70] См. п. 8 Перечня поручений по реализации Послания Президента Федеральному Собранию № Пр-616, утв. Президентом Российской Федерации 30 марта 2024 г. http://www.kremlin.ru/acts/assignments/orders/73759

[71] 19.02.2020 Европейской Комиссией опубликована Европейская стратегия данных, в рамках которой поставлена задача построить и обеспечить баланс частных и публичных интересов в экономике, основанной на данных (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A European Strategy for Data*, COM (2020) 66 final (Feb. 19, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066).
Термин «data economy» (экономика данных) упоминается в официальных публикациях на сайте Европейской Комиссии (European Commission. (2022). *Data economy* (Rolling Plan for ICT Standardisation). Interoperable Europe Portal. https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation/data-economy)

становятся активом, товаром и требуют адекватного правового регулирования с учетом необходимости обеспечения контроля субъектов данных над создаваемыми и используемыми ими данными как общего принципа, особенности сетей Интернет *Web 3.0, Web 4.0*.

II. Для обозначения лица, уполномоченного на наиболее полное управление учетной записью, следует использовать термин «обладатель». Как разъяснено в постановлении Конституционного Суда РФ от 26 октября 2017 г. № 25-П, «цель, которую преследовал федеральный законодатель, вводя понятие "обладатель информации", заключается... в описании по аналогии с гражданско-правовыми категориями "собственник", "титульный владелец"... правового статуса лица, правомочного в отношении конкретной информации решать вопрос о ее получении другими лицами и о способах ее использования как им самим, так и другими лицами»[72].

Использование терминов «собственник», «владелец», «участник» в отношении виртуальных объектов не соответствует сложившейся практике применения российского законодательства. Слово «пользователь» может быть применено в контексте описания отношений субъектов с правообладателем виртуальной среды (социальной сети) по передаче неисключительных прав на использование такой среды, «правообладатель» — в контексте прав лица в отношении результатов интеллектуальной деятельности, которые также могут быть выражены в конкретном виртуальном объекте (например, размещены на персональной странице в социальной сети).

В пункте 2 статьи 141.1 ГК РФ, посвященной цифровым правам, также употреблен термин «обладатель» применительно к лицу, уполномоченному на определение юридической судьбы цифрового права (распоряжение цифровым правом). Аналогичным образом выражение «обладатель электронных данных» используется в определении цифровой валюты, а слово «обладатель» — в отношении цифровых финансовых активов в Федеральном законе от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[73]. Термином «обладатель» оперирует и Федеральный закон от 2 августа 2019 г. № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» применительно к лицу, которому принадлежит утилитарное цифровое право[74].

Использование термина «обладатель», т.е. информационно-правового измерения соответствующих явлений (собственности, владения и пр.), в отношении учетных записей и иных виртуальных объектов позволит примирить проанализированные выше подходы к определению правового режима учетных записей: рассмотрение их в призме права собственности и имущественного интереса в США и в контексте неимущественного права доступа к учетным записям, имеющего договорную природу, в ФРГ.

Подчеркнем, что термин «обладатель» в действующем законодательстве используется *в двух значениях:* как обладатель информации (в том числе данных) и как обладатель

[72] Постановление Конституционного суда РФ № 25-П от 26.10.2017 «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона “Об информации, информационных технологиях и о защите информации" в связи с жалобой гражданина А. И. Сушкова”».

[73] Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» № 259-ФЗ от 31.07.2020, http://publication.pravo.gov.ru/Document/View/0001202007310056

[74] Федеральный закон «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» № 259-ФЗ от 02.08.2019, http://publication.pravo.gov.ru/Document/View/0001201908020032

имущественного (в том числе цифрового) права, т.е. в информационно-правовом и гражданско-правовом смыслах. Утвержденный 14 апреля 2023 г. Межпарламентской Ассамблеей государств — участников Содружества Независимых Государств Модельный закон «О цифровых правах» также применяет выражение «обладатель цифрового объекта». Однако, как обоснованно указывает А. Г. Шипикова, решение авторов Закона использовать термин «обладатель» в контексте *права собственности* на цифровые объекты не является бесспорным и требует дальнейшего научного обсуждения (Shipikova, 2024, p. 58). Между тем сам выбор термина «обладатель» является верным и обоснованным с научной точки зрения. В завершение подчеркнем, что дискуссия о выборе подходящего обозначения лица, уполномоченного на наиболее полный контроль над учетной записью и иными виртуальными (цифровыми) объектами, остается открытой. В вышеупомянутом проекте Цифрового кодекса Республики Казахстан использована диада терминов «владелец – пользователь» цифрового объекта[75].

III. Учетные записи как объект целесообразно рассматривать через призму понятия «данные» (ст. 2 Закона об информации).

Закрепленный в Федеральном законе от 31 июля 2020 г. № 259-ФЗ термин «обладатель электронных данных» является одним из ключей к ответу на вопрос, поставленный Л. К. Терещенко, А. В. Минбалеевым и Е. В. Холодной, о необходимости определения правового режима цифровых данных[76], отличного от понятия «информация».

С нашей позиции, определения сущностно иного правового режима цифровых (электронных) данных, отличного от категории «информация», закрепленной в Законе об информации, не требуется. Указанные понятия соотносятся как частное и общее. Данные представляют собой одну из форм существования информации. Данные, исходя из своей природы, являются электронными или цифровыми, так как эта разновидность информации существует в рамках информационных систем и предназначена для обработки на вычислительных машинах, передачи с использованием коммуникационных устройств, т.е. носит виртуальный характер, на что указывает А. А. Стрельцов (Strel'tsov, 2019, p. 5).

Дополнительно следует отметить, что существует и иная (широкая) трактовка понятия «данные» (с учетом ч. 1 ст. 1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных») — как разновидности информации, зафиксированной на материальном носителе в форме картотек или иных систематизированных собраний, позволяющих в соответствии с заданным алгоритмом осуществлять их поиск и (или) доступ к ним, в том числе без использования средств автоматизации.

Наука без понятийного аппарата и специальных терминов (научного языка) не является подлинной (Stepin, 2010, p. 156), в связи с чем не следует усиливать терминологическую путаницу в информационном законодательстве, о чем писали В. Б. Наумов, Л. К. Терещенко, искусственно разграничивая понятия «информация» и «цифровые данные».

Фактически термин «цифровые данные» находит отражение в законодательстве с заменой ошибочного перевода слова *digit* как «цифровой» на более привычный и корректный синоним — «электронный» (при этом правильно было бы использовать термин «числовой» (Baturin, 2022, pp. 18–20)). Закон РФ о поправке к Конституции РФ от 14 марта 2020 г. № 1-ФКЗ (в части внесения изменений в п. «м» ст. 71 Основного закона) вступил в силу 4 июля

[75] См. ст. 24–25 Проекта Цифрового кодекса Республики Казахстан, 2024. *GitHub*. https://github.com/Akylbay-Katira/digital-codex/blob/main/digital-Codex-2024-ru.md

[76] Термин был включен в текст Конституции РФ в 2020 г.

2020 г.[77] А Федеральный закон от 31 июля 2020 г. № 259-ФЗ вступил в силу позднее, 1 января 2021 г., и содержит верную трактовку рассматриваемого понятия с более корректным обозначением — «электронные данные». В связи с этим выводы исследователей о неприменении указанного термина в отраслевом законодательстве следует признать ошибочными.

С информационно-правовой точки зрения учетные записи как виртуальные объекты представляют собой данные как объект информационных правоотношений. Напомним, что сходная позиция в отношении правовой природы метавселенной высказана А. Д. Севергиным (Severgin, 2023, pp. 40–43).

С учетом изложенного, завершая дискуссию Л. К. Терещенко, А. В. Минбалеева и Е. В. Холодной по данному вопросу, повторим, что электронные (цифровые) данные в полной мере укладываются в рамки базовой для информационного законодательства категории «данные» как одной из форм существования информации. Федеральный закон от 31 июля 2020 г. № 259-ФЗ на примере словосочетания «обладатель электронных данных» демонстрирует возможность правовой регламентации новых явлений, связанных с виртуальными объектами и экономикой данных, *в пределах устоявшейся терминологии*.

Таким образом, учетные записи следует рассматривать как разновидность данных (цифровых или электронных), т.е. форму существования информации (ст. 2 Закона об информации). Закрепления правового режима цифровых данных, не связанного с понятием «информация», не требуется. В отношении подобных объектов возникают информационные правомочия (например, право обладания учетной записью или право доступа к ней), которые при обретении виртуальным объектом экономической ценности получают характер имущественного (или, как указано выше, цифрового) права для целей участия в обороте.

Подобный подход к рассмотрению природы учетных записей позволяет преодолеть концептуальную проблему неовеществленности виртуальных (цифровых) объектов, так как характеристику объекта учетная запись приобретает за счет инструментария информационного законодательства, а в имущественных отношениях участвуют права в отношении такого объекта. Аналогичный подход допустим и в отношении цифровых валют, которые определены Федеральным законом от 31 июля 2020 г. № 259-ФЗ как «совокупность электронных данных» и при этом одновременно отнесены к категории имущества[78], что не может не вызывать противоречий (принимая во внимание исключение информации из перечня объектов гражданских прав Федеральным законом от 18 декабря 2006 г. № 231-ФЗ).

Разграничение информационно-правовой и иной отраслевой природы виртуальных объектов позволяет решить данную проблему, так как в таком случае (на примере цифровых валют) в гражданском обороте выступают не сами электронные (цифровые) данные, а информационные (цифровые) права в отношении них (право доступа к распределенной информационной системе, в рамках которой осуществляется оборот цифровой валюты, право восстановления доступа к учетной записи, необходимой для операций с цифровой валютой). Данный пример демонстрирует, что определение правовой природы и правового режима учетных записей выходит за рамки социальных сетей. Так, например, не меньшее значение имеет вопрос

[77] См. п. 1 Указа Президента Российской Федерации «Об официальном опубликовании Конституции Российской Федерации с внесенными в нее поправками» № 445 от 03.07.2020, http://publication.pravo.gov.ru/Document/View/0001202007030012

[78] См. п. 3 ст. 1, ст. 17, 19, 21, 22 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» № 259-ФЗ от 31.07.2020, http://publication.pravo.gov.ru/Document/View/0001202007310056

принадлежности криптокошелька (учетной записи на криптовалютной бирже) конкретному лицу, который нередко возникает в судебной плоскости, например в делах о банкротстве, в том числе в России[79].

Предложения по изменению законодательства РФ

С учетом полученных результатов и принимая во внимание особенности построения экономики данных, предлагается внести в Закон об информации следующие изменения.

Во-первых, закрепить легальное определение цифровых (электронных) данных и указать, что совокупность данных, обладающая индивидуализирующими признаками в информационной системе, может образовывать самостоятельные объекты правовых отношений (цифровые валюты, учетные записи, доменные имена, *NFT (non-fungible token)* и пр.) (ст. 2 Закона об информации).

Во-вторых, включить в текст закона бланкетные нормы, содержащие указание на то, что особенности правового режима отдельных видов цифровых (электронных) данных, а также особенности правового статуса их обладателей могут быть предусмотрены законодательством Российской Федерации (в том числе Федеральным законом от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации») и принятыми в его исполнение подзаконными актами (статьи 5–6 Закона об информации).

В-третьих, включить в текст закона нормы, направленные на признание прав обладателей учетных записей и их защиту, в соответствии с которыми:

- к пользователям социальных сетей — обладателям учетных записей применяются общие правила о правомочиях обладателя информации (статья 6 Закона об информации);
- особенности использования учетных записей могут быть предусмотрены договором между пользователем и правообладателем социальной сети, с оговоркой, что условия указанного договора, противоречащие законодательству Российской Федерации и существу соответствующих отношений, не имеют правового значения и не подлежат применению (статья 5 Закона об информации).

Кроме того, целесообразно дополнить регулирование информационно-правового института доступа к информации применительно к учетным записям, предусмотрев правило, в соответствии с которым соглашением сторон не может быть ограничено право доступа к учетной записи и содержащейся в ней информации на сайте в сети Интернет, отнесенном к социальной сети в соответствии Законом об информации, в отношении наследников или законных представителей пользователя, в случае его гибели или признания недееспособным, частично дееспособным, безвестно отсутствующим или объявления умершим в порядке, предусмотренном гражданским процессуальным законодательством (статья 8 Закона об информации).

В-четвертых, в целях обеспечения публичных интересов государства в информационной (цифровой) среде предусмотреть, что на правоотношения, связанные с оборотом цифровых (электронных) данных, выступающих в качестве товара, распространяется законодательство о защите конкуренции, противодействии коррупции, противодействии легализации доходов, полученных преступным путем (статья 5 Закона об информации). Дополнительно отметим,

[79] Панин, В. О. (2025). *Цифровая валюта и процедуры несостоятельности: хеджирование рисков*. PROбанкротство. https://probankrotstvo.ru/articles/cifrovaia-valiuta-i-procedury-nesostoiatelnosti-xedzirovanie-riskov-9523

что необходимость внесения изменений в гражданское законодательство в части расширения категории «цифровое право» является предметом дальнейших научных дискуссий.

Заключение

Подведем итоги настоящего исследования.

1. Учетные записи, в том числе в социальных сетях, следует рассматривать как объекты правового интереса, который может подлежать судебной защите. Научные подходы, отрицающие наличие у учетных записей характеристики объекта правовых отношений или рассматривающие их через призму права интеллектуальной собственности, в современных условиях следует признать подлежащими пересмотру.

2. Для обозначения лица, управомоченного на осуществление наиболее полного контроля над учетной записью в информационной системе, в том числе в социальной сети, рекомендуется использовать термин «обладатель», который в действующем российском законодательстве воспринимается в двух значениях: как обладатель информации (в том числе данных) и как обладатель имущественного (в том числе цифрового) права, т.е. в информационно-правовом и гражданско-правовом смыслах.

Аналогичный подход (восприятие через призму «обладателя») целесообразно применять к иным виртуальным объектам, например цифровой валюте, в отношении которой законодатель уже использует соответствующий термин.

Кроме того, с учетом комплексного характера правоотношений в цифровой среде термины «пользователь» и «правообладатель» также могут быть использованы в определенном контексте: слово «пользователь» для описания отношений субъектов (обладателей учетной записи) с правообладателем виртуальной среды по передаче неисключительных прав на использование такой среды, а «правообладатель» — в контексте прав лица в отношении результатов интеллектуальной деятельности, которые также могут быть выражены в конкретном виртуальном объекте, например в содержании учетной записи, на что указал Федеральный верховный суд Германии.

3. Предлагаемые в настоящей статье законодательные изменения позволят решить следующие критически важные задачи.

Во-первых, закрепить правомочия «владельцев» учетных записей в отношении принадлежащего им виртуального объекта (признав их обладателями соответствующего сложного объекта, образованного совокупностью информации в форме электронных данных), которые в настоящее время находятся вне сферы законодательного регулирования, в том числе:

- гарантировать право на цифровое (виртуальное) наследие посредством применения к обладателю учетной записи общих полномочий обладателя информации, в том числе по определению лиц, которым может быть предоставлен доступ к информации (п. 1, 3 ч. 3 ст. 6 Закона об информации), а также запрета на ограничение доступа к такой информации для наследников или законных представителей обладателя учетной записи;
- чрезмерно не ограничивать усмотрение правообладателей социальных сетей, которые самостоятельно определяют функционал конкретной социальной сети, влияющий на перечень прав обладателя учетной записи (например, права на использование и (или) продажу поддоменных имен, на создание сообществ в социальной сети, на использование виртуальной валюты). При этом пресекать недобросовестные практики в ситуациях, когда правообладатели виртуальных сред маскируют товарообменные отношения

под внутриигровые механики, правила игры и пр., посредством возможности неприменения соответствующих договорных условий по мотиву их ничтожности и противоречия существу регулируемых отношений[80].

Во-вторых, отразить, что виртуальные объекты как совокупность электронных данных могут рассматриваться в качестве товара, в связи с чем к регулированию соответствующих отношений применяются правила о защите конкуренции, противодействии коррупции и легализации доходов, полученных преступным путем.

Предлагаемые изменения позволят устранить ложное общее место о нематериальных виртуальных объектах, которые, по мнению отдельных исследователей, не могут выступать объектом правовых отношений, а также станут значимым шагом на пути разрешения существующих противоречий о построении правового регулирования таких объектов (например, каким видом имущества является цифровая валюта, какова правовая природа цифровых финансовых активов и доменных имен, является ли учетная запись объектом правовых отношений, и т.д.).

4. Подчеркнем, что объектом информационного права и правового интереса выступают сами виртуальные объекты (например, учетные записи, доменные имена, наименования учетных записей, виртуальные предметы, цифровые валюты и пр.). *При этом в отношении таких объектов возникают информационные права (правомочия)*, например право обладания учетной записью, право доступа к учетной записи, право обладания цифровой валютой и пр. *Указанные информационные права для целей участия в имущественных отношениях следует рассматривать в качестве имущественных прав* (в том числе цифровых прав). Это означает, что в экономических отношениях юридически участвуют не сами виртуальные объекты, а информационные права на них, приобретающие гражданско-правовую характеристику (по аналогии с участием в обороте исключительных прав на результаты интеллектуальной деятельности, а не самих таких результатов, при одновременно признании за последними характеристики объекта гражданских прав).

Список литературы / References

1. Agaeva, V. V. (2023). Razdel akkaunta v sotsial'noy seti pri prekrashchenii brachno-semeynykh otnosheniy [Division of a social media account upon termination of marital and family relations]. *Vestnik Prava*, (4), 4–8.
2. Bachilo, I. L., Polyakova, T. A., Antopol'skiy, A. A., Dem'yanets, M. V., Zharova, A. K., Monakhov, V. N., Semiletov, S. I., & Talapina, E. V. (2017). Ob osnovnykh napravleniyakh razvitiya informatsionnogo prava za 2000-2015 gg. [On the main directions of the development of information law in 2000–2015]. Gosudarstvo i parvo, (1), 71–79.
3. Baturin, Y. M. (2022). *Ot Interneta do virtual'noi Zemli i metaveselennoy: Kratkaya istoriya informatsionnykh tekhnologiy na kriticheskom rubezhe* [From the Internet to the virtual Earth and the metaverse: A brief history of information technologies at a critical juncture]. IIET RAN, AmirIT.
4. Doiev, A. M. (2023). 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
5. Fairfield, J. A. T. (2023). “Veshchnoe” pravo virtual'nykh “veshchey” [Property as the law of virtual things] (A. M. Doiev, Trans.). *Digital Law Journal, 4*(3), 16–39. https://doi.org/10.38044/2686-9136-2023-4-3-16-39

[80] Аналогичным образом следует пресекать недобросовестные действия работодателей, единоличных исполнительных органов и иных лиц, направленные на уход от ответственности и (или) незаконное получение учетной записи в обладание. Однако решать указанные вопросы необходимо посредством инструментов отраслевого законодательства (гражданско-правового, трудового, законодательства о несостоятельности и пр.) по аналогии с рассмотренными судебными делами в США и ФРГ.

6. Fedorov, A. M. (2023). Ponyatie i pravovaya priroda akkaunta v sotsial'noy seti [The concept and legal nature of a social media account]. *Yuridicheskaya Nauka*, (8), 151–155.
7. Grin', E. S. (2022). Nasledovanie akkauntov v sotsial'nykh setyakh: Rossiyskiy i zarubezhnyy opyt [Inheritance of social media accounts: Russian and foreign experience]. *Actual Problems of Russian Law*, (2), 128–134. https://dx.doi.org/10.17803/1994-1471.2022.135.2.128-134
8. Kholodnaya, E. V. (2024). O pravovoy kontseptsii metavselennyh [On the legal concept of metaverses]. *Lex Russica, 77*(3), 116–128. http://dx.doi.org/10.17803/1729-5920.2024.208.3.116-128
9. Krause, D. (2024). *Web3 and the decentralized future: Exploring data ownership, privacy, and blockchain infrastructure*. Social Science Research Network. http://dx.doi.org/10.2139/ssrn.5064483
10. Khromov, E. V., & Zyablikov, V. Yu. (2024). Khishchenie bestelesnogo imushchestva [Theft of incorporeal property]. *Ugolovnoye Pravo*, (8), 46–67.
11. Kryuchkova, A. D. (2021). Pravovaya priroda Instagram-akkaunta i problema razdela dannogo "imushchestva" [The legal nature of an Instagram account and the problem of dividing this "property"]. *Voprosy Rossiyskoy Yustitsii*, (14), 233–241[81].
12. Kuznetsov, P. U. (2005). *Teoreticheskie osnovaniia informatsionnogo prava* [Theoretical foundations of information law] (Dr. Sci. dissertation, Ural State Law University).
13. Mityagin, K. S. (2014). Pravovaia priroda stranitsy sotsial'noi seti [Legal Nature of a Social Network Page]. *Zhurnal Suda po Intellektual'nym Pravam*, (5), 74–77. https://ipcmagazine.ru/articles/1729162/
14. Naumov, V. B. (2018). Negativnye zakonomernosti formirovaniya ponyatiynogo apparata v sfere regulirovaniya Interneta i identifikatsii [Negative regularities in the formation of the conceptual apparatus in the field of Internet regulation and identification]. *Informatsionnoye Pravo*, (1), 32–39.
15. Panin, A. V. (2022). Pravovoy rezhim virtual'nykh ob'yektov v informatsionnoy srede [Legal regime of virtual objects in the information environment]. *Trudi po Intellectualnoy Sobstvennosti (Works on Intellectual Property)*, *43*(4), 43–55. https://doi.org/10.17323/tis.2022.16351
16. Polyakova, T. A., & Troyan, N. A. (2025). Informatsionnoye pravo i tsifrovaya real'nost': razvitiye, prioritety i problemy v usloviyakh tsifrovoy transformatsii [Information law and digital reality: Development, priorities and problems within digital transformation]. *Pravovaya informatika*, (2), 31–41.
17. Polyakova, T. A., Minbaleyev, A. V., & Naumov, V. B. (2025). Sovremennyye prioritety razvitiya informatsionnogo prava: pravovoye obespecheniye gosudarstvennogo suvereniteta i informatsionnoy bezopasnosti v informatsionnom prostranstve Rossii [Modern priorities for the development of information law: Legal support for state sovereignty and information security in the information space of Russia]. *Gosudarstvo i pravo*, (1), 160–173.
18. Rozhkova, M. A. (2024). *Nematerial'nye ob'ekty i imushchestvennye prava na nikh v sisteme absolyutnykh prav* [Intangible objects and property rights to them in the system of absolute rights]. GAUGN Press.
19. Severgin, A. D. (2023). Pravovaya priroda metavselennoi [The legal nature of the metaverse]. *Digital Law Journal*, *4*(4), 36–53. https://doi.org/10.38044/2686-9136-2023-4-4-1
20. Shipikova, A. G. (2024). Podkhody k opredeleniyu tsifrovogo ob'yekta i tsifrovogo aktiva [Conceptual approaches to defining digital objects and digital assets]. *Digital Law Journal, 5*(2), 53–68. https://doi.org/10.38044/2686-9136-2024-5-2-1
21. Stepin, V. S. (2010). Istoriya i filosophiya nauki: Uchebnik [History and philosophy of science: Textbook] (3rd ed.). Akademicheskii Proekt.

[81] Правообладатель данной социальной сети — компания *Meta* — признан в Российской Федерации экстремистской организацией. Упоминание данных сведений носит исключительно научный характер и необходимо для целей исследования.

22. Strel'tsov, A. A. (2019). O predmete i metode informatsionnogo prava [On the subject and method of information law]. *Informatsionnoe pravo*, *62*(4), 4–11.
23. Tereshchenko, L. K. (2022). Transformatsiya ponyatiynogo apparata informatsionnogo prava v usloviyakh tsifrovizatsii [Transformation of the conceptual framework of information law in context of digitalization]. Journal of Russian Law, *26*(12), 98–110. http://dx.doi.org/10.12737/jrl.2022.131

Сведения об авторе:

Панин В. О. — младший научный сотрудник, Сектор информационного права и международной информационной безопасности, Институт государства и права Российской академии наук; ведущий юрисконсульт, юридическая компания «К12», Москва, Россия
valeri-panin@yandex.ru
ORCID: https://orcid.org/0000-0001-9022-323X

Information about the author:

Valerii O. Panin — Junior Research Fellow, Sector of Information Law and International Information Security, Institute of State and Law of the Russian Academy of Sciences; leading legal adviser, K12 Law Firm, Moscow, Russia.
valeri-panin@yandex.ru
ORCID: https://orcid.org/0000-0001-9022-323X

https://doi.org/10.38044/2686-9136-2025-6-12

СТАТЬИ

ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ ОБУЧЕНИЯ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВЕ ЕВРОПЕЙСКОГО СОЮЗА

А. А. Олифиренко[1,2]

[1]Саратовская государственная юридическая академия
410056, Россия, Саратов, ул. Вольская, 1

[2]Саратовский государственный технический университет
им. Ю. А. Гагарина
410008, Россия, Саратов, ул. Политехническая, 77к1

Аннотация

Принятие европейского Акта об искусственном интеллекте (AI Act) закрепило обязательное регулирование жизненного цикла систем искусственного интеллекта в Европейском союзе при сохранении действия Общего регламента по защите данных (GDPR). Стадия обучения ИИ-моделей оказалась в зоне пересечения двух режимов: Акт об ИИ ориентирует участников на качество и репрезентативность наборов данных, управление рисками и документирование процесса обучения, тогда как Общий регламент о защите данных фиксирует принципы правомерности, минимизации, ограничения целей и сроков хранения, а также предоставляет субъекту персональных данных комплекс гарантий и средств защиты. В практических проектах это создает риск юридически дефектного обучения, когда стремление к репрезентативности реализуется через избыточный сбор и повторное использование данных. Статья исследует допустимость и организацию обучения ИИ-моделей при совместном применении Акта об ИИ и Общего регламента о защите данных. Цель исследования состоит в обосновании правовой модели, позволяющей выстроить соразмерные технические и организационные гарантии, сохранить качество обучения и одновременно обеспечить законность обработки персональных данных и защиту основных прав. Методология включает нормативно-догматический анализ требований Акта об ИИ к системе управления рисками и управлению данными, сопоставление с принципами Общего регламента о защите данных и процедурными инструментами обеспечения законности обработки, а также систематизацию типовых управленческих артефактов, используемых при разработке и эксплуатации высокорисковых ИИ-систем. Результаты исследования представлены как согласованная модель поведения участников на стадии обучения. Обосновано прикладное разграничение «ИИ-система» и «ИИ-модель»: система квалифицируется как организационно-техническая оболочка, включающая модель, инфраструктуру, интерфейсы ввода и вывода, мониторинг и взаимодействие с человеком, тогда как модель рассматривается как алгоритмическое ядро, обученное на данных и применяемое для вывода результатов; данное разграничение используется для распределения обязанностей провайдера и лиц, внедряющих или эксплуатирующих систему. Предложен механизм согласования репрезентативности и достоверности наборов данных с принципом минимизации через документируемую инвентаризацию признаков, обоснование необходимости каждого класса данных и исключение нерелевантных атрибутов с одновременной оценкой риска косвенной дискриминации. Разработана модель

соразмерности защитных мер, связывающая выбор псевдонимизации, анонимизации, агрегирования, синтетической генерации и дифференциальной приватности с чувствительностью данных, контекстом использования и уровнем риска для основных прав, подтверждаемым результатами оценки воздействия на защиту данных и оценки воздействия на основные права. Сформулирован практический контур правового обеспечения жизненного цикла обучения: постановка цели и правового основания, ограничение повторного использования наборов данных, контроль доступа и журналирование операций, правила сроков хранения и удаления, а также процедуры пересмотра параметров обучения и мониторинга после внедрения. Предложенная модель повышает предсказуемость правоприменения и задает воспроизводимый порядок согласования требований Акта об ИИ и Общего регламента о защите данных на стадии обучения.

Ключевые слова

искусственный интеллект, обучение модели искусственного интеллекта, правовое регулирование персональных данных, минимизация данных, соразмерность мер, Общий регламент о защите данных, Регламент об искусственном интеллекте, комплаенс, жизненный цикл ИИ

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.
Для цитирования	Олифиренко, А. А. (2025). Использование персональных данных для обучения моделей искусственного интеллекта в праве Европейского союза. *Цифровое право, 6*(3), 94–124. https://doi.org/10.38044/2686-9136-2025-6-12

Поступила: 03.07.2025; принята в печать: 20.08.2025, опубликована: 30.09.2025

ARTICLES

USING PERSONAL DATA IN AI MODEL TRAINING UNDER EU LAW

Artem A. Olifirenko[1,2]

[1]Saratov State Law Academy
1, Volskaya St., Saratov, Russia, 410056

[2]Yuri Gagarin State Technical University of Saratov
77-1, Polytechnicheskaya St., Saratov, Russia, 410008

Abstract

The adoption of the EU Artificial Intelligence Act (AI Act) established mandatory life-cycle regulation of AI systems in the European Union while preserving the validity of the General Data Protection Regulation (GDPR). The training stage of AI models has consequently become a point of intersection between two regulatory regimes: while the AI Act emphasizes data quality and representativeness along with risk management and documentation of training processes, the GDPR sets out the applicable principles of lawfulness, data minimization, purpose, and storage limitation, as well as providing data subjects with a set of safeguards and remedies. In practical terms, this interaction creates a risk of legally defective model training due to the pursuit of representativeness through excessive data collection and repeated re-use of personal data. This article examines the permissibility

and organization of AI model training under the joint application of the AI Act and the GDPR. The research sets out to substantiate a legal model that enables proportionate technical and organizational safeguards while preserving training quality and ensuring the lawfulness of personal data processing that respects the fundamental rights of data subjects. As well as combining doctrinal legal analysis of the AI Act requirements on risk management and data governance with a comparative assessment of the GDPR principles and procedural tools for ensuring lawful processing, the methodology involves a systematization of typical governance artefacts used in the development and deployment of high-risk AI systems. The results are presented as an integrated compliance-by-design model for actors involved in the training stage. A practical distinction between an "AI system" and an "AI model" is substantiated: whereas an AI system is qualified as an organizational and technical envelope comprising the model, infrastructure, input and output interfaces, monitoring, and human interaction, an AI model is treated as the algorithmic core trained on data and used to infer outputs. This distinction can be applied to allocate obligations between the provider and entities deploying or operating the system. The proposed mechanism for reconciling dataset representativeness and accuracy with the GDPR data minimization principle through a documented feature inventory is based on a necessity rationale for each class of data and the exclusion of irrelevant attributes alongside an assessment of indirect discrimination risks. The choice of safeguards (pseudonymization, anonymization, aggregation, synthetic generation, and differential privacy) to data sensitivity, use context, and the level of risk to fundamental rights is carried out on the basis of a proportionality model. This model is supported by the outcomes of a data protection impact assessment and a fundamental rights impact assessment. Finally, a practical legal governance loop for the training life cycle is formulated to cover the determination of the purpose and legal basis, limits on dataset re-use, access control and logging, as well as retention and deletion rules, along with procedures for revisiting training parameters and monitoring after deployment. The proposed model increases legal certainty and provides a reproducible framework for aligning the AI Act and GDPR during the training stage.

Keywords

artificial intelligence, AI model training, data protection law, data minimization, proportionality of safeguards, GDPR, AI Act, compliance, AI life cycle

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Olifirenko, A. A. (2025). Using personal data in AI model training under EU law. *Digital Law Journal, 6*(3), 94–124. https://doi.org/10.38044/2686-9136-2025-6-12

Submitted: 3 July 2025, accepted: 20 Aug 2025, published: 30 Sep. 2025

Введение

Принятие Регламента 2024/1689 об искусственном интеллекте (Artificial Intelligence Act, далее — Акт об ИИ)[1] ознаменовало переход Европейского союза от декларативного этического подхода к нормативно-правовой детализации жизненного цикла систем искусственного интеллекта (далее — ИИ-системы). В отличие от прежнего, преимущественно этического, дискурса новый акт закрепляет юридически обязательные требования к проектированию, обучению и эксплуатации систем искусственного интеллекта при одновременном сохранении действия

[1] Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024 laying down Harmonised Rules on Artificial Intelligence and Amending Regulations 300/2008, 167/2013, 168/2013, 2018/858, 2018/1139 and 2019/2144 and Directives 2014/90/EU, 2016/797 and 2020/1828 (Artificial Intelligence Act), 2024 O.J. (L 2024/1689) 1.

Общего регламента о защите данных (*General Data Protection Regulation,* далее — *GDPR*)[2]. Уже в ст. 2(7) Акта об ИИ подчеркивается, что он «не затрагивает и не уменьшает» объем защиты, гарантированной иным законодательством Союза, прежде всего *GDPR*, формируя для участников рынка режим двойной нормативной подотчетности[3]. В доктрине при этом просматриваются по меньшей мере два конкурирующих подхода: часть авторов предлагает рассматривать Акт об ИИ как *lex specialis* (специальное регулирование по отношению к общему режиму *GDPR*) для высокорисковых систем (Hadwick, 2024, pp. 947–948; Kindt, 2025, p. 31) (сходная аргументация встречается и в политико-правовых аналитических материалах, сопровождающих обсуждение и принятие Акта об ИИ, где отдельно фиксируются риски пересечений и конкуренции регуляторных режимов[4]); другие, напротив, настаивают на автономной значимости принципов защиты данных и воспринимают Акт об ИИ лишь как техническое уточнение уже существующих обязанностей (Winau, 2023; De Hert & Hajduk, 2024, p. 292; van Bekkum, 2025, p. 2). Автор настоящей работы придерживается промежуточной позиции, исходящей из невозможности свести один режим к другому без потери содержания.

Нормативная конструкция взаимодействия Акта об ИИ и *GDPR* не может быть сведен к простому суммированию обязанностей. Акт об ИИ формулирует углубленные технические и процессуальные требования (качество данных, управление рисками, документация, оценка воздействия на права), тогда как *GDPR* закрепляет фундаментальные принципы обработки персональных данных и архитектуру прав субъектов. Нарушение последних способно превратить даже формально выстроенный процесс обучения модели в юридически дефектный. Характерно, что аналитические материалы[5] к Акту об ИИ прямо подчеркивают: соблюдение самих по себе требований данного документа не гарантирует соответствия требованиям *GDPR*[6], а оценка влияния искусственного интеллекта на основные права[7] (*Fundamental Rights Impact Assesment,* далее — *FRIA*) в работах А. Мантелеро и других авторов рассматривается как самостоятельный способ контроля, как отдельная процедура, выходящая за рамки сугубо оценки рисков для защиты персональных данных и конфиденциальности (Mantelero, 2024, p. 9; Kaminski & Malgieri, 2024, pp. 314–315).

Наибольшее напряжение между двумя режимами проявляется на обучающей стадии, где сходятся противоположные методологические векторы. С одной стороны, статья 10 Акта об ИИ закрепляет императив высококачественных, репрезентативных и, по возможности, свободных от ошибок обучающих наборов наряду с обязанностью провайдера внедрять процедуры

[2] 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 O.J. (L 119) 1.

[3] Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 45.

[4] Voss, A. (2022). *Better regulation: Potential legal overlaps & contradictions with other laws*. European Parliament. https://www.axel-voss-europa.de/wp-content/uploads/2022/03/AVoss_AIA_BetterRegulation.pdf

[5] European Data Protection Board. (2024) *Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework.* https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf

[6] Cuatrecasas. (2024). *EU AI Act: A pioneering legal framework on artificial intelligence. Practical guide.* https://www.cuatrecasas.com/resources/eu-ai-act-practical-guide-669112324626b904914005.pdf?v1.94.0.20251119

[7] Под основными правами ("fundamental rights") понимаются права и свободы, закрепленные в Хартии Европейского союза об основных правах, то есть в надотраслевом стандарте защиты личности в правопорядке ЕС, охватывающим, в частности, достоинство, свободы, равенство и солидарность, а также права граждан и гарантии правосудия; в этом значении термин используется и в контексте регулирования ИИ. См.: Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391.

выявления и коррекции алгоритмических смещений. С другой стороны, *GDPR* квалифицирует любую загрузку данных в модель искусственного интеллекта (далее — ИИ-модель) как обработку персональных данных и предписывает принцип минимизации: обрабатывать лишь те данные, которые «адекватны, релевантны и ограничены необходимым для целей, для которых они обрабатываются» (ст. 5(1)(c) *GDPR*)[8]. Здесь важно отметить, что требование репрезентативности фактически размывает правило минимизации и способствует расширению массивов данных, тогда как другие исследователи предлагают рассматривать эти требования как комплементарные при условии строгого риск-ориентированного подхода (*risk-based approach*) и прозрачной документации об источниках и о структуре датасетов[9] (Paullada et al., 2021, pp. 1, 4, 10)[10]. В настоящей работе минимизация и репрезентативность рассматриваются не как автоматически согласованные принципы, а как напряженная связка, требующая дополнительных гарантий: процедур оценки воздействия на защиту данных (*Data Protection Impact Assessment, далее — DPIA*), на основные права (*FRIA*), ведения внутреннего журнала минимизации (обоснование включения каждого класса атрибутов и сроков хранения) и ограничений на вторичное использование обучающих, валидационных и тестовых наборов персональных данных и их производных версий (включая объединенные датасеты и повторно размеченные выборки) вне первоначально заявленных целей обучения.

Возникающая коллизия имеет по меньшей мере три аспекта:

1) вопрос о допустимом объеме и структуре выборки, необходимой для нивелирования предвзятости без утраты соразмерности обработки;
2) правовая судьба повторной и переносной переработки, когда исходные пользовательские данные применены для первоначального обучения, а затем привлекаются для иных целей, включая дополнительное обучение[11] и перенос обучения[12];
3) соразмерность технических и организационных мер категории риска модели с учетом дифференциации согласно ст. 6, 7 Акта об ИИ по уровням критичности и оценки тяжести воздействия на основные права (Malgieri & Santos, 2025 pp. 3, 7; Novelli et al., 2024b, pp. 1-2, 21)[13].

Особое значение имеет статья 10(5) Акта об ИИ[14], допускающая исключительную обработку специальных категорий персональных данных при разработке и проверке высокорисковых систем лишь в той мере, в какой это строго необходимо для обеспечения выявления и коррекции возможных предвзятостей (biases)[15] в обучающих, валидационных и тестовых наборах данных

[8] General Data Protection Regulation, 2016 O.J. (L 119) 35. См. об этом: International Organization for Standardization. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001

[9] В оригинале — *"dataset governance"*, что означает управление жизненным циклом наборов данных.

[10] Niemiec, E., Davis, P., & Hauglid, M. (2024). *Will the EU AI Act help to eliminate dataset bias in medical AI?* SSRN. https://doi.org/10.2139/ssrn.5045561

[11] В первоисточнике *"fine-tuning"* характеризует дообучение модели на новых данных, в том числе на специализированных выборках, связанных с конкретной целевой задачей.

[12] В оригинале *"transfer learning"* подразумевает использование заранее обученной модели в новом контексте.

[13] Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 53–55.

[14] См.: Ibid, at 58.

[15] См.: Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 57–58. То есть *"biases"*, упомянутых в данной статье Акта, которые следует понимать как систематическую предвзятость (смещение), возникающую в данных или в результатах функционирования модели вследствие перекоса представительства отдельных групп, качества и полноты признаков, ошибок разметки, выбора критериев отбора и иных факторов, влияющих на распределение данных.

в рамках процедур управления данными, предусмотренных статьей 10(2)(f)–(g) Акта об ИИ[16], при условии соблюдения установленных данной нормой гарантий. Норма, ориентированная на снижение риска дискриминации и иных неблагоприятных эффектов, одновременно обостряет дилемму правомерности обработки: статья 9 *GDPR*[17] закрепляет общий запрет на обработку специальных категорий персональных данных, тогда как статья 10(5) Акта об ИИ[18] вводит узкоцелевое исключение, сопряженное с обязанностями по выявлению и снижению смещений и дополненное требованиями: обосновать невозможность достижения цели посредством обработки иных данных, включая синтетические или анонимизированные; применять современные меры безопасности и защиты данных, включая псевдонимизацию; ограничивать повторное использование и передачу третьим лицам, а также обеспечивать контроль доступа и документирование операций; удалять соответствующие данные после достижения цели коррекции смещений либо по истечении срока хранения. В доктрине данная конструкция обсуждается как вопрос о том, представляет ли указанное исключение допустимое точечное смягчение запрета статьи 9 *GDPR*[19] или, напротив, создает риск «ползучего расширения» (*function creep*)[20], при котором ссылка на устранение смещений фактически легитимирует устойчивую обработку чувствительной информации (van Bekkum, 2025, pp. 3, 7–8).

В отсутствие унифицированных методических разъяснений Европейской комиссии и Европейского управления искусственного интеллекта степень неопределенности усиливается недавними позициями надзорных органов. Так, в заключении 28/2024 Европейского совета по защите данных подчеркивается, что принцип минимизации «в полном объеме применим к разработке и развертыванию моделей» и что крупномасштабный веб-скрейпинг, т. е. автоматизированный сбор данных с веб-сайтов с помощью программных средств, не может автоматически опираться на исключение из информационной обязанности по ст. 14(5)(b) *GDPR*[21]. Тем самым подтверждается, что источники данных для обучения требуют индивидуальной юридической оценки, а массовый подход, предполагающий загрузку больших массивов данных без разбора, не соответствует стандартам *GDPR*. В литературе указанные выводы получают неоднозначную интерпретацию. С одной стороны, они рассматриваются как подтверждение того, что требования Акта об ИИ не подменяют и не устраняют автономную применимость *GDPR*: принципы *GDPR* и связанные оценочные процедуры сохраняют самостоятельное значение параллельно инструментам Акта об ИИ, включая *FRIA* (Mantelero, 2024, p. 4; Malgieri & Santos, 2025, pp. 1–2)[22]. С другой стороны, те же положения описываются как проявление структурной незавершенности многоуровневого регулирования, в рамках которого методологии оценки рисков и контуры правоприменения еще формируются через стандартизацию, подзаконные акты и руководства,

16 Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 57.

17 General Data Protection Regulation, 2016 O.J. (L 119) 38–39.

18 См.: Ibid, at 58. В акте *"state of the art"* понимается как соответствующие высшему уровню развития техники и практики.

19 General Data Protection Regulation, 2016 O.J. (L 119) 38–39.

20 См. European Data Protection Board. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679*. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Под "function creep" в данном контексте следует понимать риск последующего использования персональных данных для дополнительных задач, выходящих за пределы первоначально заявленной цели обработки.

21 European Data Protection Board. (2024). *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*. https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf; General Data Protection Regulation, 2016 O.J. (L 119) 42.

22 См. также: Niemiec, E., Davis, P., & Hauglid, M. (2024). *Will the EU AI Act help to eliminate dataset bias in medical AI?* SSRN. https://doi.org/10.2139/ssrn.5045561

что объективно предполагает сосуществование и конкуренцию нескольких моделей комплаенса и enforcement-практик (Novelli et al., 2024b, p. 1; Söderlund & Larsson, 2024, p. 2; van Bekkum & Zuiderveen Borgesius, 2023, p. 2).

Указанные обстоятельства формируют ядро проблемного поля настоящего исследования. Его научная новизна обусловлена тем, что, во-первых, трансграничная цифровая экономика нуждается в оперативных, но юридически выверенных методиках подготовки обучающих наборов и документирования решений на обучающей стадии; во-вторых, существующая литература преимущественно концентрируется либо на догматическом анализе Акта об ИИ и его типовых схемах правоприменения и надзорной практики (*enforcement patterns*), либо на традиционных вопросах защиты персональных данных, не предлагая синтезированной модели согласованного применения обоих актов в области разработки и эксплуатации ИИ-систем. Отдельные подходы к оценке воздействия на права человека (*FRIA*), к управлению наборами данных через практики управления данных (*data governance*) и документирование решений на стадиях формирования и использования датасетов, а также к подготовке проверяемой (*audit-ready*) технической документации для целей комплаенса по Акту об ИИ (Mantelero, 2024, p. 4; Paullada et al., 2021, pp. 1, 7, 10; Sovrano et al., 2025, pp. 1, 4) пока не сведены в единую правовую конструкцию обучения ИИ-моделей[23].

Цель исследования состоит в обосновании и описании целостной правовой модели допустимого обучения моделей искусственного интеллекта, обеспечивающей согласованное применение Акта об ИИ и *GDPR* при сохранении качества и законности обучения.

Для достижения цели ставятся следующие задачи:

1) обозначить правовые контуры стадии обучения ИИ-моделей, выявив нормативную специфику и конкурирующие регуляторные векторы Акта об ИИ и *GDPR,* включая анализ категорий субъектов, их обязанностей и юридического значения терминов «модель», «система», «обучающие данные», «предназначенная цель»;
2) проанализировать трансформацию принципа минимизации данных в условиях потребности в больших и репрезентативных обучающих наборах и связать ее с требованиями к качеству данных и предотвращению дискриминации;
3) сформулировать нормативную модель соразмерности защитных мер, сопоставив положения (ст. 6–7, 9 и 10) Акта об ИИ[24] (риск-ориентированный подход к управлению рисками ИИ-систем) и ст. 25 *GDPR*[25] с учетом результатов *FRIA;*
4) предложить прикладную схему корпоративного комплаенса по стадиям жизненного цикла ИИ-модели (сбор данных, подготовка, обучение, развертывание, мониторинг), объединяющую требования обоих регламентов и позволяющую реализовать их на уровне процедур и документации.

Правовые контуры обучения ИИ-модели

Структурирование правового поля, в котором функционируют практики обучения искусственного интеллекта, невозможно без предварительного разграничения уровней регламентации

[23] См. об этом также: Siddik, M. (2024). *Datasheets for healthcare AI: A framework for transparency and bias mitigation.* OSF Preprints. https://doi.org/10.31219/osf.io/69ykb

[24] Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 53–54, 56–58.

[25] Регламентирующую защиту персональных данных «по замыслу и по умолчанию» (*data protection by design and by default*). См.: General Data Protection Regulation, 2016 O.J. (L 119) 48.

и уточнения понятийного аппарата. Статья 2 Акта об ИИ прямо закрепляет, что его применение «не затрагивает и не уменьшает» гарантии, установленные иным правом Союза, прежде всего *GDPR*[26]. Тем самым формируется конструкция двойного регулирования: Акт об ИИ задает специальный режим для высокорисковых ИИ-систем, а *GDPR* остается горизонтальной нормой всеобщего действия, определяющей принципы обработки персональных данных и права субъектов[27].

Принцип неснижаемости стандартов *GDPR* превращает отношения между двумя актами не в классическую иерархию «общее — специальное», а в модель согласованного применения: выполнение процедур, предусмотренных Актом об ИИ, не освобождает от следования принципам законности, минимизации и целевого ограничения обработки. Любое технически корректное исполнение требований Акта об ИИ, не опирающееся на принципы *GDPR*, может быть квалифицировано как юридически дефектное. Это уже отражается в практических руководствах по комплаенсу в сфере искусственного интеллекта[28], где отдельно подчеркивается необходимость совмещать риск-ориентированный подход к управлению ИИ-системами и оценку воздействия на основные права.

Внутри этой конструкции ключевым становится вопрос о категориях правовых обязанностей. Акт об ИИ устанавливает следующие уровни требований, адресованных прежде всего провайдерам и импортерам высокорисковых систем:

- управление рисками (ст. 9)[29];
- управление данными: качество, происхождение, точность, безопасность (ст. 10)[30];
- техническая документация (ст. 11)[31];
- ведение регистрационных журналов (*record-keeping*) (ст. 12)[32];
- прозрачность и инструкции для пользователей (*transparency and instructions*) (ст. 13–14)[33] и др.

Эти нормы фактически переносят классические механизмы безопасности продукции (*product safety*) из сферы технического регулирования в область алгоритмической инженерии. *GDPR*, напротив, налагает обязанности в зависимости не от роли в цепочке поставок, а от факта обработки персональных данных[34]. В совокупности это образует *матрицу ответственности*, где каждая стадия жизненного цикла ИИ-системы соотносится с двумя наборами норм — Акта об ИИ и *GDPR*, а также с внутренними стандартами управления рисками и качеством (Söderlund & Larsson, 2024, pp. 10–11).

Примечательно, что в ст. 3(1) Акта об ИИ впервые закреплено нормативное определение ИИ-системы: машинная система, разработанная для работы с различным уровнем автономности и способная, для явных или неявных целей, выводимых человеком, генерировать результаты в виде прогнозов, рекомендаций или решений, влияющих на среду, с которой она

[26] Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 45.

[27] De Luca, S. (2025, February 26). *Algorithmic discrimination under the AI Act and the GDPR*. European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2025)769509

[28] Bird & Bird. (2025). *European Union Artificial Intelligence Act: A guide*. https://www.twobirds.com/-/media/new-website-content/pdfs/capabilities/artificial-intelligence/european-union-artificial-intelligence-act-guide.pdf

[29] Ibid. at 56–57.

[30] Ibid. at 57–58.

[31] Ibid. at 58.

[32] Ibid. at 59.

[33] Ibid. at 59–61.

[34] Об этом см., в частности, следующие положения *GDPR*: ст. 5(1)(c), 6, 9, 12–23, 35 (General Data Protection Regulation, 2016 O.J. (L 119) 35, 36–37, 38–39, 39–47, 53–54).

взаимодействует[35]. Как следует из соображения 12 преамбулы, понятие ИИ-системы в Акте об ИИ[36] конструируется функционально, вокруг способности системы осуществлять алгоритмический вывод (*inference*)[37], а не вокруг конкретного семейства технологий. В сферу регулирования включаются как подходы машинного обучения[38], обучающиеся на данных, так и логико- и знание-ориентированные подходы (символьные/экспертные методы), тогда как «более простое» традиционное программное обеспечение, основанное исключительно на правилах, заданных человеком для автоматического исполнения операций, из охвата исключается. Дополнительно, согласно заключению 28/2024 Европейского совета по защите данных, подпадают также и нейросетевые архитектуры, но и системы, основанные на заранее заданных правилах (*rule-based systems*), статистические алгоритмы и гибридные решения[39]. Функционально-ориентированный подход смещает акцент с конкретной технологии на результат и контекст использования, что принципиально для правового анализа и оценки рисков; детерминированное программное обеспечение общего назначения при этом выводится за пределы действия акта.

Такое нормативное конструирование имеет два существенных следствия. Во-первых, все процедуры обучения (начальное обучение (*initial training*), переобучение (*retraining*), дообучение модели на новых данных) прямо включаются в жизненный цикл ИИ-системы и рассматриваются как объект регулирования Акта об ИИ. Во-вторых, статья 3 Акта об ИИ вводит категории «обучающие», «проверочные» и «тестовые данные» (*training, validation u testing data*), акцентируя требования к их качеству, репрезентативности и, по возможности, свободе от ошибок[40]. Эти характеристики непосредственно связаны с обязанностью провайдера по ст. 10 Акта об ИИ выявлять и устранять смещения в наборе данных (*dataset bias*)[41], т. е. структурную предвзятость, например недопредставленность отдельных групп или использование устаревших паттернов поведения, и связывают управление данными с принципом недискриминации и защитой фундаментальных прав (van Bekkum, 2025, p. 7)[42].

На этом фоне особое значение приобретает разграничение понятий «система искусственного интеллекта» (ИИ-система) и «модель искусственного интеллекта» (ИИ-модель). ИИ-система

35 Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 46.

36 Ibid. at 4.

37 *Inference* — вывод (инференс), то есть способность ИИ-системы «выводить», как сгенерировать результаты (прогнозы, рекомендации или решения) на основе входных данных и целей, заданных человеком. Или рассуждение, с помощью которого делаются выводы по известным предпосылкам. См.: Федеральное агентство по техническому регулированию и метрологии (Росстандарт). (2024). *ГОСТ Р 71476–2024 (ИСО/МЭК 22989:2022). Искусственный интеллект. Концепции и терминология искусственного интеллекта*. https://docs.cntd.ru/document/1310068314

38 *Machine learning* — процесс автоматического обучения и совершенствования поведения системы искусственного интеллекта на основе обработки массива обучающих данных без явного программирования. См.: Федеральное агентство по техническому регулированию и метрологии (Росстандарт). (2021). *ГОСТ Р 59895–2021. Технологии искусственного интеллекта в образовании. Общие положения и терминология.* https://rst.gov.ru:8443/file-service/file/load/1682520552039

39 European Data Protection Board, *Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models* (Dec. 17, 2024), https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf

40 Ibid. at 48.

41 Ibid. at 57–58.

42 См. об этом также: Niemiec, E., Davis, P., & Hauglid, M. (2024). *Will the EU AI Act help to eliminate dataset bias in medical AI?* SSRN. https://doi.org/10.2139/ssrn.5045561

в понимании Акта об ИИ определяется функционально как машинная система, способная осуществлять алгоритмический вывод (*inference*) и генерировать результаты (прогнозы, рекомендации или решения), влияющие на среду, в которой она применяется (ст. 3(1); п. 12 преамбулы)[43]. ИИ-модель, напротив, рассматривается как алгоритмическое ядро и компонент, который может быть встроен в ИИ-систему, но сам по себе не образует ИИ-систему (п. 97 преамбулы)[44]. Юридически обязанности провайдера по Акту об ИИ структурно привязаны к ИИ-системе как объекту вывода на рынок/ввода в эксплуатацию и обеспечения соответствия требованиям регламента (для высокорисковых ИИ-систем, в частности, ст. 16 Акта об ИИ)[45], тогда как на уровне модели концентрируются ключевые технические риски для персональных данных и основных прав, оценка которых в части защиты данных традиционно проводится через призму *GDPR* и смежных актов.

В настоящей работе основное внимание уделяется именно ИИ-модели как носителю рисков, связанных с обучающими данными. Для целей анализа используется в том числе понятие «базовая модель» (*foundation model*) — разновидность модели общего назначения (*general-purpose model*), описанная в пп. 97–100 преамбулы Акта об ИИ как крупная генеративная модель с миллиардом и более параметров, способная выполнять широкий спектр задач[46]. Такая модель не образует ИИ-систему до тех пор, пока не встроена в прикладной интерфейс и не связана с конкретным сценарием принятия решений; ее правовой режим, следовательно, определяется сочетанием требований Акта об ИИ к качеству и управлению данными и принципов *GDPR,* применимых к этапу обучения.

Особого внимания заслуживает понятие смещения в наборе данных (*dataset bias*). В статьях 10 и 44 Акта об ИИ[47] оно становится связующим звеном между принципом недискриминации (ст. 21 Хартии ЕС об основных правах[48]) и принципом минимизации данных. Законодатель прямо указывает, что одного лишь количественного критерия (размера выборки) недостаточно: необходим качественный анализ предвзятости и потенциальных дискриминационных эффектов, в том числе, в исключительных случаях, использование специальных категорий данных для корректирующих целей В литературе такая постановка вопроса описывается как практическая коллизия между потребностью диагностировать предвзятость по группам и ограничениями режима специальных категорий персональных данных: верификация дискриминационных исходов нередко требует доступа к чувствительным атрибутам или их приближенным заменителям, тогда как *GDPR* в типичных сценариях ограничивает сбор и использование таких данных, а согласие часто не отвечает критерию свободного волеизъявления. Одновременно подчеркивается, что наращивание массивов сверх строгой необходимости конфликтует с принципами минимизации и целевого ограничения, повышая риск «ползучего расширения» задач и масштабов обработки (*function creep*); в качестве одного из способов удержания баланса обсуждается использование синтетических данных как инструмента снижения рисков для частной жизни при сохранении задач контроля предвзятости (*bias*) (van Bekkum, 2025, p. 7; van Bekkum & Zuiderveen Borgesius, 2023, pp. 5–6, 7; Veltmeijer & Gerritsen, 2025, pp. 3174–3175).

---

43 Niemiec, E., Davis, P., & Hauglid, M. (2024). *Will the EU AI Act help to eliminate dataset bias in medical AI?* SSRN 4, 46.

44 Ibid. at 26.

45 Ibid. at 62.

46 Ibid. at 26.

47 Ibid. at 57–58, 79.

48 Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 400.

С учетом указанной дихотомии разработчик корпоративной ИИ-системы на обучающей стадии сталкивается как минимум с тремя ключевыми задачами:

1) установить, относится ли создаваемый продукт к высокорисковым согласно ст. 6 Акта об ИИ[49] и, следовательно, подпадает ли он под жесткий режим регулирования;
2) определить, содержит ли обучающий набор персональные данные в понимании ст. 4(1) *GDPR* и специальные категории данных в смысле ст. 9 *GDPR*[50];
3) оценить наличие разумно предсказуемого риска для основных прав, что может требовать проведения процедуры *DPIA* и, в отдельных случаях, *FRIA*.

В отличие от абстрактного анализа норм процедура оценки воздействия на защиту данных (*DPIA*) позволяет продемонстрировать регулятору и самим субъектам данных, каким образом оператор учел выявленные риски и превратил их в управляемые параметры проектного цикла.

DPIA должна включать описание операций и целей обработки; правовой анализ и выбор правового основания; идентификацию и оценку рисков; перечень технических и организационных мер защиты; оценку остаточного риска и, при необходимости, консультацию с надзорным органом (ст. 36 *GDPR*)[51].

В качестве иллюстрации рассмотрим применение процедура оценки воздействия на защиту данных (*DPIA*) при обучении модели кредитного скоринга в финансовом секторе. Банк, разрабатывающий алгоритм оценки вероятности дефолта клиента, обрабатывает комплексные массивы персональных данных: кредитные истории, транзакции, сведения из процедур *KYC (Know Your Customer),* иногда дополнительные профили из внешних источников. При этом возникает реальная опасность косвенной дискриминации по косвенным социальным признакам, опосредованно связанным с защищаемыми характеристиками (например, по месту проживания, типу занятости, уровню дохода, модели потребления) и меморизации («запоминания») чувствительной информации моделью. В рамках *DPIA* банк фиксирует цели обработки, источники данных и сценарии их повторного использования. Для принятия решения о кредите правовым основанием служит статья 6(1)(b) *GDPR* (исполнение обязательства из договора), тогда как для последующего улучшения модели — статья 6(1)(f) *GDPR* (законный интерес) в сочетании с усиленной минимизацией и ограничением доступа[52]. Отбор переменных при этом осуществляется не по принципу «чем больше, тем лучше», а по доказанной значимости для качества прогнозирования и влиянию на риск дискриминации.

Следующий блок *DPIA* посвящен идентификации и оценке рисков для прав субъектов данных: непрозрачность алгоритмической логики, возможность косвенной дискриминации уязвимых групп, риск утечки информации через поведение модели. Каждый риск получает оценку вероятности и тяжести последствий, после чего формируется набор компенсирующих мер: регулярный аудит смещений (*bias*); мониторинг дрейфа данных и деградации качества; использование специальных категорий данных исключительно для тестирования справедливости и недопущение их включения в «боевую» модель. Результатом *DPIA* становится формализация остаточного риска; если он признается высоким, оператор обязан обратиться за консультацией к надзорному органу в порядке ст. 36 *GDPR*[53]. Такая консультация не является формальной,

[49] Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 53–54.
[50] General Data Protection Regulation, 2016 O.J. (L 119) 33, 38–39.
[51] Ibid. at 118–119.
[52] Ibid. at 36.
[53] Ibid. at 54–55.

а представляет собой механизм диалога о допустимых границах применения искусственного интеллекта в конкретном секторе.

Особенно показательна взаимосвязь между ст. 10 Акта об ИИ (управление данными)[54] и ст. 25 *GDPR* (защита персональных данных по замыслу и по умолчанию)[55]. Первая предписывает обеспечивать качество, репрезентативность и корректность данных, а также процедуры управления ими; вторая требует встроенной минимизации и защиты уже на этапе проектирования архитектуры обработки. Только наложение этих требований формирует юридически валидный пайплайн обучения: *GDPR* задает горизонтальные пределы допустимой обработки, а Акта об ИИ утверждает вертикальные процедуры доказательства ее безопасного и недискриминационного характера.

Дополнительное значение приобретает международный стандарт *ISO/IEC 42001:2023* — первый сертификационный стандарт для систем управления ИИ, интегрирующий риск-ориентированное мышление, предполагающее принятие решений с учетом вероятности и тяжести последствий (*risk-based thinking*), и механизмы постоянного улучшения[56]. Его практическая ценность заключается в том, что он создает процессную прослойку между нормами и инженерными практиками, подтверждая, что принцип минимизации *GDPR* и процедуры управления данными Акта об ИИ укоренены в системе менеджмента компании, а не применяются разово «под аудит».

Уточнение субъектного состава завершает правовые очертания обучения. Статья 3(3) Акта об ИИ вводит фигуру провайдера (*provider*) — лица, размещающего систему на рынке под своим именем[57], одновременно опираясь на традиционные категории, предусмотренные *GDPR*, — «контролер, оператор персональных данных» (*controller*) и «обработчик» (*processor*) (пп. 7–8 ст. 4 *GDPR*)[58]. На практике одна и та же компания может совмещать обе роли: при разработке выступать оператором по отношению к обучающему набору, а при выводе продукта на рынок становиться провайдером высокорисковой системы. В результате формируется управленческая матрица обязанностей, в которой по вертикали располагаются стадии жизненного цикла (сбор, подготовка, обучение, валидация, эксплуатация и мониторинг), а по горизонтали — кластеры регуляторных норм (обязанности по *GDPR,* требования Акта об ИИ, процедуры согласно стандарту *ISO/IEC 42001:2023*). Такая матрица служит инструментом распределения ответственности, планирования ресурсов комплаенса и включения управления рисками в цикл разработки ИИ-модели.

Принцип минимизации данных как ценностный фильтр и методологическая опора обучения ИИ-моделей

Принцип минимизации данных в ст. 5(1)(c) *GDPR* формулируется через триаду «адекватность — релевантность — ограниченность необходимым»[59]. Адекватность означает соответствие данных поставленной цели, релевантность — наличие прямой связи данных с задачей обработки,

[54] Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 57–58.

[55] General Data Protection Regulation, 2016 O.J. (L 119) 48.

[56] International Organization for Standardization. (2023). *ISO/IEC 42001:2023: Information technology — artificial intelligence — management system*. https://www.iso.org/standard/81230.html

[57] Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 45.

[58] General Data Protection Regulation, 2016 O.J. (L 119) 33.

[59] Ibid. at 35.

а ограниченность необходимым предполагает невозможность достижения цели без конкретного элемента данных. Минимизация в правовом смысле подразумевает то, что обрабатываться должен только тот объем информации, который действительно нужен для конкретной цели[60] (Finck & Biega, 2021, pp. 55–57).

На практике это превращает минимизацию в инструмент управления рисками: каждое решение о включении нового атрибута (например, даты рождения, геолокации, детализированной истории транзакций) должно оцениваться через призму необходимости для достижения заявленной цели обработки и соразмерности вмешательства в права субъекта персональных данных. Суд Европейского союза в деле *Meta Platforms Ireland v. Bundesverband der Verbraucherzentralen & Verbraucherverbände*[61] подчеркнул, что даже при наличии выраженного коммерческого интереса, включая финансирование деятельности за счет персонализированной рекламы, допустимость обработки определяется тестом необходимости и пропорциональности, а также наличием менее ограничивающих альтернатив; при этом в условиях широкого и фактически «почти тотального» мониторинга поведения пользователей интересы и основные права последних могут иметь приоритет над интересом оператора, что усиливает значение минимизации как требования исключать из обработки избыточные и идентифицирующие элементы, не являющиеся строго необходимыми для цели[62].

Дополнительный уровень сложности создает статья 10 Акта об ИИ, которая требует, чтобы обучающие выборки[63] были репрезентативными, полными и, по возможности, свободными от ошибок[64]. Репрезентативность предполагает, что выборка отражает свойства всей целевой популяции (например, база клиентов банка включает разные возрастные группы, регионы, социальные категории). Полнота означает наличие признаков, без которых задача модели не может быть решена (например, отсутствие данных о доходах делает кредитный скоринг заведомо деформированным). Требование «по возможности, свободными от ошибок» связано с очисткой выборки от дубликатов, некорректных, противоречивых и явно устаревших значений.

На уровне формальной логики требования минимизации и репрезентативности выглядят как напряженная пара: чем больше данных собрано, тем проще обеспечить статистическую устойчивость[65], но тем выше регуляторный риск избыточной обработки. Разрешение этого противоречия осуществляется через принцип соразмерности, закрепленный в ст. 52 Хартии ЕС об основных правах: вмешательство в права допускается лишь в той мере, в какой оно необходимо и пропорционально легитимной цели[66]. Для обучения моделей это означает, что использование крупных выборок оправданно только при доказанной необходимости для достижения статистической устойчивости и недискриминационного результата и при отсутствии менее

---

60 European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (Version 2.0, adopted October 20, 2020), https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

61 Case C-319/20, Meta Platforms Ireland Ltd. v. Bundesverband der Verbraucherzentralen & Verbraucherverbände, ECLI:EU:C:2022:322, ¶ 51–56, 83 (Apr. 28, 2022).
По решению органов государственной власти Российской Федерации, организация *Meta Platforms, Inc.* признана экстремистской, ее деятельность запрещена на территории России.

62 Case C-252/21, Meta Platforms Inc. v. Bundeskartellamt, ECLI:EU:C:2022:704, ¶ 108–109, 115–118, 121 (Sept. 20, 2022).

63 *Training datasets* — обучающие датасеты, массивы данных, на которых строится и корректируется модель.

64 Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 57.

65 *Robustness* — устойчивость модели к вариациям входных данных.

66 Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 407.

инвазивной альтернативы (например, работы с агрегированными данными или более грубой детализацией признаков).

Современные исследования машинного обучения подтверждают, что рост объема и детализации данных не является безусловным благом. Так, чрезмерное увеличение числа параметров модели (глубины нейронной сети, количества признаков) приводит к переобучению[67] (Rocks & Mehta, 2022, p. 15). Технически это выражается в снижении числа ошибок на обучающих данных при одновременном росте на тестовом наборе. Для правового анализа важно не само понятие дисперсии и смещения, а вывод: существует точка, после которой увеличение объема и детализации данных ухудшает качество решения и, следовательно, не может считаться необходимым в смысле ст. 5(1)(c) *GDPR*[68].

Один из практических способов совместить требования минимизации и репрезентативности — статистическая подвыборка[69]. Основанная на понятных критериях (устранение повторов, выравнивание дисбаланса групп, исключение очевидных выбросов), она одновременно снижает регуляторный риск и повышает обобщающую способность модели. В юридической плоскости это можно рассматривать как реализацию принципов минимизации и защиты данных по замыслу *(data protection by design)* (ст. 25 *GDPR*) средствами инженерного проектирования[70].

Существенную роль играют и методы обезличивания. Классическим подходом остается *k*-анонимность[71]. Исследования показывают, что разумно сконструированная *k*-анонимность может снижать риск повторной идентификации при минимальном влиянии на качество классификации (Slijepčević et al., 2021). Дополнительно используется *l*-диверсификация[72], что препятствует восстановлению личности по редким комбинациям атрибутов. Эти техники не устраняют полностью юридическую связь с понятием персональных данных, но позволяют уменьшить степень вмешательства и продемонстрировать надзорному органу, что контролер предпринял разумные шаги к минимизации риска.

В праве ЕС минимизация данных в сфере обучения ИИ-моделей трактуется не как разовое сокращение признаков, а как управленческий и юридический процесс, встроенный в деятельность контролера. Статья 5(1)(c) *GDPR* и принцип подотчетности в ст. 5(2) *GDPR* требуют, чтобы контролер мог объяснить и задокументировать, почему каждый элемент данных включен в обработку[73]. На практике это реализуется через поэтапную процедуру.

Первый этап — инвентаризация признаков. Контролер составляет полный перечень атрибутов, планируемых к использованию в обучении, и проводит их классификацию по уровню идентифицируемости. Условно можно выделить три уровня. Уровень *A* включает прямые идентификаторы (имя, паспортные данные, телефон, адрес электронной почты); их сохранение в исходном виде в обучающем наборе допустимо лишь в исключительных случаях. Как правило,

[67] Более известному как *"overfitting"* — ситуация, когда модель идеально подгоняется под обучающий набор, но теряет способность к обобщению в отношении новых случаев.

[68] General Data Protection Regulation, 2016 O.J. (L 119) 35–36.

[69] *Subsampling* — формирование уменьшенного набора данных за счет удаления дубликатов, нерелевантных и явно избыточных наблюдений.

[70] Ibid. at 48.

[71] *K-anonymity* — модель, при которой каждая запись в наборе неотличима как минимум от *k – 1* других. Если, например, *k* = 10, то каждый субъект статистически растворен в группе из не менее 10 лиц с одинаковой комбинацией основных атрибутов (возраст, регион, тип договора).

[72] *L-diversity* — условие, при котором в каждой *k*-анонимной группе присутствует не менее одного различного значения чувствительного признака, например диагноза или уровня дохода.

[73] Ibid. at 35–36.

в отношении них требуется либо удаление, либо псевдонимизация[74] (ст. 4(5) *GDPR*)[75]. Уровень *B* охватывает квази-идентификаторы (возраст, регион, профессию, комбинацию характеристик), которые по отдельности не раскрывают личность, но в совокупности могут вести к идентификации; их использование требует прохождения теста невозможности альтернативы, когда оператор должен документально подтвердить, что без этих данных невозможно обеспечить требуемое качество модели. Уровень *C* составляют менее чувствительные признаки, в отношении которых приоритет имеют укрупнение, агрегирование и обезличивание, если потери качества остаются в пределах статистически допустимого диапазона.

Результаты такой классификации фиксируются в журнале минимизации данных — внутреннем документе контролера, который совмещает управленческую и доказательственную функции. По сути, это специализированный реестр операций обработки в смысле ст. 30 *GDPR*[76], ориентированный не столько на описание целей и категорий данных, сколько на обоснование необходимости и пропорциональности использования каждого признака. Практика национальных регуляторов показывает, что именно подобные журналы становятся первым запрашиваемым документом при проверке проектов на базе ИИ: они демонстрируют, что принцип минимизации не остался декларацией, а был реализован в процессе проектирования[77].

Второй этап — отбор минимально представительного среза данных. Здесь можно говорить о двух правовых фильтрах. Во-первых, фильтр доминирующей информации: сохраняются только признаки, вклад которых в достижение цели подтвержден результатами тестирования и документирован в отчете *DPIA* или аналогичных материалах. Во-вторых, фильтр уникальности: редкие комбинации атрибутов должны быть агрегированы, чтобы каждый субъект оказался статистически скрыт в группе (по крайней мере из нескольких лиц), что снижает риск повторной идентификации, особенно при малых выборках.

Третий этап связан с применением технологий усиления приватности[78]. В качестве наиболее показательного примера в литературе обычно рассматривается дифференциальная приватность как формализованный подход к ограничению утечек о конкретных записях в наборе данных за счет добавления контролируемой случайности в результаты вычислений[79] (Dwork et al., 2006, pp. 270–271).

В техническом смысле требование описывается через устойчивость вывода алгоритма к единичным изменениям исходного набора: результат должен оставаться практически одинаково вероятным как при наличии в данных одной конкретной записи, так и при ее отсутствии. Иначе говоря, для любого возможного результата вероятность его получения на двух «соседних» наборах данных (отличающихся одной записью) может различаться лишь в строго ограниченных пределах: допускается ограниченное расхождение по масштабу вероятностей и только очень малая дополнительная вероятность отклонения за пределы этого ограничения. Эта конструкция направлена на то, чтобы по наблюдаемому выходу алгоритма нельзя было надежно восстановить факт наличия конкретного субъекта в наборе данных или извлечь

[74] *Pseudonymisation* — замена идентификаторов токенами или хешами.

[75] Ibid. at 33.

[76] Ibid. at 50–51.

[77] DLA Piper. (2025). *National data protection authority in Germany.* https://www.dlapiperdataprotection.com/?t=authority&c=DE

[78] *Privacy-enhancing technologies (PETs)* — технологии усиления защиты данных.

[79] *Differential privacy* — математически контролируемое добавление случайных искажений — «шума» — к данным или результатам вычислений, при котором вклад отдельного лица становится статистически неразличимым.

чувствительную информацию о нем. В европейской практике дифференциальная приватность все чаще рассматривается как мера, совместимая с принципом «защита данных по замыслу и по умолчанию» (*data protection by design and by default*) (ст. 25 *GDPR*)[80], при условии документирования выбранного механизма, обоснования отсутствия менее инвазивных альтернатив и оценки влияния добавленной случайности на качество и устойчивость модели при условии документирования выбранного механизма (описание примененной схемы, области применения и того, какие выходы алгоритма защищаются), обоснования отсутствия менее инвазивных альтернатив (сопоставление с вариантами, требующими меньшего объема персональных данных или меньшего вмешательства в обработку) и оценки влияния добавленной случайности на качество и устойчивость модели (в том числе на сохранение сопоставимой точности и долей ошибок для различных групп субъектов и на отсутствие систематически худших результатов для уязвимых или защищаемых групп, что важно для предотвращения дискриминационных исходов).

Особое место в сегодняшней дискуссии занимает федеративное обучение[81]. На интуитивном уровне может показаться, что сохранение данных «на месте» автоматически устраняет риски для персональных данных. Однако с точки зрения *GDPR* ситуация сложнее. В соответствии со ст. 4(1) *GDPR* персональными являются любые сведения, относящиеся к идентифицированному или идентифицируемому лицу[82], а Европейский совет по защите данных в заключении 28/2024 подчеркивал, что даже косвенные цифровые следы могут образовывать персональные данные, если существует разумная вероятность их использования для повторной идентификации[83]. Градиенты и обновления весов при определенных условиях могут быть инвертированы, что позволит восстановить отдельные характеристики исходных записей.

Это означает, что в федеративной архитектуре контролер не может автоматически считать градиенты безличной информацией. При наличии разумно предсказуемого риска реконструкции индивидуальных записей возникает высокая степень угрозы для прав и свобод субъектов, а значит, необходимо проводить *DPIA* по ст. 35 *GDPR*[84]. В рамках такой оценки контролер должен показать, что архитектурное решение дополнено достаточными гарантиями: сокращением экстремальных градиентов, использованием защищенной агрегации[85], криптографических механизмов вроде гомоморфного шифрования[86]. Эти технические меры приобретают юридическое значение, только когда описаны в *DPIA,* закреплены в политиках обработки и отражены в реестре операций обработки.

Юридический смысл такого подхода состоит в том, что минимизация данных превращается из абстрактного принципа в последовательный процесс проектных решений: от отбора признаков и структурирования датасета до выбора архитектуры обучения и применения технологий усиления защиты данных (*PETs*). Для обучения ИИ-моделей это означает, что допустимыми признаются только те конфигурации данных и процедур, по которым контролер способен

[80] General Data Protection Regulation, 2016 O.J. (L 119) 48.

[81] *Federated learning* — архитектура, при которой модель обучается распределенно, на устройствах или серверах участников, а в центральный контур передаются только обновления параметров или градиенты.

[82] Ibid. at 48.

[83] European Data Protection Board. (2024). *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*. https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf

[84] General Data Protection Regulation, 2016 O.J. (L 119) 53–54.

[85] *Secure aggregation* — протоколы, не позволяющие анализировать обновления на уровне отдельных участников.

[86] *Homomorphic encryption* — шифрование, допускающее вычисления с зашифрованными данными.

убедительно показать: каждый элемент необходим, альтернативы с меньшим объемом данных не обеспечивают сопоставимого качества, а остаточный риск для фундаментальных прав снижен до приемлемого уровня и задокументирован.

Принцип соразмерности защитных мер в регулировании обучения ИИ-моделей

Принцип соразмерности защитных мер в праве Европейского союза предполагает, что объем и характер технических и организационных мер должны соответствовать уровню риска для прав и свобод субъектов данных и серьезности возможных последствий. В сфере защиты данных он отражен прежде всего в статье 25 *GDPR,* закрепляющей требование защиты данных по замыслу и по умолчанию (*data protection by design and by default*), и в статье 32 *GDPR,* устанавливающей обязанность обеспечить надлежащий уровень безопасности с учетом состояния техники, стоимости внедрения, характера, объема, контекста и целей обработки[87]. Иначе говоря, оператор обязан не просто применить набор мер, а обосновать, почему именно такой набор является достаточным и пропорциональным рискам.

Статья 10(2) Акта об ИИ развивает эту логику применительно к высокорисковым ИИ-системам: провайдеры обязаны не только защищать данные, но и формализовать управление обучающими наборами (*data governance*), документируя их происхождение, качество, репрезентативность и отсутствие систематических искажений[88]. Тем самым Акт об ИИ смещает фокус с индивидуального риска (логика *GDPR*) на риск алгоритмического воздействия на группы и общество в целом: неправильно обученная модель может приводить к дискриминации, ошибкам в доступе к социальным услугам, кредитованию, здравоохранению (Novelli et al., 2024a, p. 8). Поэтому соразмерность здесь имеет два критерия оценки: с позиции стандарта охраны прав субъекта персональных данных (*DPIA* по ст. 35 *GDPR*)[89] и риска нарушения основных прав (*FRIA*) в духе Хартии ЕС об основных правах[90].

Базовым примером соразмерной меры выступает псевдонимизация согласно ст. 4(5) *GDPR*[91]. Она позволяет отделить идентификаторы (ФИО, паспортные данные, контактную информацию) от остальной части обучающего набора, сохранив возможность контролируемого восстановления личности через отдельный ключ в защищенной системе управления ключами. Однако международный стандарт *ISO/IEC 27559:2022* справедливо указывает, что одной псевдонимизации недостаточно: при объединении разных наборов данных сохраняется риск фоновой деанонимизации (*background re-identification*), когда лицо идентифицируется путем сопоставления псевдонимизированных записей с внешними источниками[92]. Поэтому псевдонимизация рассматривается как необходимая, но не достаточная мера и должна дополняться минимизацией, укрупнением редких сочетаний и контролем доступа.

Для специальных категорий данных (ст. 9 *GDPR*)[93] и высокочувствительных обучающих наборов усиливается роль *дифференциальной приватности*[94]. В литературе данный подход

87 Ibid. at 48, 51–52.

88 Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 57.

89 General Data Protection Regulation, 2016 O.J. (L 119) 53.

90 Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 407.

91 General Data Protection Regulation, 2016 O.J. (L 119) 33.

92 International Organization for Standardization. (2023). *ISO/IEC 42001:2023: Information technology — artificial intelligence — management system.* https://www.iso.org/standard/81230.html

93 General Data Protection Regulation, 2016 O.J. (L 119) 38–39.

94 См. подробнее о дифференциальной приватности предыдущий раздел настоящей статьи.

описывается как предпочтительный для случаев, когда одного обезличивания недостаточно для снижения риска выводимости сведений о субъекте (то есть когда по результатам обработки сохраняется вероятность восстановить связь с конкретным лицом либо извлечь о нем чувствительную информацию) (Arasteh et al., 2024, p. 2; Liu et al., 2024, pp. 737–738). С правовой точки зрения настройка используемого механизма и объема вносимой случайности образует вопрос соразмерности: недостаточная степень усиления защиты делает меры фактически формальными (результаты остаются статистически различимыми в зависимости от участия конкретной записи), тогда как чрезмерное усиление может существенно ухудшить качество модели (увеличить ошибку, снизить устойчивость и привести к неравномерному росту ошибок для отдельных групп субъектов, что повышает риск дискриминационных исходов). Для небольших выборок и редких случаев (например, редких заболеваний) это требует проведения отдельной процедуры оценки воздействия на защиту данных (*DPIA*) с фиксацией того, почему выбран именно данный способ усиления защиты и каким образом оценено его влияние на точность, устойчивость и потенциальные дискриминационные эффекты.

Следующий слой соразмерных мер связан с классическими средствами информационной безопасности: контролем доступа, ролевыми моделями и шифрованием. Принцип наименьших привилегий (*least privilege*) предполагает, что разработчик, дата-сайентист или администратор получают доступ только к тем данным, которые им действительно необходимы для выполнения задачи (Menges et al., 2021, p. 2). Статья 32(1) *GDPR* прямо называет среди мер шифрование[95], обеспечивающее защиту от несанкционированного доступа как при компрометации инфраструктуры, так и при перехвате трафика[96]. Для высокорисковых систем добавляются аппаратные технологии, например безопасные анклавы[97]. Они особенно актуальны для медицинских, биометрических и иных чувствительных сценариев, где компрометация обучающего контура приводит к необратимому ущербу (Novelli et al., 2024a, p. 7; Novelli et al., 2024b, pp. 5–6; Basdekis et al., 2023, p. 2)[98].

Отдельный класс архитектурных мер соразмерности связан с сокращением объема передаваемых данных за счет изменения самого процесса обучения. Федеративное и раздельное обучение[99] часто позиционируется как решение проблем конфиденциальности (Haripriya et al., 2025, pp. 10–11; Pham et al., 2023, pp. 988–989). Однако с точки зрения *GDPR* и Акта об ИИ эти архитектуры не снимают обязанность по оценке рисков, а лишь смещают ее в другую плоскость. Как показывают исследования по инверсии градиентов (*gradient inversion*), при недостаточно защищенной агрегации обновлений возможно восстановление исходных признаков. Следовательно, градиенты и обновления весов должны рассматриваться как потенциальные персональные данные, а применение федеративного обучения — сопровождаться *DPIA* и, при высокорисковых сценариях, *FRIA*. Соразмерный набор мер в этом контексте включает обрезку экстремальных градиентов, протоколы защищенной агрегации, исключающей анализ обновлений по отдельным клиентам, а при необходимости — криптографические механизмы, включая гомоморфное шифрование.

---

95 *Encryption* — защита данных при хранении и передаче.

96 Ibid. at 51–52.

97 *Secure enclaves* — изолированные области памяти, внутри которых выполняются вычисления с данными и параметрами модели без доступа со стороны остальной системы.

98 Krause, D. (2024). *Addressing the challenges of auditing and testing for AI bias: A comparative analysis of regulatory frameworks.* SSRN. https://doi.org/10.2139/ssrn.5050631

99 *Split learning* — разделение модели на локальную и серверную части.

В практическом управлении рисками выбор сочетания мер не может быть произвольным. Организации, работающие с высокорисковыми ИИ-системами, выстраивают многоуровневую модель анализа угроз, опираясь на четыре базовых параметра: тип и чувствительность данных, масштаб и критичность проекта, профиль потенциального нарушителя и экономическую оправданность мер. Если обрабатываются специальные категории данных в крупных массивах, риск априори оценивается как высокий, что влечет обязанность проведения *DPIA* (ст. 35 *GDPR*)[100] и зачастую *FRIA*, а также применения нескольких уровней защиты одновременно: от псевдонимизации и строгого разграничения доступа до дифференциальной приватности, защищенной агрегации и аппаратных анклавов. Для обезличенных или низкочувствительных наборов достаточно базового шифрования и ролевой модели доступа при условии, что сохранен риск-ориентированный подход.

При иных подходах эта логика институционализируется через формальные рамки управления рисками. Документы из системы актов *NIST IR (NIST Incident Response),* включая *IR 8286C*, хотя и потеряли официальный статус, демонстрируют полезную методологию: угрозы сводятся в единый реестр, каждой присваивается уровень риска, а меры защиты привязываются одновременно к бизнес-целям и нормативным требованиям[101]. В европейском контексте аналогичную функцию начинает выполнять *ISO/IEC 42001:2023* — стандарт системы управления ИИ, встраивающий риск-ориентированное мышление (*risk-based thinking*) и непрерывное улучшение в процессы разработки и эксплуатации ИИ[102]. В результате принцип соразмерности перестает быть абстрактным и превращается в управленческую практику: риск идентифицируется, оценивается и «закрывается» документированным набором мер.

Для упорядочения применения защитных средств организации, работающие с обучением моделей, как правило, формируют два слоя документации. Первый — матрица рисков, в которой категориям риска (низкий, средний, высокий) соответствуют обязательные комбинации технических и организационных мер: от псевдонимизации и базового шифрования до дифференциальной приватности, защищенной агрегации и использования аппаратных анклавов. Второй — специализированная процедура оценки рисков обучения моделей (*training DPIA*), где устанавливаются критерии запуска оценки, пороговые значения для высокого риска, роли участников и взаимосвязь между *DPIA, FRIA* и требованиями Акта об ИИ к управлению данными.

В совокупности такие меры формируют согласованный контур защит, в котором псевдонимизация и минимизация выступают базовым уровнем, дифференциальная приватность и архитектурные решения (федеративное / раздельное обучение) — усилением для чувствительных сценариев, а криптографические и аппаратные механизмы — уровнем для критически важных систем. Принцип соразмерности в этой модели означает не экономию на защите, а обязательность выбора и документирования именно тех мер, которые адекватны характеру данных, целям обучения и тяжести возможных последствий для фундаментальных прав.

---

100 General Data Protection Regulation, 2016 O.J. (L 119) 53.

101 Quinn, S., Ivy, N., Barrett, M., Witte, G., & Gardner, R. K. (2022). *Staging cybersecurity risks for enterprise risk management and governance oversight* (NIST Interagency Report No. NIST IR 8286C-upd1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8286C-upd1

102 International Organization for Standardization. (2023). *ISO/IEC 42001:2023: Information technology — artificial intelligence — management system*. https://www.iso.org/standard/81230.html

Комплаенс по жизненному циклу ИИ-модели

Жизненный цикл крупной ИИ-модели *(large-scale AI model),* т. е. программной системы, использующей методы машинного обучения и имеющей параметрический масштаб не ниже миллиардного порядка, включает несколько ключевых этапов, каждый из которых имеет самостоятельное правовое значение.

Прежде всего определяются цель и сфера применения модели. По сути, речь идет о формулировании задачи, ради которой создается или адаптируется ИИ-система: к примеру, анализ медицинских изображений, обработка естественного языка, кредитный скоринг, прогнозирование финансовых рисков и т. п. В юридической плоскости это соответствует установлению цели обработки персональных данных в смысле ст. 5(1)(b) *GDPR*[103]*:* диагностические, образовательные, управленческие, сервисные или иные задачи, подлежащие последующему документированию в политике обработки и оценке воздействия (с позиций *DPIA, FRIA* и Акта об ИИ).

На следующем этапе разработчик выбирает архитектурный подход: использовать уже существующую модель (дообучение имеющейся архитектуры нейронной сети или иной модели) либо проектировать и обучать модель с нуля[104]. От этого решения зависят состав данных, объем вычислений и набор юридических рисков: при дообучении неизбежно встает вопрос о повторной обработке ранее собранных персональных данных, при обучении с нуля — о правомерности изначального сбора и масштабах выборки.

Далее следует этап сбора и подготовки обучающих данных[105]. На этой стадии формируются обучающие выборки данных, которые будут использованы для настройки параметров модели. На практике это означает агрегирование объемных массивов данных из открытых источников, публичных реестров, ведомственных систем или коммерчески приобретенных баз. Подготовка включает очистку[106], аннотацию[107] и структурирование данных в формат, пригодный для обучения (Wang et al., 2021, pp. 776–778).

После этого наступает собственно этап обучения модели (*training*). В типичном сценарии он включает предобучение[108] и последующую тонкую настройку (*fine-tuning*). В ходе обучения применяются методы оптимизации[109] и механизмы, предполагающие участие человека, позволяющие достигать требуемой точности и управляемости поведения модели.

Следующий этап — валидация и оценка. Под валидацией понимается проверка модели на отдельной части данных, которая не использовалась при обучении, с целью убедиться в корректности и устойчивости работы. Этап оценки предполагает установление метрик точности и ошибок, а также иных критериев качества, таких как полнота, устойчивость к «шуму», *вариации входных данных* и др.[110] Одновременно исследуются смещения, включая потенциальную дискриминацию по полу, возрасту, региону или иным социально значимым признакам.

---

[103] General Data Protection Regulation, 2016 O.J. (L 119) 35.

[104] Так называемое создание модели *“from scratch”* — полное создание и обучение без базового прототипа.

[105] То есть *“dataset creation and preprocessing”* — формирование и предварительная обработка датасета.

[106] *Data cleaning* — удаление дубликатов, явных ошибок и аномалий.

[107] *Annotation* — разметка данных (аннотирование): присвоение объектам в наборе данных меток (классов, тегов) для обучения и оценки модели, выполняемое вручную либо с использованием полуавтоматических средств.

[108] *Pre-training* — начальная настройка модели на очень больших и разнообразных наборах данных для формирования общих способностей.

[109] *Optimization methods* — математические алгоритмы минимизации функции ошибки модели.

[110] См. об этом в предыдущих разделах статьи.

Завершающий технический этап — развертывание /внедрение модели (*deployment*) в эксплуатационную среду. С этого момента модель начинает использоваться в реальных бизнес- или управленческих процессах, и на разработчика/оператора ложится обязанность по непрерывному мониторингу и периодической переоценке[111] ее качества, рисков и соответствия нормативным требованиям (Wang et al., 2021, p. 781; De Silva & Alahakoon, 2022, pp. 3–4).

Формулируя цель обучения ИИ-модели, необходимо соблюдать принцип ее ограничения (*purpose limitation*). Согласно ст. 5(1)(b) *GDPR* персональные данные должны «собираться для конкретных, явных и законных целей и не подлежат дальнейшей обработке иным образом, несовместимым с этими целями»[112]. Это означает, что цель обучения должна быть заранее определена, описана в документации и связана с конкретными результатами модели; изменение цели впоследствии требует либо нового согласия субъектов персональных данных, либо иного правового основания.

Акт об ИИ дополняет эту конструкцию понятием «предназначенная цель»[113], т. е. учетом условий, контекста и предсказуемых сценариев применения. Для высокорисковых ИИ-систем законодатель прямо требует описывать и принимать к сведению все известные и разумно предсказуемые сценарии использования и злоупотребления. В соответствии со ст. 9 Акта об ИИ провайдер обязан включить предназначенную цель в систему управления рисками (*risk management system*), а любое ее изменение влечет повторную оценку рисков и при необходимости корректировку архитектуры и процессов обучения[114].

Нормы *GDPR* и Акта об ИИ в этой части согласуются: обе системы требуют прозрачности и точности формулирования целей, их документального закрепления и пересмотра при изменении сценариев использования данных.

Сбор данных для обучения должен опираться на одно из оснований, предусмотренных статьей 6(1) *GDPR:* согласие субъекта (*consent*), исполнение договора (*performance of a contract*), выполнение юридической обязанности (*legal obligation*), защита жизненно важных интересов (*vital interests*), выполнение задачи в общественных интересах или при осуществлении публичных полномочий (*public task*), а также законный интерес оператора (*legitimate interest*), если он не перевешивается правами и свободами субъекта[115]. Например, если обучение модели связано с задачами устойчивого развития или общественного здравоохранения, это может квалифицироваться как выполнение задачи в общественных интересах по ст. 6(1)(e) *GDPR*[116].

Если данные были ранее собраны для иной цели, применяется статья 6(4) *GDPR,* предписывающая проверку совместимости целей (*compatibility test*): анализируются связь между первоначальной и новой целями, контекст сбора, характер данных (обычные или специальные категории), возможные последствия для субъектов и предусмотренные меры защиты[117]. Пункт 67 преамбулы к Акту об ИИ подчеркивает необходимость прозрачности относительно исходной цели сбора и последующих трансформаций[118].

---

111 *Re-evaluation* — повторная оценка по установленным метрикам.

112 Ibid.

113 *Intended purpose* — запроектированная область и условия использования ИИ–системы.

114 Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 56–57.

115 General Data Protection Regulation, 2016 O.J. (L 119) 36.

116 Ibid.

117 Ibid. at 37.

118 Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 19–20.

Принцип минимизации данных (ст. 5(1)(c) *GDPR*) требует, чтобы собирались только те персональные данные, которые действительно необходимы для достижения заявленных целей[119]. В то же время статья 10 Акта об ИИ устанавливает требование репрезентативности обучающих данных, т. е. их сбалансированности и отражения ключевых характеристик целевой популяции (например, половозрастной структуры, этнического состава, географического распределения)[120]. На первый взгляд это приводит к противоречию: минимизация предполагает сокращение объема данных, а репрезентативность — расширение набора для отражения разнообразия. Однако в современной доктрине эти категории разводятся: минимизация понимается как отбор только релевантных признаков и исключение избыточной информации, тогда как репрезентативность — как баланс и непредвзятость внутри уже минимизированного множества данных. В практическом измерении это означает, в частности, возможность использовать анонимизированные или синтетические данные для увеличения разнообразия без нарушения принципа минимизации (van Bekkum, 2025, p. 7).

На этапе сбора данных статья 13 *GDPR* обязывает информировать субъектов персональных данных о ключевых параметрах обработки: целях использования данных, правовых основаниях, сроках хранения, получателях, а также о правах субъекта (право на доступ, исправление, удаление, ограничение обработки и др.)[121]. Это информационная основа прозрачности, без которой любая последующая работа с данными для обучения ИИ-модели будет юридически уязвимой.

Акт об ИИ дополняет эти требования концепцией практик управления данными[122]. В статье 10(2) Акта об ИИ провайдеру высокорисковой ИИ-системы вменяется в обязанность документировать происхождение данных[123], исходную цель их сбора, примененные методы очистки (*data cleaning*) и разметки (*data labelling / annotation*). В технической документации (приложение III к Акту об ИИ[124]) должны быть отражены используемые датасеты, процедуры подготовки и проверки, что позволяет контролирующим органам оценить как качество, так и правомерность подготовки обучающего массива.

Требование ст. 5(1)(c) *GDPR* о минимизации данных в контексте обучения ИИ-моделей означает обязанность оператора (*controller*) обосновать выбор каждого вида данных[125]. Оператор должен продемонстрировать, почему именно такой набор признаков необходим для достижения заявленной цели и что объем данных соотносится с критерием необходимости, а не с техническим удобством по принципу «чем больше, тем лучше».

С другой стороны, статья 10(3) Акта об ИИ вводит критерий репрезентативности и достоверности обучающих и валидационных данных (*representativeness and accuracy*): используемые наборы должны адекватно отражать целевую популяцию, исключать систематические ошибки и обеспечивать статистическую пригодность модели. Здесь проявляется различие в логике требований: репрезентативность предполагает широкий охват и разнообразие данных, а минимизация — их сокращение. Правовой подход позволяет согласовать эти требования: оператор фиксирует в документации (отчетах по результатам *DPIA;* технических отчетах по Акту об ИИ),

---

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

120 Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 57–58.

121 General Data Protection Regulation, 2016 O.J. (L 119) 40–41.

122 *Data governance practices* — практики управления качеством, происхождением и безопасностью данных.

123 То есть *"data provenance"* — источник и способ получения данных. См.: Artificial Intelligence Act, 2024 O.J. (L 2024/1689) 57.

124 Artificial Intelligence Act, 2024, annex III, O.J. (L 2024/1689) 127–129.

125 General Data Protection Regulation, 2016 O.J. (L 119) 35–36.

что объем данных минимален с точки зрения прав субъекта, но достаточен для статистической устойчивости и недискриминации. Баланс достигается, в частности, через исключение явно нерелевантных признаков; укрупнение и агрегирование чувствительных данных; использование анонимизации и синтетической генерации для расширения выборки без увеличения объема персональных данных (Laato et al., 2022, p. 4).

Сам процесс обучения моделей в праве ЕС рассматривается как непрерывная обработка персональных данных (*continuous processing*). Это означает, что на обучение целиком распространяются базовые принципы и права согласно *GDPR*: законность обработки *(lawfulness)* (ст. 6)[126]; целевое ограничение и минимизация *(purpose limitation u data minimisation)* (ст. 5)[127], обеспечение безопасности *(security of processing)* (ст. 32)[128], а также специальные правила профилирования и автоматизированного принятия решений *(profiling and automated decision-making)* (ст. 22)[129]. Если итоговая модель используется для принятия решений, затрагивающих права субъектов (например, отказ в кредите, приеме на работу, доступе к услуге), возникает дополнительная обязанность информировать о логике и последствиях обработки (ст. 13 и 22 *GDPR*)[130] и обеспечивать возможность человеческого вмешательства (*human intervention*).

Статья 9 Акта об ИИ дополняет эту конструкцию требованием к системному управлению рисками[131]. Оно должно носить постоянный, цикличный и документированный характер и охватывать весь жизненный цикл ИИ-системы: от проектирования и обучения до эксплуатации и пострыночного мониторинга. Особый акцент делается на рисках дискриминации и смещения данных. Уже на стадии проектирования и обучения провайдер обязан выявлять такие риски и принимать меры по их снижению[132].

С этой целью статья 11 Акта об ИИ[133] и приложение III к нему[134] закрепляют обязанность вести подробную техническую документацию, где фиксируются архитектура системы, используемые датасеты, критерии отбора данных, процессы очистки и проверки, протоколы тестирования, методы предотвращения предвзятости и результаты оценок. Такая документация частично пересекается по функциям с реестрами операций обработки по ст. 30 *GDPR*[135], что позволяет выстраивать единую систему комплаенса: одна часть записей ориентирована на надзор по линии защиты данных, другая — на контроль соответствия Акту об ИИ.

Принцип защиты данных по замыслу и по умолчанию (ст. 25 *GDPR*) требует от провайдера искусственного интеллекта внедрять технические и организационные меры еще на стадии обучения: шифрование (защиту данных криптографическими методами), псевдонимизацию (замену идентификаторов токенами), дифференциальную приватность (контролируемое

126 Ibid. at 36–37.

127 Ibid. at 35–36.

128 Ibid. at 51–52.

129 Ibid. at 46.

130 Ibid. at 40–41.

131 Artificial Intelligence Act, 2024, annex III, O.J. (L 2024/1689) 56–57.

132 Slattery, P., Saeri, A. K., Grundy, E. A. C., Graham, J., Noetel, M., Uuk, R., Dao, J., Pour, S., Casper, S., & Thompson, N. (2024). *The AI Risk Repository: A Comprehensive Meta-Review, Database, and Taxonomy of Risks from Artificial Intelligence.* https://doi.org/10.48550/arXiv.2408.12622

133 Artificial Intelligence Act, 2024, O.J. (L 2024/1689) 58.

134 Ibid. at 127–129.

135 General Data Protection Regulation, 2016 O.J. (L 119) 50–51.

внесение «шума», исключающего выделение человека в наборе данных), а также процедуры «машинного разучивания» (целенаправленное исключение определенных данных из обученной модели)[136]. Эти меры должны быть соразмерны риску и увязаны с требованиями статьи 32 *GDPR,* предписывающей учитывать состояние техники, стоимость внедрения, характер, объем и контекст обработки[137].

Акт об ИИ не вступает с этой логикой в противоречие, а усиливает ее: статья 10(2)(f), (g) прямо указывает на необходимость проверки обучающих данных на отсутствие незаконной предвзятости и несоответствующих смещений[138], а также на согласование таких проверок с принципами и пунктами преамбулы *GDPR,* включая п. 67 о прозрачности и поддержании актуальности данных[139].

Особое значение имеет статья 10(5) Акта об ИИ, допускающая использование специальных категорий данных (чувствительные данные о здоровье, биометрии, убеждениях и т. п.) для устранения смещений в обучении[140]. Формально это вступает в противоречие со статьей 9 *GDPR,* устанавливающей общий запрет на обработку таких данных[141]. Однако Акт об ИИ вводит конкретные условия в смысле статьи 10(5)(a), (b), (e): отсутствие менее инвазивной альтернативы, применение усиленных мер псевдонимизации и других методов защиты, удаление данных сразу после выполнения корректирующей задачи. С правовой точки зрения данную норму следует рассматривать как узкое исключение, которое допустимо только при одновременном выполнении условий ст. 9(2), (4) *GDPR*[142] и документальном обосновании в *DPIA* и технической документации. Это означает, что привлечение чувствительных признаков допустимо исключительно в режиме минимально необходимого вмешательства и под постоянным контролем регулятора и внутренних органов комплаенса.

Наконец, доказательства соблюдения указанных норм формируются в единой системе документации. *GDPR* требует ведения реестров операций обработки (ст. 30)[143], регистрации инцидентов и уведомлений (ст. 33–34)[144], *DPIA* и сопутствующих отчетов. Акт об ИИ предписывает хранить протоколы тестов, логи качества, отчеты об оценке рисков и техническое досье[145]. В совокупности эти документы составляют корпус доказательств законности и прозрачности обучения. На практике оправдан подход, при котором техническая документация по Акту об ИИ интегрируется с документами по *GDPR* (политиками обработки, *DPIA,* реестрами операций), образуя сквозную систему отчетности и повышая доверие к ИИ-системе со стороны регуляторов, партнеров и пользователей.

При валидации (тестировании) модели *GDPR* продолжает действовать в полном объеме. Если валидационные и тестовые наборы содержат персональные данные, их обработка должна опираться на правовое основание (согласие, договор, законный интерес и т. д.) и соответствовать принципам минимизации и целевого ограничения. На этой стадии особенно важна

136 General Data Protection Regulation, 2016 O.J. (L 119) 48.

137 Ibid. at 51–52.

138 Artificial Intelligence Act, 2024, O.J. (L 2024/1689) 57.

139 General Data Protection Regulation, 2016 O.J. (L 119) 13.

140 Artificial Intelligence Act, 2024, O.J. (L 2024/1689) 58.

141 General Data Protection Regulation, 2016 O.J. (L 119) 38–39.

142 Ibid.

143 Ibid. at 50–51.

144 Ibid. at 52–53.

145 Artificial Intelligence Act, 2024, annex III, O.J. (L 2024/1689) 127–129.

оценка рисков дискриминации: в соответствии со ст. 13(2)(f) *GDPR* контролер обязан заранее информировать субъектов о возможных последствиях автоматизированного прогнозирования и рисках для их прав и свобод[146].

Статья 10(2), (3) Акта об ИИ предписывает, чтобы валидационные наборы обладали теми же качественными характеристиками, что и обучающие: релевантностью (связь с задачей), репрезентативностью и способностью обеспечивать проверку точности и устойчивости модели[147]. Это означает, что тестирование должно быть спроектировано, чтобы выявлять смещения и ошибки, а результаты должны фиксироваться в отчетах и логах для целей надзора, аудита и подтверждения соответствия как Акту об ИИ, так и *GDPR*.

На этапе внедрения ИИ-модели в эксплуатацию юридические обязанности оператора и провайдера существенно ужесточаются. Если модель используется для принятия решений, затрагивающих права и законные интересы физических лиц, применяется статья 22 *GDPR* об автоматизированном принятии решений, предусматривающая право субъекта на вмешательство (пересмотр решения человеком), оспаривание решения и получение объяснений относительно логики обработки[148]. Эти требования корреспондируют со статьей 14 Акта об ИИ, закрепляющей принцип человеческого надзора (*human oversight*)[149], а также со статьей 13 *GDPR*, устанавливающей обязанность информировать о целях обработки, логике принятия решений и возможных последствиях для субъектов данных[150].

В этом контексте особое значение приобретает концепция так называемого пакета прозрачности[151]. Под ним в практике применения Акта об ИИ понимается передача по всей цепочке внедрения и эксплуатации исчерпывающего набора материалов: руководств пользователя, технического описания, отчетов о тестировании, ограничений применимости, условий корректного использования и сценариев, при которых система может создавать повышенные риски. Пункт 27 преамбулы к Акту об ИИ подчеркивает, что все лица, участвующие в проектировании, интеграции и эксплуатации системы, должны быть осведомлены о ее характеристиках, возможностях и рисках[152]. В свою очередь *GDPR* в ст. 12–14 дополняет это требованием прозрачности в отношении обработки персональных данных и доступности информации для субъектов, включая сведения об их правах, основаниях обработки и механизмах их реализации[153].

Мониторинг после внедрения (*post-market monitoring*) закреплен в обоих нормативных актах. Статьи 33–34 *GDPR* обязывают контролера сообщать о нарушениях безопасности персональных данных в надзорный орган и при необходимости информировать субъектов данных[154], а также обеспечивать реализацию права на стирание *(right to erasure)* (ст. 17 *GDPR*)[155]. Статьи 61–62 Акта об ИИ, в свою очередь, требуют от провайдера регистрировать серьезные инциденты, поддерживать систему пострыночного мониторинга и фиксировать результаты

146 General Data Protection Regulation, 2016 O.J. (L 119) 41.
147 Artificial Intelligence Act, 2024, O.J. (L 2024/1689) 57.
148 General Data Protection Regulation, 2016 O.J. (L 119) 46.
149 Artificial Intelligence Act, 2024, O.J. (L 2024/1689) 60–61.
150 General Data Protection Regulation, 2016 O.J. (L 119) 40–41.
151 *Transparency pack* — совокупность документов и сведений о системе.
152 Artificial Intelligence Act, 2024, O.J. (L 2024/1689) 8.
153 General Data Protection Regulation, 2016 O.J. (L 119) 39–41.
154 Ibid. at 52–53.
155 Ibid. at 43–44.

в технической документации[156]. Формируется правовая симметрия: обе системы регулирования исходят из обязанности постоянного контроля, регулярной корректировки и документированного подтверждения соответствия.

Отдельный проблемный блок связан с принципом целевого ограничения (*purpose limitation*). В соответствии со ст. 5(1)(b) *GDPR* персональные данные могут использоваться только для конкретных, заранее определенных и законных целей и не подлежат дальнейшей обработке способом, несовместимым с этими целями[157]. Логика коммерческого использования ИИ-моделей, напротив, предполагает расширение сфер применения: модель, изначально обученная для одной задачи (например, внутреннего риск-анализа), впоследствии адаптируется для иных функций или встраивается в новые бизнес-процессы. Такое расширение цели[158] очевидно противоречит конструкции целевого ограничения.

Для частичного разрешения этой коллизии европейское право предусматривает специальный режим исследовательской дерогации (*research derogation*). Статья 89 *GDPR* допускает использование персональных данных в научных и исследовательских целях при условии дополнительных гарантий: псевдонимизации, ограничения доступа, строгого документирования исследовательских целей и процедур[159]. Пункт 159 преамбулы к *GDPR* прямо относит обучение и тестирование алгоритмов к сфере научного и технологического развития, при этом подчеркивая, что такой режим допустим, пока результаты не используются в отношении конкретных субъектов в контексте оказания услуг или принятия решений[160]. На этой стадии первична именно исследовательская цель, а не коммерческая эксплуатация.

Статья 2 Акта об ИИ ограничивает сферу действия регламента системами, которые размещаются на рынке или вводятся в эксплуатацию (*placing on the market / putting into service*)[161]. Соответственно, сугубо исследовательский этап разработки и внутреннего тестирования ИИ-моделей, когда система не предлагается на рынке и не используется для принятия решений в отношении внешних пользователей, напрямую не подпадает под действие Акта об ИИ и регулируется исключительно *GDPR*. На этом этапе применим режим исследовательской дерогации, несколько смягчающий требования при условии строгих дополнительных гарантий (ограничение доступа, псевдонимизация, минимизация и т.д.).

Ситуация принципиально меняется в момент вывода модели на рынок[162] или ее ввода в эксплуатацию во внешнем контуре. С этого момента для разработчика/провайдера возникает комплекс новых обязательств.

Во-первых, необходимо пересмотреть правовое основание обработки данных в соответствии со ст. 6 *GDPR*[163]. Если на исследовательском этапе обработка опиралась на исключение для научных целей *(research basis)* (в сочетании со ст. 89 *GDPR*)[164], то при коммерческом использовании требуется иное основание: согласие субъекта *(consent)* (ст. 6(1)(a)), необходимость

---

156 Artificial Intelligence Act, 2024, O.J. (L 2024/1689) 94–95. См. также соответствующие приложения к Акту: Ibid., annexes IV, V, O.J. (L 2024/1689) 130–132.

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

158 *Purpose creep* — постепенный выход за исходные цели обработки.

159 Ibid. at 84–85.

160 Ibid. at 30.

161 Ibid. at 45–46.

162 Имеется ввиду первое предоставление системы на рынке ЕС (*"placing on the market"*).

163 *Intended purpose* — запроектированная область и условия использования ИИ-системы.

164 Ibid. at 36–37.

обработки для исполнения договора с субъектом данных (или принятия мер до заключения договора по его запросу) *(performance of a contract)* (ст. 6(1)(b))[165], выполнение юридической обязанности, публичный интерес или законный интерес оператора *(legitimate interests)* (ст. 6(1)(f)) при выполнении теста баланса интересов[166].

Во-вторых, в силу ст. 27 Акта об ИИ и приложения IV к нему разработчик/провайдер обязан обновить описание целей эксплуатации, областей применения и ограничений системы и зафиксировать их в нормативной и технической документации[167]. Эти сведения становятся частью паспорта ИИ-системы, ее технической документации, которая должна включать описание предназначенной цели, целевой среды, категорий пользователей, ограничений и ключевых рисков.

В-третьих, обязательной становится повторная оценка воздействия на защиту данных (обновленная *DPIA* по ст. 35 *GDPR*)[168]. Переход от исследовательского режима к коммерческой эксплуатации изменяет характер обработки, масштаб воздействия и зачастую категории субъектов. Контролер обязан пересмотреть перечень рисков, обновить перечень мер защиты и зафиксировать измененный уровень остаточного риска.

В-четвертых, при наличии серьезных рисков для фундаментальных прав и свобод (по Хартии ЕС об основных правах[169]) возникает необходимость проведения отдельной оценки воздействия на основные права *(FRIA).* Она проводится как дополнение к *DPIA* применительно к высокорисковым ИИ-системам, подпадающим под приложение III к *AI Act (*Mantelero, 2024, p. 17; Malgieri & Santos, 2025, p. 69).

В результате формируется двухступенчатая модель регулирования обучения и использования ИИ-моделей. На стадии разработки и внутреннего тестирования действует исследовательский режим согласно *GDPR* (п. 159 преамбулы и ст. 89)[170], допускающий дерогацию при условии дополнительных гарантий и отсутствия внешнего воздействия на субъектов. С момента вывода продукта на рынок или ввода в эксплуатацию активируется полный комплекс обязательств одновременно по *GDPR* и Акту об ИИ. Фактический момент вывода системы на рынок становится юридической точкой отсчета смены режима: именно с этого времени разработчик обязан пересмотреть правовые основания обработки, обновить техническую и правовую документацию, встроить систему пострыночного мониторинга, усилить меры защиты данных и прав субъектов и при необходимости провести как *DPIA,* так и *FRIA.*

Заключение

Проведенный анализ позволяет утверждать, что этап обучения ИИ-моделей выступает не только технологически, но и юридически значимой фазой жизненного цикла ИИ-систем. Именно на этой стадии концентрируются ключевые обязанности по *GDPR* и Акту об ИИ, связанные с выбором цели и правового основания обработки, управлением качеством и репрезентативностью данных, минимизацией и оценкой рисков для фундаментальных прав. Специфика обучающего этапа проявляется в сочетании масштабной обработки данных, статистического обобщения и высоких рисков профилирования, дискриминации и снижения прозрачности.

[165] Ibid. at 36.

[166] Ibid. at 84–85.

[167] Artificial Intelligence Act, 2024, O.J. (L 2024/1689) 69–70, 130–131.

[168] General Data Protection Regulation, 2016 O.J. (L 119) 53–54.

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

[170] General Data Protection Regulation, 2016 O.J. (L 119) 30, 84–85.

Одновременно отсутствие унифицированных методических разъяснений на уровне институтов ЕС (Европейской комиссии, Европейского управления по искусственному интеллекту, надзорных органов по защите данных) обусловливает правоприменительную неопределенность и расхождение в национальных подходах.

С учетом выявленных противоречий и разнонаправленных регуляторных векторов предлагается прикладная модель поведения разработчиков и операторов, построенная по логике «*R&D* → *Market*» («от исследовательской стадии к стадии рыночного внедрения»). Суть модели состоит в том, что обучение рассматривается как самостоятельный юридически значимый процесс в рамках общего жизненного цикла ИИ-системы, для которого устанавливается порог перехода от исследовательской дерогации по ст. 89 *GDPR* к полному режиму Акта об ИИ. Такая конструкция не претендует на единственно возможное решение: в доктрине обсуждаются и более жесткие подходы, исходящие из необходимости изначально применять к обучающим процедурам весь комплекс требований Акта об ИИ, и, напротив, более мягкие позиции, фактически сводящие регулирование обучения к общим нормам о научной обработке данных. Предлагаемая модель занимает промежуточную позицию, увязывая момент вывода системы на рынок с усилением регуляторного режима и формализацией обязанностей по обоим актам.

В рамках данной модели разработчик (или связка «разработчик — провайдер») выстраивает документационную и организационную структуру, включающую определение и фиксацию цели обработки и правового основания (ст. 5, 6 *GDPR*); правовую и техническую экспертизу обучающих выборок (*data governance* в смысле ст. 10 Акта об ИИ); предпочтительное использование анонимизированных, агрегированных и синтетических данных там, где это допустимо без ущерба для статистического качества; проведение оценки воздействия на защиту данных (*DPIA*) в случаях высокого риска (ст. 35 *GDPR*); ведение внутренней отчетности и журналов операций; соблюдение требований прослеживаемости, устойчивости и подотчетности, закрепленных в Акте об ИИ, включая техническую документацию и протоколы тестирования. С практической точки зрения эта модель превращает набор разрозненных обязанностей в последовательную дорожную карту для корпоративного комплаенса, но одновременно повышает нагрузку на субъекты, лишенные зрелых процедур управления рисками, что уже сегодня является предметом критики со стороны представителей малого и среднего бизнеса.

Значение модели «*R&D* → *Market*» состоит в том, что она предлагает операционализированную схему согласованного применения двух параллельных режимов: горизонтальных требований *GDPR* к обработке персональных данных и вертикальных требований Акта об ИИ к высокорисковым ИИ-системам. При надлежащей имплементации такая схема позволяет не только формально соблюдать ст. 5, 6, 9, 25, 30, 35 *GDPR* и ст. 10, 11, 69 Акта об ИИ, но и выстраивать доказуемую линию поведения на случай регуляторного запроса или судебного спора. Вместе с тем остается открытым вопрос о стандартизации подобных моделей: пока речь идет о доктринальной конструкции, а не о закрепленном регулятором эталоне, от компаний требуется самостоятельная адаптация предложенного подхода к отраслевым и национальным особенностям.

Отдельным элементом предлагаемой модели выступает тест невозможности альтернативы при работе со специальными категориями данных, используемыми для устранения смещений в обучении (ст. 10(5) Акта об ИИ в сочетании со ст. 9 *GDPR*). Содержание теста сводится к необходимости документально обосновать, что привлечение чувствительных признаков (например, этнической принадлежности или состояния здоровья) является единственно необходимым и пропорциональным способом достижения заявленной исследовательской или эксплуатационной

цели и что сопоставимого уровня недискриминации или точности нельзя достичь путем использования синтетических, анонимизированных или менее инвазивных данных. Такой подход отражает более рестриктивное прочтение ст. 10(5) Акта об ИИ, ограничивающее сферу применения исключения, и тем самым снижает риск признания обработки несоразмерной при проверке надзорным органом или судом.

В совокупности результаты исследования позволяют квалифицировать обучение ИИ-модели как юридически значимый этап, от качества правового сопровождения которого зависит соответствие всей ИИ-системы требованиям *GDPR* и Акта об ИИ. Вместе с тем предложенная модель носит характер концептуального предложения и должна рассматриваться как основа для дальнейшей доктринальной дискуссии и последующей регуляторной конкретизации, прежде всего через разъяснения Европейской комиссии, Европейского управления по искусственному интеллекту и Европейского совета по защите данных.

Список литературы / References

1. Arasteh, S. T., Ziller, A., Kuhl, C., Makowski, M. R., Nebelung, S., Braren, R. F., Rueckert, D., Truhn, D., & Kaissis, G. (2024). Preserving fairness and diagnostic accuracy in private large-scale AI models for medical imaging. *Communications Medicine*, (4), Article 46 (2024). https://doi.org/10.1038/s43856-024-00462-6
2. Basdekis, I., Kloukinas, C., Agostinho, C., Vezakis, I., Pimenta, A., Gallo, L., & Spanoudakis, G. (2023). Pseudonymisation in the context of GDPR-compliant medical research. In 2023 *19th International Conference on the Design of Reliable Communication Networks (DRCN)* (pp. 1–6). IEEE. https://doi.org/10.1109/DRCN57075.2023.10108370
3. De Hert, P., & Hajduk, P. (2024). EU cross-regime enforcement, redundancy and interdependence: Addressing overlap of enforcement structures in the digital sphere after Meta. *Technology and Regulation*, *2024*, 291–308. https://doi.org/10.71265/fydwsg59
4. De Silva, D., & Alahakoon, D. (2022). An artificial intelligence life cycle: From conception to production. *Patterns*, *3*(6), Article 100489. https://doi.org/10.1016/j.patter.2022.100489
5. Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In S. Halevi & T. Rabin (Eds.), *Lecture notes in computer science, Vol. 3876. Theory of cryptography* (pp. 265–284). Springer. https://doi.org/10.1007/11681878_14
6. Finck, M., & Biega, A. (2021). Reviving purpose limitation and data minimisation in data-driven systems. *Technology and Regulation, 2021,* 44–61. https://doi.org/10.26116/techreg.2021.004
7. Hadwick, D. (2024). Slipping through the cracks, the carve-outs for AI tax enforcement systems in the EU AI Act. *European Papers: A Journal on Law and Integration*, *9*(3), 936–955. https://doi.org/10.15166/2499-8249/793
8. Haripriya, R., Khare, N., & Pandey, M. (2025). Privacy-preserving federated learning for collaborative medical data mining in multi-institutional settings. *Scientific Reports*, (15), Article 12482 (2025). https://doi.org/10.1038/s41598-025-97565-4
9. Kaminski, M. E., & Malgieri, G. (2025). Impacted stakeholder participation in AI and data governance. *Yale Journal of Law & Technology*, *27*(1), 247–326.
10. Kindt, E. J. (2025). EU biometric data regulation: Part 2: The AI Act. *IEEE Biometrics Council Newsletter*, *54*, 30–41.
11. Laato, S., Birkstedt, T., Mäntymäki, M., Minkkinen, M., & Mikkonen, T. (2022). AI governance in the system development life cycle: Insights on responsible machine learning engineering. In *Proceedings of the 1st*

International Conference on AI Engineering: Software Engineering for AI (pp. 113–123). ACM. https://doi.org/10.1145/3522664.3528598

12. Liu, W., Zhang, Y., Yang, H., & Meng, Q. (2024). A survey on differential privacy for medical data analysis. *Annals of Data Science*, *11*, 733–747. https://doi.org/10.1007/s40745-023-00475-3
13. Malgieri, G., & Santos, C. (2025). Assessing the (severity of) impacts on fundamental rights. *Computer Law & Security Review*, *56*, Article 106113. https://doi.org/10.1016/j.clsr.2025.106113
14. Mantelero, A. (2024). The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template. *Computer Law & Security Review*, *54*, Article 106020. https://doi.org/10.1016/j.clsr.2024.106020
15. Menges, F., Latzo, T., Vielberth, M., Sobola, S., Pöhls, H. C., Taubmann, B., Köstler, J., Puchta, A., Freiling, F., Reiser, H. P., & Pernul, G. (2021). Towards GDPR-compliant data processing in modern SIEM systems. *Computers & Security*, *103*, Article 102165. https://doi.org/10.1016/j.cose.2020.102165
16. Novelli, C., Casolari, F., Hacker, P., Spedicato, G., & Floridi, L. (2024a). Generative AI in EU Law: Liability, privacy, intellectual property, and cybersecurity. *Computer Law & Security Review*, *55*, Article 106066. https://doi.org/10.1016/j.clsr.2024.106066
17. Novelli, C., Casolari, F., Rotolo, A., Taddeo, M., & Floridi, L. (2024b). AI risk assessment: A scenario-based, proportional methodology for the AI Act. *Digital Society*, *3*, Article 13. https://doi.org/10.1007/s44206-024-00095-1
18. Paullada, A., Raji, I. D., Bender, E. M., Denton, E., & Hanna, A. (2021). Data and its (dis)contents: A survey of dataset development and use in machine learning research. *Patterns*, *2*(11), Article 100336. https://doi.org/10.1016/j.patter.2021.100336
19. Rocks, J. W., & Mehta, P. (2022). Memorizing without overfitting: Bias, variance, and interpolation in over-parameterized models. *Physical Review Research*, *4*(1), Article 013201. https://doi.org/10.1103/PhysRevResearch.4.013201
20. Slijepčević, D., Henzl, M., Klausner, L. D., Dam, T., Kieseberg, P., & Zeppelzauer, M. (2021). *k*-Anonymity in practice: How generalisation and suppression affect machine learning classifiers. *Computers & Security*, *111*, Article 102488. https://doi.org/10.1016/j.cose.2021.102488
21. Sovrano, F., Hine, E., & Anzolut, S. (2025). Simplifying software compliance: AI technologies in drafting technical documentation for the AI Act. *Empirical Software Engineering*, *30*, Article 91. https://doi.org/10.1007/s10664-025-10645-x
22. Söderlund, K., & Larsson, S. (2024). Enforcement Design Patterns in EU Law: An Analysis of the AI Act. *Digital Society*, *3*, Article 41. https://doi.org/10.1007/s44206-024-00129-8
23. Van Bekkum, M. (2025). Using sensitive data to de-bias AI systems: Article 10(5) of the EU AI Act. *Computer Law & Security Review*, *56*, Article 106115. https://doi.org/10.1016/j.clsr.2025.106115
24. Van Bekkum, M., & Zuiderveen Borgesius, F. (2023). Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception? *Computer Law & Security Review*, *48*, Article 105770. https://doi.org/10.1016/j.clsr.2022.105770
25. Veltmeijer, E., & Gerritsen, C. (2025). Legal and ethical implications of AI-based crowd analysis: The AI Act and beyond. *AI and Ethics*, *5*, 3173–3183. https://doi.org/10.1007/s43681-024-00644-x
26. Wang, L., Liu, Z., Liu, A., & Tao, F. (2021). Artificial intelligence in product lifecycle management. *The International Journal of Advanced Manufacturing Technology*, *114*, 771–796. https://doi.org/10.1007/s00170-021-06882-1
27. Winau, M. (2023). On the lack of substantive balancing and coordinated legal concretisation in the European Commission's proposal for a regulation on AI. *European Data Protection Law Review*, *9*(2), 123–135. https://doi.org/10.21552/edpl/2023/2/7

Сведения об авторе:

Олифиренко А. А. — магистрант, кафедра информационного права и цифровых технологий, Саратовская государственная юридическая академия; магистрант, кафедра «Информационная безопасность автоматизированных систем», Институт электронной техники и приборостроения, Саратовский государственный технический университет имени Ю. А. Гагарина, Саратов, Россия; специалист по защите данных, ответственный за безопасность ИИ-систем, ООО «Экосистема недвижимости "Метр квадратный"», Москва, Россия.
panolifer@gmail.com
ORCID: https://orcid.org/0000-0002-2186-281X

Information about the author:

Artem A. Olifirenko — Master's student, Department of Information Law and Digital Technologies, Saratov State Law Academy; Master's student, Department of Information Security of Automated Systems, Institute of Electronic Engineering and Instrumentation, Yuri Gagarin State Technical University of Saratov, Saratov, Russia; Data Protection Specialist, responsible for AI governance and security, "Ecosystem Real Estate 'Metr Kvadratny'" LLC, Moscow, Russia.
panolifer@gmail.com
ORCID: https://orcid.org/0000-0002-2186-281X

https://doi.org/10.38044/2686-9136-2025-6-14

СТАТЬИ

ЦИФРОВИЗАЦИЯ СУДЕБНОГО ПРОЦЕССА: ОПЫТ ИНТЕГРАЦИОННЫХ ОБЪЕДИНЕНИЙ

М. В. Тучина

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

Аннотация

Статья посвящена исследованию цифровой трансформации судебных процессов в интеграционных объединениях: Европейском союзе (ЕС), Евразийском экономическом союзе (ЕАЭС), Общем рынке стран Южного конуса (МЕРКОСУР) и Ассоциации государств Юго-Восточной Азии (АСЕАН). Актуальность исследования обусловлена тем, что эффективная цифровизация правосудия становится ключевым условием функционирования интеграционных судебных механизмов: трансграничные споры требуют унифицированных электронных процедур, а различия в цифровой зрелости государств-членов препятствуют доступу к правосудию и тормозят развитие общего правового пространства. Цель исследования — выявить институциональные решения, технические инструменты и ограничения, характерные для цифровизации судебных процессов в интеграционных объединениях. Методы исследования включают сравнительно-правовой подход, институциональный анализ, а также изучение нормативных актов, стратегических документов и научных публикаций, посвященных цифровому правосудию в период 2010–2024 гг. Результаты исследования показывают разноуровневую цифровую зрелость интеграционных объединений. В ЕС внедрены единая электронная система *e-Curia,* портал *e-Justice,* цифровое взаимодействие с национальными судами; основные ограничения: неодинаковость технических стандартов государств-членов и сложность модернизации судебной инфраструктуры. В ЕАЭС реализованы электронная подача обращений в Суд ЕАЭС, цифровые публикации решений, пилотное использование видеоконференций; препятствия: отсутствие единой цифровой платформы Союза и низкая совместимость национальных ИТ-систем. В МЕРКОСУР наблюдается фрагментарная цифровизация (электронный документооборот и дистанционные заседания арбитражных органов), но отсутствуют единые цифровые регламенты и интеграция с национальными системами правосудия. В АСЕАН цифровизация развивается только в рамках национальных инициатив, поскольку объединение не располагает собственным судебным органом; ключевое ограничение — невозможность унификации процедур в силу межправительственного характера ассоциации. В работе автором сделан вывод, что цифровизация способна повысить прозрачность, ускорить судебные процедуры и улучшить трансграничный доступ к правосудию, однако критическими барьерами остаются несогласованность правовых режимов, отсутствие общих технических стандартов и инфраструктурная асимметрия государств-членов.

Ключевые слова

цифровизация правосудия, электронное судопроизводство, интеграционные объединения, ЕС, ЕАЭС, МЕРКОСУР, АСЕАН, цифровые судебные процессы

Конфликт интересов Автор сообщает об отсутствии конфликта интересов.

Финансирование Исследование не имеет спонсорской поддержки.

Для цитирования Тучина, М. В. Цифровизация судебного процесса: опыт интеграционных объединений. *Цифровое право, 6*(3), 125–148. https://doi.org/10.38044/2686-9136-2025-6-14

Поступила: 12.07.2025, принята в печать: 23.08.2025, опубликована: 30.09.2025

ARTICLES

DIGITALIZATION OF JUDICIAL PROCEEDINGS: THE EXPERIENCE OF REGIONAL INTEGRATION ORGANIZATIONS

Maria V. Tuchina

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

Abstract

The article examines the digital transformation of judicial processes within the following integration organizations: the European Union (EU), the Eurasian Economic Union (EAEU), the Southern Common Market (MERCOSUR), and the Association of Southeast Asian Nations (ASEAN). The relevance of the study stems from the fact that effective digitalization of justice has become a key prerequisite for the functioning of integration-based judicial mechanisms. Thus, cross-border disputes require unified electronic procedures, while disparities in the digital maturity of member states hinder access to justice and slow the development of a common legal space. The aim was to identify the institutional solutions, technological tools, and constraints characteristic of the digitalization of judicial processes in integration organizations. The methodological framework included a comparative legal approach, institutional analysis, as well as the examination of legal acts, strategic documents, and academic publications on digital justice issued between 2010 and 2024. The study revealed varying levels of digital maturity across the integration organizations in question. In the EU, the following elements have been implemented: the e-Curia unified electronic system, the e-Justice portal, and digital interaction with national courts. The main limitations include inconsistent technological standards among member states and the complexity of modernizing judicial infrastructure. In the EAEU, the following components have been implemented: electronic submission of applications to the EAEU Court, digital publication of its decisions, and pilot use of videoconferencing. The key obstacles are the absence of a unified digital platform for the Union and low interoperability among national IT systems. In MERCOSUR, digitalization is fragmented (electronic document management and remote hearings of arbitration bodies), yet there are no unified digital regulations or integration with national justice systems. In ASEAN, digitalization progresses exclusively within national initiatives, since the organization does not possess its own judicial body. Here, the main constraint is the impossibility of procedural harmonization due to the intergovernmental nature of ASEAN. The study concludes that digitalization can enhance transparency, accelerate judicial procedures, and improve cross-border access to justice. However,

critical barriers persist, including inconsistent legal frameworks, the lack of common technological standards, and infrastructural asymmetry among member states.

Keywords

digitalization of justice, electronic litigation, integration organizations, European Union, Eurasian Economic Union, MERCOSUR, ASEAN

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Tuchina, M. V. Digitalization of judicial proceedings: The experience of regional integration organizations. *Digital Law Journal, 6*(3), 125–148. https://doi.org/10.38044/2686-9136-2025-6-14

Submitted: 12 Jul. 2025, accepted: 23 Aug. 2025, published: 30 Sep. 2025

Введение

В последнее десятилетие судебные системы не только государств, но и судебные органы интеграционных объединений переживают этап цифровой трансформации, стремясь повысить эффективность судопроизводства и доступ к правосудию за счет внедрения современных информационных технологий[1]. Цифровизация правосудия охватывает внедрение электронного документооборота, онлайн-порталов подачи исков, систем видео-конференц-связи для проведения дистанционных судебных заседаний, электронных баз данных судебных решений и иных технических решений, призванных облегчить взаимодействие участников процесса с судом (Onţanu, 2023, pp. 97–104; Fabri, 2024, pp. 2–10). Пандемия *COVID-19* придала мощный импульс этим реформам, вынудив суды срочно осваивать формат дистанционных заседаний и электронного обмена документами[2]. Одновременно цифровизация влечет за собой новые вызовы: необходимо обеспечить соблюдение принципов справедливого судебного разбирательства, защиты данных и процессуальных прав в условиях перехода от бумажного к электронному судопроизводству (Reiling & Contini, 2022, pp. 2–10).

Особый интерес представляет анализ судебных механизмов интеграционных объединений, понимаемых в широком смысле как устойчивые формы регионального сотрудничества. К ним относятся как объединения с развитым наднациональным элементом, такие как Европейский союз (ЕС) и Евразийский экономический союз (ЕАЭС), так и объединения, действующие преимущественно в рамках межправительственного управления, например Общий рынок стран Южного конуса (МЕРКОСУР) и Ассоциация государств Юго-Восточной Азии (АСЕАН). Эти организации находятся на разных стадиях интеграционного развития и обладают различными моделями разрешения споров. ЕС располагает разветвленной судебной системой во главе с Судом Европейского союза, решения которого обязательны для государств-членов, тогда как в МЕРКОСУР применяется арбитражно-судебный механизм *ad hoc* трибуналов и Постоянного ревизионного трибунала с ограниченной юрисдикцией. ЕАЭС как более молодое объединение находится в процессе институционального становления и формирует собственный наднациональный судебный

[1] Программа развития Организации Объединённых Наций. (2022). *Цифровая стратегия на 2022–2025 годы.* https://digitalstrategy.undp.org/documents/Digital-Strategy-2022-2025-Full-Document_RU_Interactive.pdf

[2] Там же.

орган — Суд ЕАЭС, а в АСЕАН отсутствует постоянно действующая судебная инстанция и урегулирование споров осуществляется преимущественно через консультации и посредничество. Существенные различия в объеме переданных полномочий и степени институционализации требуют ясно обозначить критерии сравнения: ЕС и ЕАЭС демонстрируют модель интеграции с элементами наднациональности, тогда как МЕРКОСУР и АСЕАН представляют более гибкие и менее формализованные варианты координации. Тем не менее опыт всех указанных объединений остается значимым для исследования региональных практик разрешения споров, позволяя выявлять широкий спектр судебных и квазисудебных подходов, применяемых в различных типах интеграционных объединений.

Актуальность исследования обусловлена тем, что цифровизация судопроизводства способна существенно увеличить эффективность региональных механизмов правосудия, ускорив рассмотрение споров между государствами и участниками интеграции, повысив прозрачность и предсказуемость решений наднациональных судов. И, как следствие, возрастет активность интеграционной группировки в целом. В то же время недостаточная проработка правовых аспектов и несовместимость технологий способны тормозить внедрение электронного правосудия. Сравнительный анализ опыта интеграционных группировок позволяет выявить лучшие практики и типичные проблемы на этом пути.

В литературе тема электронного правосудия в региональных объединениях получила развитие в отдельных работах. Так, в отношении ЕС подробно исследованы платформы электронного правосудия (например, система *e-Curia* для электронного обмена документами с Судом ЕС) и их влияние на принцип справедливого отправления правосудия (Reiling & Contini, 2022, pp. 6–7). С 2018 г. использование *e-Curia* стало обязательным при обращении в Суд общей юрисдикции, что демонстрирует высокую степень институционализации электронного документооборота[3]. В отношении ЕАЭС Т. Михалёва и Г. Василевич подчеркнули, что «цифровое правосудие должно стать важным элементом политики евразийской интеграции: создание электронных кабинетов сторон в Судебной системе ЕАЭС, использование электронной подписи и цифрового обмена документами способны сделать наднациональное правосудие более доступным и повысить доверие граждан к интеграции» (Mikhaliova & Vasilevich, 2023, p. 191). Отмечается необходимость гармонизации подходов к онлайн-разрешению споров в трансграничном контексте ЕАЭС и создания оптимальной онлайн-платформы для урегулирования споров под эгидой Евразийской экономической комиссии. В МЕРКОСУР академические и экспертные работы посвящены в основном анализу механизмов электронного разрешения споров и внедрению электронного правосудия в государствах Латинской Америки (Szlak, 2012, p. 553). В АСЕАН больше внимание в литературе уделяется исследованию влияния цифровой трансформации на экономическую интеграцию самой группировки (Le, 2025, p. 1).

Отдельного внимания заслуживают ключевые работы отечественных исследователей, в которых суды интеграционных объединений рассматриваются как самостоятельная группа международных судебных органов, обладающая особыми чертами правовой природы, компетенциями и механизмами воздействия на интеграционные процессы. В трудах Л. П. Ануфриевой и В. Л. Толстых последовательно анализируется институциональная эволюция международных судов, включая суды интеграционных объединений, с акцентом на их место в системе международного правосудия и соотношение с классическими межгосударственными судебными органами (Anufriyeva & Tolstykh, 2014). Значительный вклад в разработку теоретических

[3] Decision of the General Court of 11 July 2018 on the lodging and service of procedural documents by means of e-Curia, 2018 O.J. (L 240) 72.

оснований функционирования судов интеграционных объединений внес А. С. Исполинов. Он обосновывает тезис о том, что суды интеграционных объединений выходят за рамки классической модели международного правосудия, сочетая в себе элементы международного и наднационального правосудия (Ispolinov, 2018). Работы Р. А. Каламкаряна посвящены вопросам юрисдикции международных судов, их легитимности и взаимодействию с национальным суверенитетом (Kalamkaryan, 2011, 2012). В исследованиях Т. Н. Нешатаевой анализируется роль наднациональных судебных органов на примере Суда ЕАЭС, а также влияние судебных решений на формирование интеграционного правопорядка (Neshatayeva, 2017, 2021). Существенный вклад в изучение судебного измерения интеграции внесли работы А. С. Смбатян, в которых обосновывается роль судов интеграционных объединений не только как органов разрешения споров, но и как факторов интеграционного строительства (Smbatyan, 2012). Ранние, но концептуально значимые труды Г. Г. Шинкарецкой и М. Л. Энтина заложили основы отечественного анализа судебных и квазисудебных интеграционных органов, включая проблемы соотношения международного и интеграционного права, а также роль судебных органов в обеспечении эффективности интеграции (Shinkaretskaya, 1992; Entin 1984, 1987). Современные работы В. Л. Толстых и К. В. Энтина развивают эти подходы, уделяя внимание актуальным тенденциям интеграционного судебного строительства (Entin, 2020; Tolstykh, 2015, 2023).

Таким образом, отечественная доктрина сформировала разносторонний и методологически устойчивый подход к исследованию судов региональных интеграционных объединений, что позволяет рассматривать их не только как вспомогательные механизмы разрешения споров, но и как самостоятельные институты, оказывающие существенное влияние на развитие интеграционного правопорядка.

В то же время сравнительных работ, охватывающих одновременно ЕС, ЕАЭС, МЕРКОСУР и АСЕАН, недостаточно. Настоящее исследование стремится восполнить этот пробел, сопоставляя правовые и технологические аспекты цифровизации судебных процессов в указанных интеграционных объединениях. Гипотеза исследования состоит в том, что более глубокая степень интеграции (при которой страны объединения делегируют наднациональным органам часть государственного суверенитета (Aleksandrov & Butorina, 2016, p. 17) коррелирует с более продвинутым внедрением электронного правосудия, тогда как менее продвинутые объединения (со слаборазвитым наднациональным механизмом разрешения споров, такие как МЕРКОСУР, АСЕАН) отстают в цифровой трансформации судебных процессов. Для проверки этой гипотезы в разделе «Результаты» представлена характеристика механизмов электронного правосудия в ЕС, ЕАЭС, МЕРКОСУР и АСЕАН. В разделе «Дискуссия» сравниваются эффекты цифровизации (доступность, прозрачность, скорость, защита прав) и формулируются рекомендации. Заключение содержит синтез ключевых выводов и перспективные направления дальнейших исследований.

Результаты

Европейский союз: правовые основы и технологии электронного правосудия

Правовые аспекты

Европейский союз является наиболее продвинутым интеграционным объединением в сфере цифровизации правосудия. Наднациональная судебная система ЕС — Суд Европейского союза (включает Суд и Суд общей юрисдикции) — активно внедряет электронные способы коммуникации с участниками процесса. Правовую базу составляют как акты Суда ЕС

(Процессуальный регламент Суда ЕС, закрепляющий нормы по электронной подаче документов[4]), так и инициативы институтов ЕС. В частности, Европейская комиссия в декабре 2020 г. приняла сообщение «Цифровизация правосудия в Европейском союзе: инструментарий возможностей»[5], в котором предложен набор инструментов для перехода судов в цифровой формат. Одновременно была подготовлена поправка в регламенты ЕС о судебном сотрудничестве, предусматривающая обязательное использование цифровой коммуникационной системы для трансграничных гражданских и уголовных процедур[6]. Совет ЕС также утвердил заключения, призывающие разработать всеобъемлющую стратегию цифровизации правосудия в Европе[7]. На уровне всего ЕС функционирует Европейский портал электронного правосудия (*European e-Justice Portal*) — веб-ресурс, предоставляющий доступ к правовой информации и сервисам[8]. Кроме того, принят Регламент (ЕС) 2022/850, устанавливающий правовые условия для использования системы *e-CODEX* — общей для ЕС децентрализованной инфраструктуры обмена судебными документами между государствами-членами[9]. Помимо этого, за последние 12 месяцев Европейская комиссия актуализировала ключевые документы по цифровой трансформации ЕС в различных областях[10]. Отдельные акты, хотя и косвенно, также затрагивают

4 Rules of Procedure of the Court of Justice, 2012 O.J. (L 265) 1; Amendments to the Rules of Procedure of the Court of Justice, 2018 O.J. (L 173) (July 3); Amendments to the Rules of Procedure of the Court of Justice, 2020 O.J. (L 380) (Oct. 31).

5 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Digitalisation of justice in the European Union — A toolbox of opportunities*, COM (2020) 710 final (Dec. 2, 2020), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:710:FIN

6 Regulation 2023/2844, of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation, 2023 O.J. (L 2023/2844) (EU), https://eur-lex.europa.eu/eli/reg/2023/2844/oj

7 Council of the European Union, Council Conclusions: *Access to Justice — Seizing the Opportunities of Digitalisation*, ST-11599/2020 INIT (Oct. 8, 2020), https://data.consilium.europa.eu/doc/document/ST-11599-2020-INIT/en/pdf

8 Согласно п. 3.4 сообщения Европейской комиссии «Цифровизация правосудия в Европейском союзе: инструментарий возможностей» «граждане, государственные органы и компании уже получают выгоду от цифровых инструментов, которые повышают прозрачность, облегчают доступ к доказательствам в уголовных производствах и сокращают задержки и ненужные административные издержки. Так, портал e-Justice является основным источником правовой и практической информации в сфере правосудия в ЕС для широкой общественности. Он также обеспечивает доступ к взаимосвязанным реестрам, в частности через систему межгосударственных торговых реестров (Business Registers Interconnection System, BRIS), которая объединяет торговые реестры государств-членов и стран Европейской ассоциации свободной торговли (European Free Trade Association, EACT), предоставляет публичный доступ к информации более чем о 20 млн обществ с ограниченной ответственностью по всей Европе и позволяет торговым реестрам обмениваться информацией по трансграничным делам» (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Digitalisation of justice in the European Union — A toolbox of opportunities*, COM (2020) 710 final (Dec. 2, 2020), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:710:FIN).

9 Regulation 2022/850, of the European Parliament and of the Council of 30 May 2022 on a computerised system for communication in cross-border civil and criminal proceedings (e-CODEX system), and amending Regulation 2018/1726, 2022 O.J. (L 150) 1 (EU), https://eur-lex.europa.eu/eli/reg/2022/850/oj

10 Regulation 2025/327, of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation 2024/2847, 2025 O.J. (L 2025/327) (EU), https://eur-lex.europa.eu/eli/reg/2025/327/oj; Regulation 2024/2847, of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations 168/2013 and 2019/1020 and Directive 2020/1828 (Cyber Resilience Act), 2024 O.J. (L 2024/2847) (EU), https://eur-lex.europa.eu/eli/reg/2024/2847/oj; Communication from the Commission, *State of Digital Decade 2025: Keep Building the EU's Sovereignty and Digital Future* (June 16, 2025), https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package

вопросы судебной системы[11]. Таким образом, на уровне законодательства ЕС сформирован комплекс мер, направленных на цифровое преобразование как национальных систем правосудия, так и работы наднациональных судебных органов.

Технические решения

В судебных органах ЕС внедрено несколько ключевых электронных платформ. Главная из них — *e-Curia*, электронный портал Суда ЕС. Запущенная в 2011 г. система *e-Curia* предоставляет зарегистрированным пользователям (представителям сторон) возможность электронной подачи документов (исковых заявлений, жалоб и др.) и получения судебных уведомлений онлайн (Reiling & Contini, 2022, p. 7). После регистрации учетной записи и ее подтверждения канцелярией Суда пользователь может загружать процессуальные документы в формате *PDF;* при загрузке каждому документу присваивается метка времени и уникальный хеш-код для подтверждения целостности. Документы автоматически помещаются в электронное досье по делу, доступ к которому стороны получают через свой аккаунт на *e-Curia.* Система отображает статус каждого документа (например, «ожидает принятия», «принят»). С 1 декабря 2018 г. использование *e-Curia* стало обязательным для всех представителей, участвующих в процессе в Суде общей юрисдикции: обмен документами с канцелярией теперь ведется только в электронной форме. Это свидетельствует о высокой степени зрелости цифровой инфраструктуры Суда ЕС. Помимо *e-Curia,* в ЕС реализуется проект *e-CODEX,* направленный на взаимодействие национальных электронных систем правосудия[12]. Программа *e-CODEX* обеспечивает безопасную пересылку судебных документов между государствами-членами (например, при европейском приказе о взыскании задолженности) с использованием электронной подписи и шифрования. Для удаленного участия в судебных заседаниях активно применяется видео-конференц-связь: пандемия побудила Суд ЕС (особенно Суд общей юрисдикции) одним из первых проводить отдельные слушания по видеосвязи, что потребовало технического оснащения залов Суда и принятия соответствующих процессуальных норм[13]. Наконец, Суд ЕС задействует и вспомогательные цифровые инструменты, в частности системы автоматического перевода и управления документами, учитывая многоязычный характер правосудия в ЕС.

Оценка эффективности

Цифровизация принесла ощутимые улучшения показателей деятельности судебных органов ЕС. *Доступность правосудия* выросла: географически удаленные участники могут обращаться в Суд ЕС онлайн, без затрат на почтовую пересылку и поездки в Люксембург. Количество

[11] Regulation 2025/327 не регулирует судебную процедуру как таковую, но формирует режим обмена чувствительными данными, которые могут использоваться и в судебных процессах (например, трансграничные медицинские дела). Joint Communication to the European Parliament and the Council, *An International Digital Strategy for the European Union*, JOIN (2025) 140 final (June 5, 2025), https://digital-strategy.ec.europa.eu/en/library/joint-communication-international-digital-strategy-eu включает разделы о цифровом сотрудничестве в области права, в том числе регламентирует судебное сотрудничество и стандарты обмена данными. European Commission, *Public Consultation on the Review of the European Electronic Communications Code* (launched June 2025), https://ec.europa.eu/newsroom/dae/redirection/document/105481 потенциально затрагивает сферу доказательств и электронного взаимодействия, включая органы правосудия.

[12] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Digitalisation of justice in the European Union — A toolbox of opportunities*, COM (2020) 710 final (Dec. 2, 2020), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:710:FIN

[13] Там же.

пользователей *e-Curia* неуклонно растет с момента запуска, расширяя круг лиц, вовлеченных в наднациональное правосудие. Официальные источники подтверждают:

- стабильный рост пользователей *e-Curia;*
- увеличение доли подаваемых исков в электронной форме;
- расширение круга участников наднационального правосудия за счет нормативных актов.

Это свидетельствует о росте пользователей и расширении круга вовлеченных лиц[14]. *Прозрачность* судебного процесса усилилась: электронный доступ к материалам дела для сторон в режиме реального времени повышает информированность и доверие. Кроме того, ЕС развивает открытые базы данных решений (например, публичный доступ к базам порталов *EUR-Lex* и *e-Justice*), что делает практику Суда более прозрачной[15]. *Скорость рассмотрения дел* возросла за счет устранения почтовых задержек: документы поступают мгновенно, а процессуальные сроки сокращены. По оценкам Еврокомиссии, повсеместное внедрение видеоконференций и электронного обмена документами значительно сократило среднюю продолжительность судебных процессов[16]. *Защита прав участников* при этом обеспечивается соблюдением регламентов: *e-Curia* гарантирует аутентичность и сохранность документов (через хеширование и отметки времени), а процедура верификации пользователей предотвращает несанкционированный

[14] Рост пользователей и электронных подач исков: Court of Justice of the European Union. (2025, February). Annual Report 2024. The Year in Review. https://curia.europa.eu/panorama/2024/en/at-a-glance.html; Court of Justice of the European Union. (2022). 2021 at a glance, Year in Review 2021. https://curia.europa.eu/panorama/2021/en/at-a-glance.html; Court of Justice of the European Union. (2019). Annual Report — The Year in Review 2018. https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-04/ra_pan_2018_en.pdf; Court of Justice of the European Union. (2025). Annual Report 2024 — Statistics Concerning the Judicial Activity of the Court of Justice. https://curia.europa.eu/jcms/upload/docs/application/pdf/2025-03/ra_en_statistiques_24_-_cour.pdf Расширение круга участников (нормативные акты и рекомендации): Decision of the General Court of 10 July 2024 on the lodging and service of procedural documents by means of e-Curia [2024/2096], 2024 O.J. (L 2024/2096) (Aug. 12, 2024); Practice Rules for the Implementation of the Rules of Procedure of the General Court [2024/2097], 2024 O.J. (L 2024/2097) (Aug. 12, 2024) (pt. 121); Recommendations to National Courts and Tribunals in Relation to the Initiation of Preliminary Ruling Proceedings, 2024 O.J. (C 2024/6008) (Oct. 9, 2024); Court of Justice of the European Union, *Conditions of Use of e-Curia* (Sept. 5, 2024), https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-09/2024-09-05_conditions-utilisation-ecuria_en_2024-09-25_10-50-7_866.pdf

[15] Электронный доступ сторон к материалам дела / повышение прозрачности: Decision of the General Court of 10 July 2024 on the lodging and service of procedural documents by means of e-Curia [2024/2096], 2024 O.J. (L 2024/2096) (Aug. 12, 2024); Court of Justice of the European Union, *Conditions of Use of e-Curia* (Sept. 5, 2024), https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-09/2024-09-05_conditions-utilisation-ecuria_en_2024-09-25_10-50-7_866.pdf (доступ к процессуальным документам дела в электронном виде; подтверждение времени подачи); Court of Justice of the European Union. (n.d.). *e-Curia.* https://curia.europa.eu/jcms/jcms/P_78957/en/ (описание подачи/подтверждения времени); European Commission. (2021, November 17). *EU case law. European e-Justice Portal*. https://e-justice.europa.eu/topics/legislation-and-case-law/eu-case-law_en (доступ к судебной практике ЕС); Court of Justice of the European Union. (n.d.). *Case-law database*. https://curia.europa.eu/juris. Скорость рассмотрения, устранение почтовых задержек, сокращение процессуальных задержек: Decision of the General Court of 10 July 2024 on the lodging and service of procedural documents by means of e-Curia [2024/2096], 2024 O.J. (L 2024/2096) (Aug. 12, 2024); Regulation 2023/2844. Оценки Еврокомиссии: видеоконференции и электронный обмен ускоряют процессы / сокращают длительность (European Commission. (2020, December 2). *Digitalisation of justice in the European Union — A toolbox of opportunities* (COM(2020) 710 final). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:710:FIN). Дополнительно в подтверждение общей тенденции эффективности: *European e-Justice Strategy 2024–2028*, 2025 O.J. (C 2025/437).

[16] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *DigitalJustice@2030*, COM (2025) 802 final (Nov. 20, 2025), https://commission.europa.eu/document/download/95918716-ce7d-401b-b6d5-e23effae5b36_en?filename=JUST_template_comingsoon_standard_4.pdf

доступ. В то же время в научной среде обращают внимание на новые риски: цифровые платформы, по сути, навязывают определенные стандартизированные алгоритмы действий, что может ограничивать процессуальную гибкость и усмотрение судей. Российские и международные эксперты указывают, что кодирование процедурных норм в программном обеспечении Суда вызывает вопросы сохранения судебной независимости и справедливости, требуя надлежащего судебного управления ИТ-проектами. ЕС старается решать эти проблемы путем разработки рекомендаций по этичному использованию ИИ и ИТ в судебной сфере и обмена лучшими практиками между странами-членами[17].

Евразийский экономический союз: первые шаги к «цифровому правосудию»

Правовые аспекты

Евразийский экономический союз, созданный Договором о ЕАЭС 2014 г.[18], имеет собственный наднациональный судебный орган — Суд ЕАЭС (действует с 2015 г., г. Минск). В базовых нормативных актах ЕАЭС вопросы цифровизации судебного процесса специально не регламентированы, однако необходимость модернизации Суда ЕАЭС с применением цифровых технологий осознается на высшем уровне. В 2019 г. на международной конференции, посвященной пятилетию Договора о ЕАЭС, подчеркивалась роль Суда в формировании правопорядка интеграции и звучали предложения активнее внедрять электронные формы взаимодействия с национальными судами и заявителями[19]. В 2023 г. судья Суда ЕАЭС В. Сейтимова заявила, что для обеспечения доступа к правосудию в Союзе актуальны «оперативные способы цифровой

[17] См., например: Council of Europe, European Commission for the Efficiency of Justice (CEPEJ), *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment* app. I, at 15–16 (2018), https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment (отмечается, что инструменты ИИ, «почти предписывающие», формируют «новую нормативность», регулируют «судебное усмотрение» и ведут к стандартизации решений); Consultative Council of European Judges (CCJE), *Opinion No. 26 (2023) on the Use of Technology in the Judiciary* 56, 59–60 (Dec. 1, 2023), https://rm.coe.int/ccje-opinion-no-26-2023-final/1680adade7 (подчеркивается, что системные "defaults/prompts" и ИИ-инструменты при рассмотрении дел способны снижать автономию судебного усмотрения, встраивать смещения при назначении слушаний и подрывать прозрачность и апелляционную подотчетность); Reiling & Contini, 2022, § 5.1 (показано, что при кодировании процедур на платформе e-Justice формальные стандарты «вшиваются» в софт, что оказывает стандартизирующее воздействие и снижает усмотрение секретарей, юристов и в ряде случаев — судей); OECD. (2025). *Governing with artificial intelligence: The state of play and way forward in core government functions* (AI in justice administration and access to justice). OECD Publishing. https://www.oecd.org/en/publications/2025/06/governing-with-artificial-intelligence_398fa287/full-report/ai-in-justice-administration-and-access-to-justice_f0cbe651.html (подтверждает системные риски неправильных разработки и/или использования ИИ в сфере правосудия и необходимость государственного ограничения в целях предотвращения искажений стандартов и процедур); Court of Justice of the European Union. (2025, February). Annual Report 2024. The Year in Review. https://curia.europa.eu/panorama/2024/en/at-a-glance.html (e-Curia описывается как единый канал электронного обмена процессуальными документами; демонстрирует стандартизацию шагов и статусов); Globenko, 2021; Belyakova, 2024; Zanin, 2023; Shundikov, 2023; Kukartseva, 2023; Лаптев, В. А. (2025). Нейросети как угроза развитию судебной практики и профессиональная юридическая этика. Право.ru. https://pravo.ru/opinion/260283/

[18] *Treaty on the Eurasian Economic Union*, May 29, 2014, Astana (as amended Mar. 6, 2024), https://eec.eaeunion.org/upload/medialibrary/ef8/ixygbob0o9pvcm5vjrb0sl4vj4pgoiq7/dogovor_o_eaes_2024.pdf

[19] См., например, доклады Н. В. Павловой и Р. К. Сарпекова в ходе Международной конференции «Пять лет Договору о Евразийском экономическом союзе: роль Суда» (г. Минск, 19–20 сентября 2019 г.), организованной Судом Евразийского экономического сообщества: Pavlova, 2020; Sarpekov, 2020.

коммуникации между судом и участниками судопроизводства», отметив необходимость срочной цифровизации работы Суда ЕАЭС[20]. Таким образом, на уровне заявлений и рекомендаций формируется запрос на создание правовой базы электронного судопроизводства[21]. В частности, предлагается внести изменения в Статут Суда ЕАЭС, позволив подавать заявления и жалобы в электронном виде с использованием электронной подписи, а также закрепить возможность дистанционного участия сторон в заседаниях. В пока еще редкой практике Суда ЕАЭС уже были прецеденты, когда документы от сторон принимались по электронной почте в исключительных ситуациях, однако это не оформлено нормативно[22]. Кроме того, государства – члены ЕАЭС предпринимают шаги для взаимного признания электронных доверенных сервисов (электронных подписей, почтовых сервисов) в рамках реализации «Цифровой повестки ЕАЭС до 2025 года», что создаст основу для юридической силы электронных документов в наднациональном судопроизводстве. Пока же каждое обращение в Суд ЕАЭС оформляется на бумаге и направляется заказной почтой либо курьером, что создает издержки по времени. Формирование правовой базы электронного правосудия в ЕАЭС требует согласованных усилий: очевидно, что нормативные изменения должны быть утверждены на уровне Высшего Евразийского совета или посредством поправок к Договору о ЕАЭС, чтобы придать электронным коммуникациям юридическую значимость.

Технические решения

На текущий момент Суд ЕАЭС не располагает полноценной собственной электронной платформой подачи документов, сопоставимой с *e-Curia*. Официальный сайт Суда ЕАЭС публикует информацию о поданных делах и вынесенных решениях, однако интерактивные сервисы для сторон отсутствуют (нет личных кабинетов для подачи и отслеживания исков). В долгосрочной перспективе обсуждается создание электронного кабинета заявителя на сайте Суда, где уполномоченные представители сторон могли бы авторизоваться и загружать процессуальные документы. Такой кабинет предполагает использование проверенных средств аутентификации — например, интеграцию с национальными системами электронного правительства или применение двухфакторной идентификации с защитой от несанкционированного доступа. Неотъемлемый элемент — внедрение электронной цифровой подписи (ЭЦП), признанной всеми государствами ЕАЭС, для удостоверения поданных обращений и процессуальных документов. Технически это требует взаимной доверенной инфраструктуры: возможно, опора на российскую или белорусскую систему валидации ЭЦП либо создание наднационального удостоверяющего центра в рамках ЕАЭС. Еще одно направление — организация видео-конференц-связи для судебных заседаний. Пока все заседания Суда

[20] Российское агентство правовой и судебной информации (РАПСИ). (2023, 25 сентября). *Суд ЕАЭС нуждается в цифровизации и оперативной коммуникации сторон процесса — эксперт*. https://rapsinews.ru/digital_law_news/20230925/309247410.html

[21] См., например: Pavlova, 2020; Sarpekov, 2020.

[22] См., например: постановление Большой коллегии Суда ЕАЭС от 7 июля 2025 г. по делу Р-3/25 (с. 4; зафиксировано, что 30 июня 2025 г. в Суд по электронной почте поступили два заявления об оставлении без рассмотрения ранее поданного обращения); Суд Евразийского экономического союза. (2024). *Практические рекомендации по составлению заявлений о разрешении спора и жалоб на решения Коллегии Суда для хозяйствующих субъектов и Евразийской экономической комиссии*. (п. 9 разд. «Носители»: заявление и приложения представляются в одном экземпляре на бумажном носителе и на электронном (USB/CD)); с. 10 (п. 5: при направлении жалобы следует уведомить Суд по электронной почте); с. 11 (п. 7 разд. «Носители»: по жалобам требуется та же форма).

ЕАЭС проходят очно в Минске, однако, учитывая географию Союза, прорабатывается идея дать сторонам возможность участвовать дистанционно. Заместитель главы Администрации Президента Республики Беларусь Ольга Чуприс в 2024 г. отметила, что «предоставление онлайн-доступа к судебным заседаниям» Суда ЕАЭС — важная, хотя и не ближайшая, перспектива[23]. Это могло бы происходить через защищенную платформу видеоконференций (по аналогии с решениями, применяемыми в судах государств-членов, например, ВКС через специализированный программный комплекс)[24]. Для подготовки к этому Суд ЕАЭС технически оснащается: известно, что зал заседаний оборудован системами аудиозаписи и возможно, средствами для подключения видео; проводятся учебные испытания дистанционных соединений. Наконец, электронный архив и база судебной практики Суда ЕАЭС — еще один необходимый компонент. В Беларуси Национальный центр правовой информации уже инициативно создал банк данных «Судебная практика» на Национальном правовом интернет-портале, где размещены оцифрованные тексты 381 решения Суда ЕАЭС. Однако официально решения Суда ЕАЭС не интегрированы ни в один общеевразийский ресурс, ни в национальные правовые базы государств-членов. Предстоит разработать единую электронную систему публикации и поиска решений ЕАЭС, возможно на базе сайта Суда или портала ЕАЭС, что повысит прозрачность и предсказуемость правоприменения.

Оценка эффективности (прогноз и текущая ситуация)

Поскольку цифровизация правосудия в ЕАЭС находится в начале пути, ее эффект пока носит потенциальный характер. *Доступность правосудия* в наднациональном измерении сейчас ограничена: например, хозяйствующие субъекты из Казахстана или Кыргызстана, желающие обжаловать акт ЕЭК, сталкиваются с языковым барьером (рабочие языки Суда: русский и, возможно, английский) и процедурными сложностями подачи документов в Минск (Diyachenko & Entin, 2017, pp. 67–72). Внедрение электронного кабинета и онлайн-подачи исков резко повысило бы доступность, устранив необходимость физической пересылки документов и личного присутствия при подаче. Это особенно значимо для хозяйствующих субъектов, осуществляющих деятельность в удаленных регионах государств-членов ЕАЭС. Развитие дистанционных форм взаимодействия с Судом Союза способно снизить пространственные и организационные барьеры доступа к наднациональной судебной защите. В данном контексте речь идет не о «приближении правосудия к гражданину» в классическом смысле, а о функциональном упрощении доступа к судебным механизмам интеграционного объединения для экономических субъектов, вовлеченных в трансграничные экономические отношения. *Прозрачность* деятельности Суда ЕАЭС частично обеспечивается публикацией решений, но страдает из-за отсутствия удобных инструментов их поиска и анализа. Цифровая база данных решений с расширенным поиском по ключевым словам и темам, открытая общественности, повысит прозрачность и научную проработку интеграционного права. *Скорость рассмотрения дел* в Суде ЕАЭС теоретически могла бы возрасти с цифровизацией: даже при небольшом количестве дел (в среднем несколько в год) электронная коммуникация позволила бы сократить сроки обмена документами и подготовки позиций сторон. Например, сейчас пересылка запроса или доказательств почтой может занимать недели, тогда как электронная подача — минуты.

[23] Белорусское телеграфное агентство. (2024, 21 ноября). Чуприс: важно внедрять цифровой компонент в деятельность Суда ЕАЭС. *БелТА*. https://belta.by/society/view/chupris-vazhno-vnedrjat-tsifrovoj-komponent-v-dejatelnost-suda-eaes-677116-2024/

[24] Там же.

Кроме того, видео-конференц-связь дала бы возможность оперативно заслушивать представителей сторон, экспертов без организационных задержек. *Защита прав участников процесса* в цифровой среде — ключевой момент: необходимо обеспечить, чтобы переход к электронным формам не ущемлял прав на справедливое разбирательство. Важно сохранить принцип равноправия сторон (например, гарантировать, что все имеют равный доступ к технологиям, предоставлять альтернативы в случае технических сбоев), конфиденциальность совещаний судей, надежную защиту подаваемых в электронной форме доказательств от подделки. В этом смысле ЕАЭС может опираться на стандарты ЕС в области защиты данных (*GDPR*) и на лучшие национальные практики (в России, Казахстане уже есть опыт электронного правосудия в национальных судах с соблюдением ГОСТов безопасности (Baimoldina, 2024, p. 44). В целом эксперты сходятся во мнении, что цифровизация Суда ЕАЭС при политической поддержке способна модернизировать судебную систему Союза, сделав ее более эффективной, открытой и ориентированной на потребности участников экономических отношений, формирующимся в условиях цифровой трансформации XXI в.[25] Однако для реализации этого потенциала предстоит преодолеть инерцию и скептицизм, а также вложиться в создание современной ИТ-инфраструктуры.

МЕРКОСУР: ограниченное применение электронного судопроизводства

Правовые аспекты

Механизм разрешения споров в МЕРКОСУР значительно отличается от ЕС и ЕАЭС. В основе — Протокол Оливос 2002 г. о решении споров, который учредил многоуровневую арбитражную систему[26]. При возникновении спора государства-участники сначала проводят прямые переговоры; если соглашение не достигнуто, создается трибунал *ad hoc* (временный третейский суд) из трех арбитров для рассмотрения конкретного спора (Avila Paz de Robledo, 2007). Решение этого трибунала может быть пересмотрено Постоянным ревизионным трибуналом (*Tribunal Permanente de Revisión, TPR*, далее — ПРТ), который находится в г. Асунсьоне. ПРТ состоит из шести арбитров (по одному от пяти стран и один запасной) и выступает своего рода апелляционной инстанцией. Следует отметить, что ПРТ не является постоянно действующим судом, как Суд ЕС; он собирается эпизодически при наличии дел. Правовая база функционирования ПРТ и арбитражей — Протокол Оливос и Регламент. Специальных положений о цифровой подаче документов или дистанционном рассмотрении в этих актах изначально не было, что отражает уровень технологий начала 2000-х гг. Однако в последние годы в рамках Рабочей группы МЕРКОСУР по правовым вопросам поднимается тема модернизации процедур. В частности, государства обмениваются нотами о возможности направления материалов дел в электронной форме. Так, в октябре 2023 г. на заседании Форума центральных органов МЕРКОСУР по правовым вопросам было подчеркнуто значение электронного обмена запросами о правовой помощи между странами. В ходе этого совещания представители договорились, что, например, Перу (ассоциированный член) будет принимать от Бразилии запросы в электронном виде наравне с другими странами, где эта практика уже

[25] Московский государственный институт международных отношений (МГИМО). (2025, 17 апреля). Конференция «Интеграционные процессы в Евразии: состояние, вызовы, перспективы» [Новость]. https://mgimo.ru/about/news/departments/konf-integratsionnye-protsessy-v-evrazii-25/

[26] *Olivos Protocol for the Settlement of Disputes in MERCOSUR*, Feb. 18, 2002, https://www.mercosur.int/?wpdmdl=63394 (entered into force Jan. 1, 2004).

налажена[27]. Кроме того, на уровне министров юстиции МЕРКОСУР планируется принять декларацию о поощрении перехода на электронное делопроизводство при межгосударственном взаимодействии судов и центральных органов[28]. Таким образом, правовая база МЕРКОСУР в части цифровизации находится на стадии формирования через соглашения и декларации о сотрудничестве, хотя формальные правила арбитражного процесса пока не обновлены.

Технические решения

В силу ограниченного числа споров и отсутствия постоянной судейской инфраструктуры МЕРКОСУР не создал единого электронного портала для подачи исков как таковых: обращения в арбитраж оформляются по дипломатическим каналам между государствами-членами. Тем не менее некоторые технические элементы электронного правосудия применяются. Во-первых, Секретариат ПРТ ведет электронный архив решений и заключений. Официальный веб-сайт ПРТ публикует тексты всех *laudos* (арбитражных решений) и *opiniones consultivas* (консультативных заключений) на испанском и португальском, а также нормативные документы, что обеспечивает открытый доступ к практике МЕРКОСУР в онлайн-режиме (https://www.tprmercosur.org/es/opi_consultivas.htm). Во-вторых, в условиях пандемии *COVID-19* впервые были опробованы дистанционные форматы: по сведениям СМИ, некоторые совещания арбитров и консультации сторон в 2020–2021 гг. проводились в режиме видеоконференции, хотя официально это не афишировалось. По крайней мере, Совет глав судей стран МЕРКОСУР (неформальный форум национальных судебных органов) в этот период перешел на онлайн-заседания. В-третьих, МЕРКОСУР инвестирует в общие проекты по интеграции информационных систем судебных властей государств-участниц. Например, действует южноамериканская информационная сеть *IberRed* (https://iberred.notariado.org/), к которой присоединены и страны МЕРКОСУР, облегчающая обмен судебными уведомлениями в электронной форме (проект похожий по идее на европейскую систему *e-Justice*, но в Латинской Америке). Имеются наработки по созданию платформы для обмена судебными поручениями (аналог европейской *e-CODEX,* но в более скромном масштабе). Отдельно стоит упомянуть, что среди стран МЕРКОСУР уровень цифровизации правосудия неравномерен: Бразилия и Аргентина достигли значительного прогресса (системы электронного процесса — *Projudi* и др., — позволяющие полностью электронное ведение дел в судах общей юрисдикции, https://www.tjpi.jus.br/), тогда как Парагвай, Уругвай и Боливия находятся в процессе реформ. Эти национальные достижения частично создают фундамент для наднационального уровня; например, если все страны-участницы внедрят совместимые механизмы электронной подписи и документооборота, то и для МЕРКОСУР станет проще построить общую цифровую площадку.

Оценка эффективности

Доступность правосудия на уровне МЕРКОСУР традиционно ограниченна, поскольку частные лица напрямую не могут инициировать разбирательства в ПРТ (только через свои государства, хотя ст. 39–44 Протокола Оливос допускают механизм *denuncia* для частного лица, требующего

[27] Ministério da Justiça e Segurança Pública. (2023, 19 октября). *Mercosul discute acesso à Justiça e aprofunda digitalização da cooperação jurídica* [МЕРКОСУР обсуждает доступ к правосудию и углубляет цифровизацию юридического сотрудничества] (обновлено 20 октября 2023 г.). https://www.gov.br/mj/pt-br/assuntos/noticias/mercosul-discute-acesso-a-justica-e-aprofunda-digitalizacao-da-cooperacao-juridica

[28] Там же.

от национальных секций Группы общего рынка инициировать разбирательство)[29]. Поэтому влияние цифровизации на доступность для бизнеса или граждан опосредованно. Однако в случае, если спор начинается, электронные коммуникации между национальными органами могут ускорить и облегчить участие сторон. Например, возможность подачи документов государствами-участниками в Секретариат ПРТ по защищенному электронному каналу ускорила бы формирование арбитражей. *Прозрачность* механизма разрешения споров в системе МЕРКОСУР носит умеренный характер: хотя арбитражные решения подлежат публикованию, сами разбирательства проводятся в закрытом формате, без публичных слушаний, участия третьих лиц и открытого доступа к процессуальным материалам. Введение онлайн-трансляций заседаний арбитражей или хотя бы публикация расписания и процессуальных документов повысило бы открытость, однако пока такое не практикуется. Тем не менее выход в онлайн уже осуществляется в части просвещения: ПРТ, позиционируя себя как «юридическая столица МЕРКОСУР», организует вебинары и выкладывает информационные материалы на своем сайте. *Скорость рассмотрения споров* в МЕРКОСУР трудно сравнивать с ЕС из-за очень небольшого количества дел (несколько десятков за более чем 20 лет). В целом арбитражные процедуры по Протоколу Оливос рассчитаны на месяцы. Цифровизация способна устранить некоторые задержки, например ускорить коммуникацию между национальными координаторами спора. Недавний пример — достигнутая договоренность о взаимном признании электронных запросов об обмене документами с Перу[30], позволяющая не ждать бумажных оригиналов. Это ускорит сотрудничество по гражданско-правовым вопросам, что косвенно улучшает и инвестиционный климат. *Защита прав участников* в цифровом аспекте для МЕРКОСУР пока не стала предметом отдельного анализа. Поскольку споры ведутся государствами, ключевой момент — защита конфиденциальности обмена позициями. Электронная связь через безопасные каналы (например, зашифрованная электронная почта между министерствами иностранных дел) уже применяется и считается надежной. Если же в будущем МЕРКОСУР пойдет по пути допуска частных сторон к платформам онлайн-разрешения споров (*online dispute resolution, ODR*) для рассмотрения трансграничных споров (например, потребителей в рамках регионального рынка), тогда надо будет учитывать вопросы юрисдикции, применимого права и исполнения решений в цифровой среде. Пока такие проекты находятся на этапе обсуждений, причем скорее под эгидой Организации американских государств для всей Латинской Америки (Szlak, 2012, pp. 542–545), чем в самом МЕРКОСУР.

В целом можно констатировать, что МЕРКОСУР отстает от ЕС в институционализации электронного правосудия: отсутствует постоянный суд, нет жесткой потребности в собственной цифровой платформе из-за низкой нагрузки. Однако интеграционные задачи, такие как улучшение взаимного доступа к правосудию граждан стран МЕРКОСУР, стимулируют хотя бы ограниченную цифровизацию процессов взаимодействия (правовая помощь, признание решений). В 2022 г. министры юстиции стран-участниц обсудили «углубление цифровизации юридического сотрудничества», что свидетельствует о политической воле к прогрессу[31]. Возможно,

[29] *Olivos Protocol for the Settlement of Disputes in MERCOSUR*, Feb. 18, 2002, https://www.mercosur.int/?wpdmdl=63394 (entered into force Jan. 1, 2004).

[30] MERCOSUR. (2019, 11 декабря). *Acuerdo de reconocimiento mutuo de firmas digitales en el MERCOSUR* [Соглашение о взаимном признании цифровых подписей в МЕРКОСУР]. https://www.mercosur.int/acuerdo-de-reconocimiento-mutuo-de-firmas-digitales-en-el-mercosur

[31] Pena, C., Zelicovich, J., Thorstensen, V., & Mota, C. (2023). MERCOSUR: Strategic divergences and pragmatic consensus (Mercosur Report No. 26). Inter-American Development Bank (INTAL). https://publications.iadb.org/publications/english/document/Mercosur-Report-No-26-MERCOSUR-Strategic-Divergences-and-Pragmatic-Consensus.pdf

со временем МЕРКОСУР придет к созданию некоего подобия единого электронного окна для трансграничных юридических услуг (аналог *e-Justice Portal* ЕС, но с учетом двух официальных языков: испанского и португальского).

АСЕАН: координация национальных инициатив и отсутствие наднационального суда

Правовые аспекты

В отличие от предыдущих объединений АСЕАН не располагает постоянно действующим судебным органом, способным рассматривать споры между участниками интеграции или между частными лицами и государствами. Согласно Уставу АСЕАН 2007 г. споры между государствами разрешаются мирными средствами, включая переговоры, консультации, посредничество и встречи старших должностных лиц по экономике стран-участниц[32]. Также в рамках экономических соглашений АСЕАН действует механизм, похожий на ВТО: создаются арбитражные панели *ad hoc* из экспертов для рассмотрения споров о толковании соглашений, с последующим возможным апелляционным рассмотрением (хотя постоянного апелляционного органа нет)[33]. Таким образом, говорить о «судебном процессе» в АСЕАН можно условно — скорее это арбитражно-дипломатические процессы. Тем не менее АСЕАН предпринимает коллективные усилия по модернизации правовой сферы с учетом цифровой эпохи. Принят ряд согласованных документов, например, Бангкокская цифровая декларация АСЕАН 2019 г., которая хотя и фокусируется на цифровой экономике, но затрагивает и аспекты электронной идентификации, защиты данных и кибербезопасности — необходимые предпосылки для электронного правосудия[34]. Кроме того, в сфере уголовного правосудия АСЕАН сотрудничает по линии АСЕАНАПОЛ (сеть полицейского сотрудничества) и *ASEAN Mutual Legal Assistance Agreement*, где всё активнее используются электронные средства коммуникации для обмена запросами о правовой помощи. Особую роль играет Совет главных судей АСЕАН (*Council of ASEAN Chief Justices, CACJ*) — неинтеграционный орган, объединяющий руководителей верховных судов 10 стран АСЕАН. Совет не является наднациональным судом, но служит платформой для обмена опытом и выработки общих подходов. В 2018 г. Советом судей была принята Сингапурская декларация, определяющая рамки судебного сотрудничества в АСЕАН и предусматривающая развитие электронных механизмов обмена информацией между судебными органами государств-членов[35]. В 2020–2021 гг. Совет провел серию онлайн-совещаний, где обсуждались уроки пандемии: главные судьи пришли к выводу о необходимости активно внедрять видео-конференц-связь и электронное дело в национальных судах, а также обеспечивать совместимость технологий между странами. В 2023 г. Совет судей презентовал несколько совместных публикаций, включая Свод передового опыта по проведению судебных заседаний в режиме видеоконференции в странах

[32] *Charter of the Association of Southeast Asian Nations*, Nov. 20, 2007, https://asean.org/wp-content/uploads/2021/09/21069.pdf (entered into force Dec. 15, 2008).

[33] Understanding on Rules and Procedures Governing the Settlement of Disputes, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 2, https://www.wto.org/english/tratop_e/dispu_e/dsu_e.htm

[34] VietnamPlus. (2025, 20 января). *Члены АСЕАН договорились о создании безопасной цифровой среды*. https://ru.vietnamplus.vn/chleni-asean-dogovorilis-o-sozdanii-bezopasnoi-tsifrovoi-sredi-post75392.vnp

[35] Singapore Declaration, 6th Meeting of the Council of ASEAN Chief Justices (July 27, 2018), https://cacj-ajp.org/web/wp-content/uploads/2021/05/Singapore-Declaration-2018.pdf

АСЕАН[36]. Этот документ служит руководством для национальных судов по эффективному использованию видеотехнологий, повышая эффективность и доступность правосудия. Хотя он не накладывает обязательств, наличие подобной согласованной инструкции — шаг к унификации практик электронного правосудия в регионе.

Технические решения

Поскольку интеграционные судебные процессы как таковые в АСЕАН минимальны, основные цифровые решения реализуются на национальном уровне, с координацией через Совет судей. Наиболее продвинутыми считаются суды Сингапура и Малайзии: Сингапур еще до пандемии запустил систему *Electronic Litigation System (eLitigation)* — платформу для электронной подачи исков и управления делами во всех судах, с возможностью удаленного доступа адвокатов и судебных сотрудников[37]. В Малайзии функционирует комплекс *e-Kehakiman (e-Court System)* с электронной подачей документов, отслеживанием статуса дела и даже мобильным приложением для судей[38]. Индонезия в 2019 г. ввела онлайн-суды (*e-Court*) по гражданским и религиозным делам, включая электронную регистрацию и рассмотрение простых споров онлайн[39]. Таким образом, к 2020 г. большинство стран АСЕАН имели базовые элементы *e-justice* в национальных судах. Пандемия дала толчок: например, Верховный суд Филиппин утвердил правила для дистанционных судебных слушаний через видеоконференцию, главным образом по уголовным делам (для допроса обвиняемых, находящихся в тюрьме, по видеосвязи)[40]. В Таиланде программа *D-Court 2020* нацелена на полную цифровизацию судопроизводства к 2020 г. (сейчас реализована подача исков онлайн и использование видеоконференций)[41]. В рамках сотрудничества АСЕАН создала *ASEAN Judicial Portal* — закрытую платформу для обмена информацией между судами, где размещаются базы данных прецедентов, контакты, обучающие материалы. Отдельно стоит упомянуть проекты с международными партнерами: Совет Европы реализует *Octopus Project* с участием 9 стран АСЕАН, обучающий судей работе с электронными доказательствами и киберпреступления[42]. Такие тренинги

[36] Supreme Court of the Philippines, Pub. Info. Office, *Council of ASEAN Chief Justices Launch Publications on Human Trafficking, Cross-Border Disputes Involving Children and Videoconferencing Hearings* (Nov. 28, 2024), https://sc.judiciary.gov.ph/council-of-asean-chief-justices-launch-publications-on-human-trafficking-cross-border-disputes-involving-children-and-videoconferencing-hearings/

[37] Singapore Judiciary, *eLitigation* (https://www.judiciary.gov.sg/services/elitigation); Supreme Court of Singapore. (2013). *Supreme Court Practice Directions 2013 (To be read with the Rules of Court (Cap. 322, R 5, 2014 Rev. Ed.)).* https://epd2013-supremecourt.judiciary.gov.sg/

[38] Malay Mail. (2025). *Explained: What e-Kehakiman means for lawyers, media and the public.* https://www.malaymail.com/news/malaysia/2025/12/22/explained-what-ekehakiman-means-for-lawyers-media-and-the-public/202752

[39] Bich Thao, N. & Huynh Nga, T. (2022). *E-courts in Indonesia and experience for Vietnam: Towards judicial harmonization and modernization in the ASEAN region* (Draft paper). Asian Law Centre, Melbourne Law School. https://law.unimelb.edu.au/__data/assets/pdf_file/0009/4356675/NGUYEN-Bich-Thao-and-TRUONG-Huynh-Nga.pdf

[40] Office of the Court Administrator, Supreme Court of the Philippines. (2020, December 29). *OCA Circular No. 209-2020* (videoconferencing guidelines implementation). https://oca.judiciary.gov.ph/wp-content/uploads/OCA-Circular-No.-209-2020.pdf; Philippine Daily Inquirer. (2019, August 6). *SC allows videoconferencing for detainees in proceedings.* https://newsinfo.inquirer.net/1151039/sc-allows-videoconferencing-for-detainees-in-proceedings

[41] Baranda, E., Thammasujarit, P., Lovita, T., & Vu, Y. (2020, July 10). *E-filings and hearings in courts in South East Asia.* Rouse. https://rouse.com/insights/news/2020/e-filings-and-hearings-in-courts-in-south-east-asia

[42] Council of Europe, Cybercrime Programme Office (C-PROC). (2024, October 3). *Octopus Project: Judicial knowledge exchange between ASEAN countries on cybercrime and electronic evidence.* https://www.coe.int/en/web/cybercrime/-/octopus-project-judicial-knowledge-exchange-between-asean-countries-on-cybercrime-and-electronic-evidence

косвенно улучшают готовность судебных систем АСЕАН к цифровым процессам. Кроме того, в некоторых странах (например, Вьетнаме) внедряются пилотные онлайн-платформы медиации для разрешения коммерческих споров, которые могут со временем масштабироваться на регион, особенно для споров в сфере *e-commerce* внутри АСЕАН.

Оценка эффективности

В силу отсутствия единого суда АСЕАН оценивать *доступность, прозрачность и скорость* наднационального правосудия сложно: споры между государствами редки, и их разрешение носит скорее политико-дипломатический характер. Однако эффекты цифровизации проявляются в упрощении судебного сотрудничества между странами. Например, электронный обмен запросами о выдаче или о вручении документов в рамках соглашения АСЕАН о взаимной правовой помощи ускоряет процесс содействия и снижает бюрократические барьеры. Это означает, что частное лицо, вовлеченное в трансграничный спор (скажем, предприятие из Таиланда судится с партнером в Индонезии), быстрее получит необходимые документы или признание решения, если соответствующие органы обмениваются данными онлайн. *Прозрачность* региональных процессов, таких как деятельность Совета главных судей АСЕАН, повышается за счет публикации согласованных итоговых документов (например, упомянутого Свода по видеоконференциям) и освещения инициатив в СМИ. Хотя решения по межгосударственным спорам в АСЕАН практически не публикуются (поскольку всё стараются уладить тихо), сами национальные судебные системы становятся более открытыми для общественности благодаря электронным сервисам (например, в некоторых странах введены онлайн-трансляции ключевых процессов, электронные кабинеты для отслеживания дел). *Скорость правосудия* в регионе возрастает по мере цифровизации национальных судов: сокращаются очереди, процессы вроде подачи иска или жалобы происходят быстрее (в Сингапуре значительное число действий можно выполнить за считанные минуты через *eLitigation,* что ранее требовало личного визита в суд). Перекрестное признание электронных подписей и электронных судебных документов между странами АСЕАН могло бы еще ускорить исполнение судебных решений за границей, хотя до этого пока далеко. *Защита прав* в цифровой среде — важный вопрос, особенно ввиду разнообразия правовых систем АСЕАН (континентальная, система общего права, мусульманское право). Совет судей АСЕАН в упомянутом Своде по видеоконференциям отмечает принципы: добровольность согласия на видеослушание, обеспечение конфиденциальности, техническая поддержка для участников, не владеющих технологией[43]. Это призвано гарантировать, что переход на виртуальные заседания не нарушит право на справедливое разбирательство. Тем не менее, в менее развитых странах региона сохраняются проблемы с инфраструктурой (неустойчивый интернет, нехватка оборудования), что может приводить к «цифровому неравенству» участников процесса. Решением может быть помощь более развитых членов АСЕАН: известно, что Сингапур «делится» с соседями программными наработками и обучающими программами для судебных ИТ-специалистов.

Подводя итог, можно сказать, что интеграция судебных процессов в АСЕАН носит «мягкий» характер — через унификацию подходов и обмен опытом, а не через единые нормы и политики. Цифровизация правосудия рассматривается в контексте «человекоориентированной» АСЕАН,

[43] Supreme Court of the Philippines, Pub. Info. Office, *Council of ASEAN Chief Justices Launch Publications on Human Trafficking, Cross-Border Disputes Involving Children and Videoconferencing Hearings* (Nov. 28, 2024), https://sc.judiciary.gov.ph/council-of-asean-chief-justices-launch-publications-on-human-trafficking-cross-border-disputes-involving-children-and-videoconferencing-hearings/

где упор делается на улучшение жизни и благосостояния граждан. В этом смысле электронное правосудие — часть более широкой цифровой трансформации интеграционного управления. Опыт АСЕАН показывает, что даже без наднационального суда интеграционное объединение может стремиться к сближению стандартов электронного судопроизводства, что со временем призвано облегчить и потенциальное урегулирование споров, и взаимное признание судебных решений.

Дискуссия

Сопоставление опыта четырех интеграционных объединений позволяет выявить общие тенденции и оценить, насколько успешна цифровизация судебных процессов в разных условиях интеграционного строительства.

Степень интеграции и прогресс цифровизации

Прослеживается прямая зависимость между глубиной интеграции объединения и уровнем внедрения «цифрового правосудия». ЕС, как активное интеграционное объединение с развитой наднациональной составляющей, достиг наибольшего успеха: разработана комплексная стратегия цифровизации правосудия, действуют обязательные для всех институтов требования (*e-Curia* в Суде ЕС, *e-CODEX* для государств-членов). ЕАЭС, стремительно развивающееся молодое интеграционное объединение, только формирует подобную повестку: цифровизация Суда ЕАЭС провозглашается целью, но еще не реализована практически. МЕРКОСУР и АСЕАН, имеющие низкую степень наднациональности, демонстрируют и низкий уровень институциональной цифровизации: у них нет сильного наднационального суда, а потому нет «локомотива» электронного правосудия. Однако они идут путем координации национальных усилий и частичной модернизации процедур сотрудничества (взаимная правовая помощь и т.п.). Таким образом, гипотеза о корреляции интеграции и цифровизации подтверждается: наднациональные судебные структуры стимулируют внедрение технологий сильнее, чем межправительственные формы взаимодействия.

Доступность правосудия и вовлеченность участников

Цифровизация везде декларируется как средство повышения доступности судов для граждан и бизнеса. В ЕС это выразилось конкретно: уменьшились издержки для обращающихся в Суд ЕС, барьеры (географические, финансовые) стали ниже. В ЕАЭС и МЕРКОСУР эффект пока потенциальный: сами суды этими возможностями не оснащены. Но в перспективе, как отмечают эксперты, электронное правосудие способно «приблизить» интеграционные суды к заинтересованным сторонам (Mikhaliova & Vasilevich, 2023, p. 190), что особенно важно для обоснования существования наднациональных судов в глазах населения. Для АСЕАН вопрос доступности решается преимущественно на национальном уровне: благодаря электронным сервисам жители ряда стран Юго-Восточной Азии могут быстрее и проще обратиться в суд, хотя на региональном уровне прямого доступа нет. Здесь можно говорить о «парадоксе интеграции»: регион без наднационального суда (АСЕАН) все же выигрывает от цифровизации национальных систем, способствуя косвенному сближению правовых пространств и облегчая взаимный доступ к судам стран-участниц. Например, если все суды АСЕАН будут предоставлять услуги онлайн и на английском языке (рабочем языке АСЕАН), то иностранному участнику будет проще инициировать процесс в другой стране.

Прозрачность и доверие

Электронные инструменты обычно повышают прозрачность работы судов: публикация решений онлайн, открытые реестры, трансляции заседаний — все это делает суд более понятным обществу. В ЕС и ЕАЭС прозрачность наднационального правосудия важна для укрепления легитимности интеграции. ЕС добился значительного прогресса: решения Суда ЕС доступны на всех языках Союза, портал *e-Justice* содержит подробные сведения о судебной системе. В ЕАЭС же до сих пор решения Суда не интегрированы даже в национальные базы данных всех государств-членов, что снижает их видимость. Цифровизация здесь должна сыграть роль: размещение практики Суда ЕАЭС в единой электронной базе открытого доступа повысит прозрачность и доверие деловых кругов к правовой предсказуемости Союза. В МЕРКОСУР прозрачность ограничена: арбитражный механизм по природе менее публичен. Впрочем, публикация ПРТ отдельных значимых дел и инициатив свидетельствует о стремлении улучшить общественное понимание регионального правосудия[44]. АСЕАН, не имея наднационального суда, делает ставку на прозрачность реформ — информирование общественности о шагах по модернизации. Это формирует доверие и мнение, что судебные власти адаптируются к современности и учитывают интересы граждан. В целом прозрачность — один из показателей эффективности реформ: можно утверждать, что ЕС и АСЕАН более успешно продвигают открытость (каждое объединение на своем уровне), в то время как ЕАЭС и МЕРКОСУР следует активнее доводить информацию о своей судебной деятельности до конечных пользователей.

Скорость и эффективность разрешения споров

Все объединения сходятся во мнении, что цифровые технологии ускоряют судебные процессы[45]. Практика ЕС подтверждает сокращение сроков отдельных процедур (например, электронное уведомление через *e-Curia* экономит в среднем 7–10 дней на каждый процессуальный шаг по сравнению с почтовым отправлением). Кроме того, автоматизация рутинных операций (регистрации дел, рассылки повесток) разгружает аппарат Суда, позволяя сосредоточиться на юридической сути. ЕАЭС, имея небольшой поток дел, возможно, не ощутит драматического сокращения сроков, но для истцов даже неделя-другая имеет значение, особенно в спорах, связанных с рынками и бизнес-решениями. МЕРКОСУР и АСЕАН, где споры разрешаются больше политически, также выигрывают от скорости коммуникации: оперативный обмен мнениями и проектами решений между правительствами государств – членов АСЕАН по электронной почте может предотвратить эскалацию конфликта. Интересный кейс — электронная платформа *ODR* для мелких трансграничных споров. ЕС уже обсуждает создание общеевропейской системы *ODR* для потребителей (прототип — платформа разрешения споров онлайн в сфере *e-commerce* в ЕС). Авторы предлагают ЕАЭС рассмотреть аналогично платформу для малозначительных трансграничных споров под эгидой ЕЭК (Mikhaliova & Vasilevich, 2023, p. 198). Это могло бы значительно ускорить разрешение типичных небольших споров (например, по электронным торговым площадкам) и разгрузить суды. Бразилия, например, запустила портал *Consumidor.gov.br* для онлайн-примирения потребителей и компаний, что повысило скорость удовлетворения претензий (Schmidt-Kessen et al., 2020, p. 659). Если

[44] MERCOSUR, Secretaría del MERCOSUR. (2025). Tribunal Permanente de Revisión del MERCOSUR presenta el libro “Amicus Curiae” [Постоянный трибунал пересмотра МЕРКОСУР представляет книгу «Amicus Curiae»]. https://www.mercosur.int/tribunal-permanente-de-revision-del-mercosur-presenta-el-libro-amicus-curiae/

[45] McCoubrey, S. (2022). *e-Justice: Digital transformation to close the justice gap.* United Nations Development Programme (UNDP). https://www.undp.org/sites/g/files/zskgke326/files/2022-06/E%20justice-Report%2005.pdf

подобное внедрять на интеграционном уровне, это станет революцией в доступности и скорости правосудия.

Защита прав и справедливость процесса

Один из центральных вопросов — не пострадает ли качество правосудия при цифровизации. Критики опасаются, что «виртуальный суд» может ущемлять права (например, право быть выслушанным судом очно, право на личное общение с адвокатом и т.д.). В ЕС эти опасения артикулированы особенно четко: подчеркивается, что цифровые процедуры должны оставаться справедливыми. Это требует адаптации процессуальных норм — и ЕС этим занимается (вносятся изменения о допустимости видеодопросов, об обязательном предоставлении технической возможности удаленного участия в заседаниях с использованием средств аудио- и видеосвязи и т.п.). В ЕАЭС нужно заранее учесть подобные моменты: например, если внедрять видеоконференцию, прописать в регламенте, что сторона может возражать против нее, если у нее нет доступа к оборудованию, и тогда заседание должно быть очным, чтобы не нарушился баланс. Другой аспект — защита данных и кибербезопасность. Судебные документы часто содержат коммерческую тайну, личные данные. Их утечка или неправомерный доступ к цифровой системе недопустимы. ЕС здесь опять лидирует, имея строгие правила шифрования и хранения данных. В ЕАЭС, МЕРКОСУР и АСЕАН вопрос защиты данных также становится частью повестки цифровизации: АСЕАН приняла в 2016 г. рамочные принципы защиты персональных данных, и страны синхронизируют законодательство, что поспособствует и безопасности судебных ИТ-систем. МЕРКОСУР в 2020 г. разработал Декларацию о правах человека в цифровую эпоху, где признаются права на приватность и прозрачность, созвучные задачам электронного правосудия[46]. Таким образом, обеспечение киберустойчивости судебной инфраструктуры — общее требование. Без этого доверие к электронному правосудию не закрепится. К счастью, технологий для защиты (электронная подпись, блокчейн-хранение судебных решений, многоуровневая аутентификация пользователей) достаточно; важно, чтобы политическая воля и финансирование позволили их внедрить.

Лучшие практики и обмен опытом

Рассмотренные объединения могут многому научиться друг у друга. ЕС представляет собой эталон в части комплексного подхода — сочетание нормативных изменений (регламенты, директивы) с разработкой ИТ-решений (порталы, сети) и постоянным мониторингом результатов (ежегодные оценки правосудия в странах ЕС, индекс электронного правосудия и пр.). В ЕАЭС ряд доктринальных и экспертных работ, посвященных цифровизации правосудия в Союзе, в качестве ориентира рассматривает модель европейского портала *e-Justice,* включая идею единой точки доступа к судебной информации и сервисам для участников процесса[47]. МЕРКОСУР, хотя географически далек, испытывает схожие проблемы с ЕАЭС (многоуровневое право, разные правовые традиции). Его опыт показывает, как важно при скромных ресурсах сфокусироваться на приоритетах: возможно, вместо создания дорогой системы *e-Curia* МЕРКОСУР выберет

[46] Blanchet, A. (2023, November 27). New human rights in the digital age: Mercosur's contribution to international regulation. *Equal Times*. https://www.equaltimes.org/new-human-rights-in-the-digital

[47] См. подробнее: Решение Высшего евразийского экономического совета № 12 «Об утверждении Основных направлений реализации цифровой повестки Евразийского экономического союза до 2025 года» от 11 октября 2017 г.; Правовой портал ЕАЭС. https://docs.eaeunion.org; Портал открытых данных ЕАЭС. https://data.eaeunion.org; Информационный портал ЕАЭС. https://eaeunion.org; Afanas'yev et al., 2022; Laptev & Solovyanenko, 2021.

сначала облачное хранилище решений или систему видеозаседаний для арбитров. АСЕАН демонстрирует ценность координационного механизма судей: было бы полезно ЕАЭС учредить подобный Совет председателей судов (например, председателей верховных судов стран ЕАЭС) для обсуждения цифровой трансформации правосудия на национальном и наднациональном уровне. Это бы обеспечило и вовлеченность национальных судов в процессы Суда ЕАЭС.

Наконец, все четыре региона заинтересованы в совместимости своих систем с глобальными трендами. Международные организации (ООН, Всемирный банк) проводят исследования и реализуют пилотные проекты в области *e-justice.* Активное участие интеграционных объединений в этих инициативах (например, как АСЕАН делает через *UNDP Judicial Integrity Network*) помогает избежать ошибок и ускорить внедрение цифровых технологий.

Подводя итог дискуссионной части, подчеркнем: цифровизация судебных процессов не просто техническое новшество, а существенное изменение институциональной логики интеграционного правосудия. Она способна придать новые смыслы старым структурам (Суд ЕС стал ближе к гражданам, Суд ЕАЭС может стать эффективнее и заметнее через онлайн-форматы) и даже компенсировать некоторые недостатки интеграции (например, отсутствие суда в АСЕАН отчасти смягчается общим ростом уровня судопроизводства в регионе благодаря технологиям). Важно помнить, что технология должна служить праву, а не заменять его. Судебные органы несут ответственность за то, чтобы, внедряя ИТ, сохранить высшие ценности правосудия: независимость, беспристрастность, равенство сторон и соблюдение всех процедурных гарантий.

Заключение

Цифровая трансформация судопроизводства становится неотъемлемой частью развития интеграционных объединений в XXI в. Проведенное исследование сравнительного опыта ЕС, ЕАЭС, МЕРКОСУР и АСЕАН подтверждает, что «цифровое правосудие» из концепции превращается в реальность, принося конкретные выгоды. В то же время прогресс крайне неравномерен. Европейский союз выступает лидером, продемонстрировав целостный подход: сочетание общеевропейских нормативных инициатив и передовых технологий (*e-Curia, e-Justice,* видеоконференции) позволило вывести наднациональное правосудие ЕС на новый уровень удобства и открытости для пользователей. Евразийский экономический союз, имеющий схожую с ЕС задачу обеспечения единообразного применения права, находится лишь в начале пути цифровизации своего Суда. Основной вывод здесь: необходимы целенаправленные усилия по созданию нормативной основы электронного судопроизводства и внедрению технических решений, учитывающих лучшие мировые практики. При политической поддержке и совместной работе с национальными судебными органами внедрение электронного кабинета, системы электронного документооборота и дистанционных судебных заседаний в ЕАЭС вполне достижимо в обозримой перспективе. Это повысит эффективность интеграции, укрепит доверие бизнеса к правовой среде Союза и сократит издержки правоприменения. В МЕРКОСУР и АСЕАН ситуация иная: отсутствие постоянно действующих судебных механизмов не позволяет быстро продвигать цифровизацию судебных процессов на наднациональном уровне. Тем не менее оба объединения демонстрируют понимание важности цифровых технологий в правовой сфере: в МЕРКОСУР — через модернизацию процедур правовой помощи и возможное обновление правил арбитража, в АСЕАН — через активное взаимодействие глав судов, унификацию подходов к видеоконференциям и обмен знаниями. Эти шаги хотя и не заменяют полноценного электронного правосудия, но создают фундамент для более глубокого сотрудничества. В перспективе, по мере усиления интеграционных

процессов, МЕРКОСУР и АСЕАН смогут использовать наработанный ЕС и ЕАЭС опыт, минуя некоторые этапы методом технологического скачка.

Таким образом, главной рекомендацией для интеграционных объединений является необходимость стратегического планирования цифровизации правосудия. Это включает (а) развитие нормативной базы (от соглашений о взаимном признании электронных документов до изменений в учредительных договорах объединений); (б) инвестиции в общую или совместимую инфраструктуру (защищенные коммуникационные сети, порталы, базы данных); (в) обучение кадров и обмен лучшими практиками между странами; (г) постоянный контроль за тем, чтобы цифровые нововведения соответствовали принципам верховенства права и прав человека.

Для дальнейших исследований остаются открытыми вопросы, как именно цифровизация влияет на результаты правосудия (например, на качество судебных решений, процент обращаемости в наднациональные суды) и как измерить ее успех количественно. Перспективным направлением является изучение восприятия пользователями — гражданами и компаниями — электронных сервисов судов интеграционных объединений, а также анализ киберрисков в судебной сфере. Кроме того, заслуживает внимания проблема цифрового разрыва: как обеспечить равный доступ к электронному правосудию для всех государств-членов, учитывая различия в их техническом развитии.

В заключение отметим: цифровизация судебных процессов не панацея от всех проблем правосудия, но мощный инструмент, грамотное использование которого способно существенно повысить эффективность и справедливость судебных механизмов интеграционных группировок. Опыт ЕС, ЕАЭС, МЕРКОСУР и АСЕАН подтверждает, что при верном балансе технологий и права электронное правосудие становится важным фактором укрепления интеграции, облегчения реализации прав и продвижения верховенства закона в наднациональном масштабе.

Список литературы / References

1. Afanas'yev, S. F., Borisova, V. F., & Branovitskiy, K. L. (Eds.). (2022). *Tsifrovyye tekhnologii i yurisdiktsionnaya deyatel'nost': Obraz budushchego pravosudiya po grazhdanskim delam: Monografiya* [Digital technologies and jurisdictional activities: The future of civil justice: Monograph]. Statut.
2. Aleksandrov, O. B., & Butorina, O. V. (Eds.). (2016). *Evropeyskaya integratsiya* [European integration] (2nd ed.). Aspekt Press.
3. Anufriyeva, L. P., & Tolstykh, V. L. (Eds.). (2014). *Instituty mezhdunarodnogo pravosudiya: Uchebnoye posobiye* [Institutions of International Justice: A Study Guide]. Mezhdunarodnyye Otnosheniya.
4. Avila Paz de Robledo, R. A. (2007). Sistema de solución de controversias en el MERCOSUR bajo el régimen del Protocolo de Olivos, su reglamento con sus modificatorias y complementarias: Aspectos procesales [Dispute settlement system in MERCOSUR under the Olivos Protocol regime, its regulations with amendments and additions: Procedural aspects]. *Anuario del CIJS,* 308–328. https://www.corteidh.or.cr/tablas/r29555.pdf
5. Baimoldina, Z. K. (2025). Primeneniye informatsionnykh tekhnologiy v kazakhstanskom grazhdanskom sudoproizvodstve [Application of information technology in Kazakh civil proceedings]. *Digital Law Journal*, *5*(4), 41–54. https://doi.org/10.38044/2686-9136-2024-5-3
6. Belyakova, A. V. (2024). «Ob'yektivnaya istina» v usloviyakh «tsifrovogo» pravosudiya ["Objective truth" in the context of "digital" justice]. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia,* (5), 12–19. https://doi.org/10.24412/2073-0454-2024-5-12-19
7. Burdina, E. V., Zuyev, S. V. (Eds.). (2021). *Elektronnoye pravosudiye* [Electronic justice]. RGUP.
8. Diyachenko, E., & Entin, K. (2017). The Court of the Eurasian Economic Union: Challenges and perspectives. *Russian Law Journal*, *5*(2), 53–74. https://doi.org/10.52783/rlj.v5i2.94

9. Entin, K. V. (2020). *Pravo Evropeyskogo Soyuza skvoz' prizmu praktiki Suda Evropeyskogo Soyuza* [European Union law through the lens of the practice of the Court of Justice of the European Union]. Statut.
10. Entin, M. L. (1984). *Mezhdunarodnyye sudebnyye uchrezhdeniya: Rol' mezhdunarodnykh arbitrazhnykh i sudebnykh organov v razreshenii mezhgosudarstvennykh sporov* [International judicial institutions: The role of international arbitration and judicial bodies in resolving interstate disputes]. Mezhdunarodnyye Otnosheniya.
11. Entin, M. L. (1987). *Sud evropeyskikh soobshchestv: Pravovyye formy obespecheniya zapadnoyevropeyskoy integratsii* [Court of Justice of the European Communities: Legal forms of ensuring Western European integration]. Mezhdunarodnyye Otnosheniya.
12. Fabri, M. (2024). From court automation to e-Justice and beyond in Europe. *International Journal for Court Administration*, *15*(3). https://doi.org/10.36745/ijca.640
13. Globenko, O. A. (2021). Tsifrovizatsiya, sudebnaya diskretsiya, priroda pravosudiya: Eshche raz o probleme balansa [Digitalisation, judicial discretion, the nature of justice: Revisiting the issue of balance]. *Pravo i Gosudarstvo: Teoriya i Praktika*, *7*, 141–146.
14. Ispolinov, A. S. (2018). *Sudy regional'nykh integratsionnykh ob'yedineniy v sisteme mezhdunarodnogo pravosudiya (na primere suda ES i suda EAES)* [Courts of regional integration associations in the system of international justice (on example of the Court of justice of the EU and the Court of the EAEU)]. Yustitsinform.
15. Kalamkaryan, R. A. (2011). Mezhdunarodnyy sud OON: Stanovleniye i razvitiye [International court of Justice. Formation and evolution]. *Gosudarstvo i Pravo*, *5*, 62–71. https://doi.org/10.7868/S20000617-6-1
16. Kalamkaryan, R. A. (2012). *Mezhdunarodnyy sud v miroporyadke na osnove gospodstva prava* [International court in the world order based on the rule of law]. Nauka.
17. Kukartseva, A. N. (2023). Vliyaniye tsifrovizatsii na osushchestvleniye sudebnoy vlasti v Rossiyskoy Federatsii [The impact of digitalization on the exercise of judicial power in the Russian Federation]. *Vestnik Kemerovskogo Gosudarstvennogo Universiteta. Seriya: Gumanitarnyye I Obshchestvennyye Nauki*, *7*(1), 112–118. https://doi.org/10.21603/2542-1840-2023-7-1-112-118
18. Laptev, V. A., & Solovyanenko, N. I. (2021). *Tsifrovoe pravosudie. Tsifrovoi dokument* [Digital justice. Digital document]. Prospekt.
19. Le, T. A. T. (2025). The impact of digital transformation on economic integration in ASEAN-6: Evidence from a Generalized Least Squares (GLS) model. *Journal of Risk and Financial Management*, *18*(4), Article 189. https://doi.org/10.3390/jrfm18040189
20. Mikhaliova, T., & Vasilevich, G. (2023). Integration political and legal analysis of dispute resolution and prospects for digitalization of justice in the Eurasian Economic Union. *WISDOM*, *28*(4), 190–200. https://doi.org/10.24234/wisdom.v28i4.1089
21. Neshatayeva, T. N. (2017). Sud Evraziyskogo ekonomicheskogo soyuza: Ot pravovoy pozitsii k deystvuyushchemu pravu [Eurasian Economic Union Court: From legal position to applicable law]. *Mezhdunarodnoye Pravosudiye*, *2*, 64–79.
22. Neshatayeva, T. N. (2021). *Sud i pravo: Evraziyskaya integratsiya* [Justice and law: Eurasian integration]. Norma Infra-M.
23. Onţanu, E. A. (2023). (2020). The Digitalisation of European Union Procedures: A New Impetus Following a Time of Prolonged Crisis. *Law, Technology and Humans*, *5*(1), 93–110. https://doi.org/10.5204/lthj.2706
24. Pavlova, N. V. (2020). Rol' natsional'nogo pravosudiya v realizatsii prava Evraziyskogo ekonomicheskogo soyuza [The role of national justice in implementing the law of the Eurasian Economic Union]. In: N. N. Kulesh, A. S. Bugayeva, E. S. Orlova, E. E. Rafalyuk, E. E. Sadykov, A. A. Turekhanov, M. S. Shmelev (Eds.), *Pyat' let Dogovoru o Evraziyskom ekonomicheskom soyuze: rol' Suda: Mezhdunaraya konferentsiya (19–20 sentyabrya 2019 g., g. Minsk): sbornik materialov* (pp. 161–166). Medisont.

25. Reiling, D., & Contini, F. (2022). E-Justice platforms: Challenges for judicial governance. *International Journal for Court Administration*, *13*(1), Article 6. https://doi.org/10.36745/ijca.445
26. Sarpekov, R. K. (2020). O vzaimodeystvii Suda EAES s natsional'nymi organami gosudarstv — chlenov Soyuza (na primere Respubliki Kazakhstan): Praktika, problemy i puti dal'neyshego sovershenstvovaniya [On the interaction between the EAEU Court and the national authorities of the Union member states (using the Republic of Kazakhstan as an example): Practice, problems, and ways for further improvement]. In: N. N. Kulesh, A. S. Bugayeva, E. S. Orlova, E. E. Rafalyuk, E. E. Sadykov, A. A. Turekhanov, M. S. Shmelev (Eds.), *Pyat' let Dogovoru o Evraziyskom ekonomicheskom soyuze: rol' Suda: Mezhdunaraya konferentsiya (19–20 sentyabrya 2019 g., g. Minsk): sbornik materialov* (pp. 167–175). Medisont.
27. Schmidt-Kessen, M. J., Nogueira, R., & Cantero Gamito, M. (2020). Success or failure?—Effectiveness of consumer ODR platforms in Brazil and in the EU. *Journal of Consumer Policy*, *43*(3), 659–686. https://doi.org/10.1007/s10603-020-09448-y
28. Shinkaretskaya, G. G. (1992). *Mezhdunarodnaya sudebnaya protsedura* [International judicial procedure]. Nauka.
29. Shundikov, K. V. (2023). Iskusstvennyy intellekt v rossiyskom pravosudii: Sostoyaniye i perspektivy [Artificial intelligence in Russian justice: Status and prospects]. *Obrazovaniye i Pravo,* (8), 315–321. https://doi.org/10.24412/2076-1503-2023-8-315-321
30. Smbatyan, A. S. (2012). *Resheniya organov mezhdunarodnogo pravosudiya v sisteme mezhdunarodnogo publichnogo prava* [Decisions of international judicial bodies in the system of public international law]. Statut.
31. Szlak, G. R. (2012). Online dispute resolution in Latin America: Challenges and opportunities. In: M. A. Wahab, D. Rainey, & E. Katsh (Eds.), *Online dispute resolution: Theory and practice: A treatise on technology and dispute resolution* (pp. 529–559). Eleven International Publishing.
32. Tolstykh, V. L. (2015). *Mezhdunarodnyye sudy i ikh praktika: Uchebnoye posobiye* [International courts and their practice: A study guide]. Mezhdunarodnyye Otnosheniya.
33. Tolstykh, V. L. (2023). *Resheniya mezhdunarodnykh sudov: Treteyskiye sudy, Postoyannaya palata mezhdunarodnogo pravosudiya, Mezhdunarodnyy tribunal po morskomu pravu* [Judgements, advisory opinions and orders of international courts: Arbitration tribunals, Permanent Court of International Justice, International Tribunal for the Law of the Sea]. Mezhdunarodnyye Otnosheniya.
34. Zanin, V. E. (2023). Perspektivy razvitiya fenomena sudebnoy diskretsii v usloviyakh tsifrovizatsii: Kognitivnyy aspekt [The prospects for the development of the phenomenon of judicial discretion in the context of digitalization: A cognitive aspect]. *Pravo i Gosudarstvo: Teoriya i Praktika*, *7*, 103–106. https://doi.org/10.47643/1815-1337-2023-7-103

Сведения об авторе:

Тучина М. В. — преподаватель кафедры интеграционных процессов, Евразийский учебный институт, МГИМО МИД России, Москва, Россия.
m.tuchina@my.mgimo.ru
ORCID: https://orcid.org/0000-0003-1214-3108

Information about the author:

Maria V. Tuchina — Lecturer, Department of Integration Processes, Eurasian Studies Institute, MGIMO University, Moscow, Russia.
m.tuchina@my.mgimo.ru
ORCID: https://orcid.org/0000-0003-1214-3108

https://doi.org/10.38044/2686-9136-2025-6-11

СТАТЬИ

КОНВЕНЦИЯ ООН ПРОТИВ КИБЕРПРЕСТУПНОСТИ: ИСТОРИЯ И ПРАВОВЫЕ ПЕРСПЕКТИВЫ

Л. В. Божко[1,2]

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

[2]Райффайзенбанк
119002, Россия, Москва, пл. Смоленская-Сенная, 28

Аннотация

В результате стремительного развития информационных технологий и роста киберпреступности обеспечение международной информационной безопасности становится важнейшей задачей мирового сообщества. Статья анализирует перспективы принятой 24 декабря 2024 г. Конвенции ООН против киберпреступности как механизма координации усилий государств в области обеспечения международной информационной безопасности. Цель исследования заключается в оценке данного международного договора в качестве основы для сотрудничества государств в сфере международной информационной безопасности и противодействия киберпреступности. Особое внимание уделяется положениям Конвенции, касающимся обязанности государства криминализировать устанавливаемый договором перечень деяний, а также проблеме соблюдения прав человека в связи с ее применением. В ходе исследования автором были использованы историко-правовой, формально-юридический и сравнительно-правовой методы, в рамках которого были оценены отдельные аспекты международного и регионального регулирования киберпреступности. Эмпирическую основу статьи составляют нормативно-правовые акты и акты рекомендательного характера в сфере обеспечения международной информационной безопасности, а также юридическая доктрина, посвященная проблемам указанной отрасли. Выявленные результаты сводятся к следующему: принятие анализируемого международного договора является итогом балансирования противоположных позиций участников переговорного процесса относительно необходимости универсального регулирования кибербезопасности и озабоченности государств риском нарушения прав человека. Установлено, что, несмотря на преодоление спорных вопросов, Конвенция содержит существенные недостатки: высокая вероятность быстрой утраты актуальности вследствие сложности внесения изменений, риск расширительного толкования отдельных положений, что препятствует унификации практики, и в особенности отсутствие эффективного контрольного механизма для мониторинга исполнения обязательств. Автор приходит к выводу о важности принятия Конвенции, ставшей первым универсальным международным договором в области обеспечения международной информационной безопасности, отмечая при этом недостатки Конвенции и правовые риски, связанные со вступлением документа в силу.

Ключевые слова

международная информационная безопасность, киберпреступность, универсальное регулирование, информация, международный договор

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.
Для цитирования	Божко, Л. В. (2025). Конвенция ООН против киберпреступности: история и правовые перспективы. *Цифровое право, 6*(3), 149–164. https://doi.org/10.38044/2686-9136-2025-6-11

Поступила: 25.07.2025; принята в печать: 15.09.2025, опубликована: 30.09.2025

ARTICLES

UN CONVENTION AGAINST CYBERCRIME: HISTORY AND LEGAL PROSPECTS

Lada V. Bozhko[1,2]

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

[2]Raiffeisenbank
28, Smolenskaya-Sennaya Sq., Moscow, Russia, 119002

Abstract

As a result of the rapid development of information technology and associated increase in cybercrime, the need to ensure international information security has become a critical challenge for the global community. This article analyzes the prospects of the UN Convention against Cybercrime adopted on 24 December 2024 as a mechanism for coordinating the efforts of states in the field of international information security. The aim was to evaluate this international treaty as a basis for cooperation between states in the field of international information security and combating cybercrime. Particular attention is paid to the provisions of the Convention concerning the obligation of states to criminalize the list of acts established by the treaty, as well as ensuring human rights compliance in connection with its application. In the course of the study, the author used historical-legal, formal-legal, and comparative-legal methods to assess certain aspects of international and regional regulation of cybercrime. The empirical basis of the article comprises normative legal acts and those of a recommendatory nature in the field of international information security, as well as legal doctrine devoted to the problems of this industry. The findings can be summarized as follows: the adoption of the international treaty under analysis is an attempt to balance the opposing positions of the participants in the negotiation process regarding the need for universal regulation of cybersecurity with concerns about human rights violations. While the Convention sets out to resolve controversial issues, several significant shortcomings are identified, including a high probability of quickly becoming obsolete due to the complexity of carrying out amendments and the risk of permitting the broad interpretation of certain provisions, which hinders the unification of practice. In particular, the Convention lacks an effective control mechanism for monitoring the fulfilment of obligations. While noting these shortcomings and associated legal risks, the Convention represents the first universal international treaty in the field of international information security and can be recommended for adoption into force.

Keywords
international information security, cybercrime, universal regulation, information, international treaty

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Bozhko, L. V. (2025). The UN Convention against Cybercrime: History and legal prospects. *Digital Law Journal, 6*(3), 149–164. https://doi.org/10.38044/2686-9136-2025-6-11

Submitted: 25 July 2025, accepted: 15 Sept. 2025, published: 30 Sep. 2025

Введение

На современном этапе развития общества ключевая роль принадлежит информации. В связи с беспрецедентным ростом ее значения в современном мире необходимо уделять внимание всем аспектам ее использования. Цифровизация и развитие информационно-коммуникационных технологий породили множество угроз и вызовов для международного сообщества. В связи со сложной геополитической ситуацией особое значение приобретает использование информационного пространства в террористических целях, в целях разжигания межгосударственных конфликтов, вмешательства во внутренние дела государств посредством информационных кампаний, кибератак, мошенничества и т.д. Так, отмечается, что «технологии дезинформации активно использовались при подготовке вооруженных вторжений в Югославию (1999 г.), в Ирак (2003 г.), в Ливию (2011 г.) и в Сирию (2016 г.)» (Krutskikh et al., 2021, p. 18).

Вызовы, возникающие в связи с цифровизацией, носят транснациональный характер и требуют реакции как на национальном, так и на двустороннем и универсальном уровнях. Именно с этой целью 24 декабря 2024 г. была принята Конвенция Организации Объединенных Наций против киберпреступности[1]. Данный документ был воспринят неоднозначно и получил широкое обсуждение преимущественно в зарубежной доктрине: вопросам международной информационной безопасности и, в частности, роли данного международного договора в ее обеспечении посвящены работы таких авторов, как А. Ассаф (Assaf, 2023), Э. Шер-Цагир (Scher-Zagier, 2024). Среди отечественных авторов особое внимание Конвенции уделила Д. Д. Штодина (Shtodina, 2025). Так, актуальность настоящего исследования обосновывается неоднозначностью роли принятой Конвенции в области регулирования вопросов международной информационной безопасности и ростом транснациональных киберугроз (Gorelik, 2022, p. 32). Гипотеза исследования заключается в том, что, несмотря на значимость анализируемой Конвенции как первого шага

[1] Полное название конвенции — Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям. См.: U.N. Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, Dec. 24, 2024, U.N. Doc. A/RES/79/243, https://docs.un.org/ru/A/RES/79/243

к установлению универсального регулирования, этот документ не станет окончательным решением комплексных проблем международной информационной безопасности. Его ограниченная эффективность обусловлена сохраняющимися фундаментальными разногласиями государств — участников переговорного процесса.

История развития регулирования в области обеспечения международной информационной безопасности

Ключевой характеристикой существующего универсального регулирования в сфере международной информационной безопасности является рекомендательный характер принимаемых актов.

Основным регулятором выступает ООН, в рамках деятельности которой были приняты резолюции (в частности, резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 5 декабря 2018 г. № 73/27[2] и «Противодействие использованию информационно-коммуникационных технологий в преступных целях» от 17 декабря 2018 г. № 73/187[3]) и доклады Генерального секретаря (на ту же тему от 19 июля 2016 г. A/71/172[4], от 11 августа 2017 г. 72/315[5]).

Среди международных организаций, которые предпринимали шаги по решению проблемы информационной безопасности на региональном уровне, следует также выделить Совет Европы, в рамках которого была принята Конвенция о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.)[6] (далее — Будапештская конвенция). Среди недостатков данной конвенции особо подчеркивались положения ст. 32, позволяющие одной из сторон конвенции без согласия другой стороны получать доступ к ее компьютерным данным, а также несоответствие документа актуальным тенденциям и вызовам в области информационной безопасности[7].

Попытки ответить на вызовы цифровизации гармонизированным регулированием предпринимались также в рамках Содружества Независимых Государств[8], Организации Договора

[2] G.A. Res. 73/27 (Dec. 5, 2018), https://docs.un.org/ru/A/RES/73/27

[3] G.A. Res. 73/187 (Dec. 17, 2018), https://docs.un.org/ru/A/RES/73/187

[4] U.N. Secretary-General, *Developments in the field of information and telecommunications in the context of international security,* U.N. Doc. A/71/172 (July 19, 2016), https://docs.un.org/ru/A/71/172

[5] U.N. Secretary-General, *Developments in the field of information and telecommunications in the context of international security,* U.N. Doc. A/73/315 (Aug. 11, 2017), https://docs.un.org/ru/A/72/315

[6] Convention on Cybercrime, Mar. 1, 2002, ETS No. 185, 2296 U.N.T.S. 167, https://treaties.un.org/doc/Publication/UNTS/Volume%202296/v2296.pdf. См. неофициальный перевод: https://rm.coe.int/1680081580

[7] Толстухина, А. (2023, 14 сентября). *Российские инициативы в сфере международной информационной безопасности.* Российский Совет по международным делам. https://russiancouncil.ru/analytics-and-comments/analytics/rossiyskie-initsiativy-v-sfere-mezhdunarodnoy-informatsionnoy-bezopasnosti/?sphrase_id=126850521

[8] См., например: Совет глав государств Содружества Независимых Государств, Решение о Концепции сотрудничества государств — участников Содружества Независимых Государств в сфере обеспечения информационной безопасности и о Комплексном плане мероприятий по её реализации на период 2008–2010 годов (10 октября 2008 г.); Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в области обеспечения информационной безопасности (20 ноября 2013 г.), http://publication.pravo.gov.ru/Document/View/0001201506040007?index=1

о коллективной безопасности[9], БРИКС[10], Шанхайской организации сотрудничества[11], Организации по безопасности и сотрудничеству в Европе[12], Регионального форума Ассоциации государств Юго-Восточной Азии по безопасности[13] и «Группы восьми»[14].

Российская Федерация играет важнейшую роль в развитии регулирования в сфере информационной безопасности на универсальном уровне. Первым шагом в этом направлении стало письмо Постоянного представителя РФ при Организации Объединенных Наций на имя Генерального секретаря от 23 сентября 1998 г. (Boyko, 2023, p. 8), в котором было обращено внимание на необходимость предотвращения конфронтации в информационной среде. Затем Российская Федерация в декабре 1998 г. в Первом комитете Генеральной Ассамблеи ООН предложила проект резолюции «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности»[15], положивший начало практике ежегодных резолюций Генеральной Ассамблеи по данному вопросу.

Большой вклад в решение проблемы обеспечения международной информационной безопасности был внесен в рамках переговорных механизмов. Среди них Группа правительственных экспертов, начавшая работу в 2004 г. Результаты ее деятельности выразились в принятии докладов, посвященных анализу возможных угроз в международном информационном пространстве и способов их устранения: 2010[16],

[9] См., например, Соглашение о сотрудничестве государств — членов Организации Договора о коллективной безопасности в области разработки, производства, эксплуатации, ремонта, модернизации, продления сроков эксплуатации и утилизации продукции военного назначения (10 декабря 2010 г.), http://pravo.gov.ru/proxy/ips/?doc_itself=&backlink=1&&nd=201079109&&page=1&rdk=0#I0; Соглашение о сотрудничестве государств — членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности (Минск, 30 ноября 2017 г.), http://publication.pravo.gov.ru/document/0001201904260001?index=1

[10] См., например, BRICS, Sanya Declaration of 14 April 2011, https://brics.br/pt-br/documentos/acervo-de-presidencias-anteriores/leaders-declarations/2011-iii-bric-summit-sanya-declaration.pdf/@@download/file; BRICS, Johannesburg Declaration of 26 July 2018, https://brics.br/pt-br/documentos/acervo-de-presidencias-anteriores/leaders-declarations/2018-x-brics-summit-johannesburg-declaration.pdf/@@download/file

[11] См., например, Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, 16 июня 2009 г., Бюллетень международных договоров январь 2012, № 1, С. 13–21; Циндаоская декларация Совета глав государств-членов Шанхайской организации сотрудничества, 10 июня 2018 г., https://rus.sectsco.org/images/07e8/0b/1b/1603039.pdf

[12] См., например, Org. for Sec. & Co-operation in Eur. [OSCE], *Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, OSCE Doc. PC.DEC/1202 (Mar. 10, 2016), https://www.osce.org/sites/default/files/f/documents/d/a/227281.pdf; OSCE, *Efforts Related to Reducing the Risks of Conflict Stemming from the Use of Info. & Commc'n Tech,* OSCE Doc. MC.DEC/5/16 (Dec. 9, 2016), https://www.osce.org/sites/default/files/f/documents/2/8/288086.pdf

[13] См., например, Ass'n of Se. Asian Nations [ASEAN] & Russian Fed'n, Statement on Cooperation in the Field of Security of and in the Use of Info. & Commc'n Techs. (Nov. 14, 2018), https://asean.org/wp-content/uploads/2018/11/FINAL-Statement-of-ASEAN-and-the-Russian-Federation-on-Cooperation-in-the-Field-of-Security-of-and-in-the-Use-of-Information-and-Communication-Technologies.pdf

[14] См., например, Group of Eight [G8], Okinawa Charter on the Global Info. Soc'y (July 21, 2000).

[15] Russian Federation: draft resolution Developments in the field of information and telecommunications in the context of international security. U.N. Doc. A/C.1/56/L.3 (October 15, 2001), https://docs.un.org/ru/a/c.1/56/l.3

[16] Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, transmitted by Note dated 30 July 2010 from the Secretary-General. U.N. Doc. A/65/201 (July 30, 2010), https://docs.un.org/ru/A/65/201

2013[17], 2015[18] и 2021[19] гг. Еще одной важной площадкой для решения проблем в области международной информационной безопасности является Рабочая группа открытого состава ООН по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-телекоммуникационных технологий (далее — РГОС), созванная по инициативе Российской Федерации.

Существующий уровень регулирования наглядно демонстрирует острую необходимость создания юридически обязывающего многостороннего международного договора, который сможет закрепить минимальные стандарты защиты на основе выработанной единообразной практики государств и будет отвечать актуальным вызовам в данной области.

В этой связи 27 декабря 2019 г. Генеральной Ассамблеей ООН была принята Резолюция № 74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях», согласно которой Генеральная Ассамблея постановила «учредить специальный межправительственный комитет экспертов открытого состава, представляющий все регионы, для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях»[20].

Именно с этой целью на 77-й сессии Генеральной Ассамблеи ООН Российская Федерация предложила обновленную концепцию конвенции Организации Объединенных Наций по международной информационной безопасности (далее — Концепция)[21]. Соавторами инициативы выступили Республика Беларусь, Боливарианская Республика Венесуэла, Корейская Народно-Демократическая Республика, Республика Никарагуа и Сирийская Арабская Республика.

Предложенная в 2023 г. инициатива стала уже третьей попыткой Российской Федерации разрешить дискуссию об установлении регулирования международной информационной безопасности на универсальном уровне.

Впервые проект конвенции Организации Объединенных Наций по международной информационной безопасности Российская Федерация представила 22 сентября 2011 г. В рамках него предлагалось установить основные принципы обеспечения международной информационной безопасности. Несмотря на то, что в документе отмечалась приверженность принципам, закрепленным в международных договорах о правах человека, и сами положения не затрагивали национальный уровень регулирования, а лишь определяли общий вектор действий государств в области обеспечения международной информационной безопасности, проект был подвергнут критике со стороны стран Запада по причине

[17] Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, transmitted by Note dated 24 June 2013 from the Secretary-General. U.N. Doc. A/68/98* (June 24, 2013), https://undocs.org/ru/a/68/98

[18] Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, transmitted by Note dated 22 July 2015 from the Secretary-General. U.N. Doc A/70/174 (July 22, 2015), https://docs.un.org/ru/a/70/174

[19] Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, transmitted by Note dated 14 July 2021 from the Secretary-General. U.N. Doc A/70/174 (July 14, 2021), https://docs.un.org/ru/a/76/135

[20] G.A. Res. 74/247, at 3 (Dec. 27, 2019), https://docs.un.org/ru/A/Res/74/247

[21] Updated Concept for a Convention of the United Nations on Ensuring International Information Security, Letter dated May 15, 2023 from the Permanent Representatives of Belarus, the Democratic People's Republic of Korea, Nicaragua, the Russian Federation and the Syrian Arab Republic to the United Nations addressed to the Secretary-General, U.N. Doc. A/77/894 (May 16, 2023), https://docs.un.org/ru/A/77/894

возможного установления им чрезмерного контроля государства над информационным пространством[22].

Следующим шагом в данном направлении стал предложенный Российской Федерацией 11 октября 2017 г. проект конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности[23]. Инициатива охватывает аспекты криминализации и правоохранительной деятельности, а также общие принципы международного сотрудничества и взаимной помощи в области предупреждения и противодействия противоправным деяниям в информационном пространстве. Отличительной чертой данной инициативы можно считать закрепление обязательств государств установить во внутреннем законодательстве ответственность за ряд перечисленных в проекте деяний, среди которых, например, неправомерный доступ к информации в электронной форме, незаконный оборот устройств, сбор информации в электронной форме путем введения пользователя в заблуждение.

Российской Федерацией также был представлен проект конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях от 29 июня 2021 г.[24] Данный проект также подчеркивает приверженность принципу уважения прав и свобод человека, а также принципу суверенитета государств, в частности в киберпространстве. Инициатива предлагает закрепить обязательства государств по криминализации 23 деяний, среди которых, в частности, незаконное распространение фальсифицированных лекарственных средств и медицинских изделий, преступления, связанные с распространением наркотических средств и психотропных веществ, подстрекательство к подрывной или вооруженной деятельности и т. д.

Впрочем, предлагаемые инициативы не были приняты в качестве основы для международного договора в рамках ООН. Указанные проекты подвергались критике со стороны иных государств — участников ООН, в частности по причине риска широкого толкования положений, что может нанести ущерб законной деятельности журналистов и других лиц, работающих в сфере информации и связи, а также повлечь иные нарушения прав человека[25].

В свою очередь в ранее упомянутой нами обновленной Концепции были сохранены основные принципы предыдущих инициатив, однако документ подвергся изменениям в связи с активной критикой его положений. Важнейшим достижением инициатив Российской Федерации является приверженность единообразной практике, выработанной государствами. Так, Концепция основана на «рекомендациях ежегодных резолюций Генеральной Ассамблеи ООН "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности", а также консенсусных докладов профильной Рабочей группы открытого состава

---

22 Черненко, Е. (2023, 21 мая). Третья пошла. Россия внесла на рассмотрение ООН новый проект конвенции по международной информационной безопасности. Коммерсантъ. https://www.kommersant.ru/doc/5999161

23 Draft United Nations Convention on Cooperation in Combating Cybercrime, in Letter dated Oct. 11, 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, U.N. Doc. A/C.3/72/12* (Oct. 16, 2017), https://docs.un.org/en/A/C.3/72/12

24 Ad Hoc Комитет ООН по разработке Конвенции против киберпреступности. (2021, 29 июня). *Проект конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях.* https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf

25 Office of the High Commissioner on Human Rights. (2022, January 17). *Key-messages Relating to a Possible Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.* United Nations. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf

(РГОС) ООН 2021 года и групп правительственных экспертов 2010, 2013, 2015 и 2021 годов»[26]. Кроме того, она содержит ссылки на акты, выработанные как на универсальном, так и на региональном уровнях.

Целью конвенции, согласно проекту, является формирование «системы обеспечения международной информационной безопасности на основе равноправного сотрудничества между государствами в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий»[27].

Концепция предлагает закрепить принципы предотвращения и урегулирования межгосударственных конфликтов в глобальном информационном пространстве, стремление к развитию сотрудничества в области обеспечения международной информационной безопасности и содействию наращиванию потенциала государств в данной области.

Достоинством Концепции является также положение о необходимости создания механизмов контроля за исполнением государствами положений конвенции, а также механизмов урегулирования и разрешения споров. В качестве образца предлагаются «постоянно действующие органы с участием всех государств, присоединившихся к конвенции, либо обзорные конференции, созываемые на регулярной основе»[28].

Несмотря на высокий уровень разработанности документа, нужно отметить ряд недостатков. В первую очередь к недостаткам Концепции следует отнести низкий уровень конкретизированности и «мягкость» обязательств. Критика предыдущих проектов конвенции на международной арене привела к отказу от закрепления четких обязательств государств, в частности по криминализации определенных деяний. С учетом сложной геополитической ситуации такой шаг был необходим, однако он привел к отдалению от первоначально поставленной цели — создания юридически обязывающего международного договора, который приведет к формированию эффективного универсального регулирования. Во вторую очередь недостатком Концепции является узкий круг ее потенциальных участников: среди соавторов Российской Федерации Республика Беларусь, Боливарианская Республика Венесуэла, Корейская Народно-Демократическая Республика, Республика Никарагуа, Сирийская Арабская Республика. Государства, играющие ключевую роль в обеспечении международной информационной безопасности, являются противниками Концепции.

Анализ Конвенции ООН против киберпреступности

Финалом дискуссии вокруг проекта конвенции стало принятие Резолюцией Генеральной Ассамблеей от 24 декабря 2024 г. 79/243 Конвенции Организации Объединенных Наций против киберпреступности[29]. На 25 августа 2025 г. Конвенция еще не начала действовать, поскольку в соответствии со ст. 65(1) дата вступления ее в силу привязана к дате сдачи на хранение

[26] Updated concept for a convention of the United Nations on ensuring international information security, in Letter dated May, 15 2023 from the Permanent Representatives of Belarus, the Democratic People's Republic of Korea, Nicaragua, the Russian Federation and the Syrian Arab Republic to the United Nations addressed to the Secretary-General, U.N. Doc. A/77/894 (May 16, 2023), https://docs.un.org/ru/A/77/894

[27] Ibid.

[28] Ibid.

[29] U.N. Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, Dec. 24, 2024, U.N. Doc. A/RES/79/243, https://docs.un.org/ru/A/RES/79/243

40-й ратификационной грамоты или документа о принятии, утверждении или присоединении[30]. Можно отметить риск невступления Конвенции в силу в связи с обилием противоречий, связанных с текстом и объектом документа. Предметом споров, в частности, стало и название Конвенции. Вариант, принятый Резолюцией, стал своего рода компромиссом, объединив широкий круг преступлений, совершаемых с использованием информационно-коммуникационных систем, а также отразив фокус на киберпреступности, за который выступали оппоненты Российской Федерации в дискуссии вокруг текста Конвенции[31].

Вопрос названия связан с охватом Конвенцией деяний, которые государства-участники должны будут криминализировать в результате присоединения к документу. Как было упомянуто ранее, Российская Федерация предлагала 23 состава, тогда как финальная версия Конвенции содержит лишь одиннадцать:

1) незаконный доступ;
2) незаконный перехват;
3) воздействие на электронные данные;
4) воздействие на информационно-коммуникационную систему;
5) неправомерное использование устройств;
6) подлог с использованием информационно-коммуникационной системы;
7) хищение или мошенничество с использованием информационно-коммуникационной системы;
8) преступления, связанные с размещением в Интернете материалов со сценами сексуальных надругательств над детьми или их сексуальной эксплуатации,
9) домогательство или создание доверительных отношений с целью совершения сексуального преступления в отношении ребенка;
10) распространение интимных изображений без согласия; и
11) отмывание доходов от преступлений.

При этом возможность дальнейшего расширения перечня осложняется не только разнополярностью позиций договаривающихся государств, но и тем, что обязательным требованием для принятия дополнительного протокола является наличие не менее 60 государств — участников договора. Не менее труднореализуема и процедура внесения поправок, которая предполагает истечение пяти лет после вступления Конвенции в силу. Следует также отметить, что особенностью сферы информационной безопасности является быстрота изменений, в связи с чем сложность внесения поправок и длительные сроки особенно ощутимы для обеспечения эффективности регулирования.

Помимо сокращения перечня криминализируемых деяний, в юридической доктрине выделяют также иные недостатки Конвенции. Так, Д. Д. Штодина в качестве лакун документа указывает вопросы реализации пассивного персонального принципа установления юрисдикции и защиты персональных данных пользователей Интернета (Shtodina, 2025, p. 118). Согласно пассивному персональному принципу определяющим фактором для установления государством

---

30 U.N. Convention against Cybercrime, art. 65, ¶ 1.

31 Черненко, Е. (2024, 30 июля). Киберчувствительная тема. Проект конвенции ООН по борьбе с компьютерной преступностью не нравится ни России, ни ее оппонентам. *Коммерсантъ*. https://www.kommersant.ru/doc/6864552?query=%D0%9A%D0%BE%D0%BD%D0%B2%D0%B5%D0%BD%D1%86%D0%B8%D1%8F%20%D0%BF%D0%BE%20%D0%BC%D0%B5%D0%B6%D0%B4%D1%83%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%BE%D0%B9%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9%20%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8

юрисдикции является гражданство жертвы преступления. В ходе переговорного процесса Российская Федерация, а также Иран, Кабо-Верде, Пакистан, Панама, Эритрея и Сирия предлагали распространить данный принцип также на случаи совершения противоправных деяний в отношении юридических лиц, учрежденных или имеющих постоянное представительство на территории государства, устанавливающего свою юрисдикцию. Возможность установления данного принципа в отношении преступлений против международной информационной безопасности была раскритикована в связи с риском расширительного толкования, вызванным отсутствием в Конвенции ограничений данного положения (Scher-Zagier, 2024, p. 366). Тогда как Комиссия международного права в отчете от 2006 года[32] пришла к выводу о том, что на национальном уровне государства ограничивают область применения пассивного персонального принципа перечнем наиболее тяжких преступлений, среди которых, в частности, терроризм. Среди иных ограничительных условий также применяется требование двойной криминализации, применение данного принципа только в отношении преступлений, предусматривающих минимальную меру наказания (Watson, 1993, p. 23), отказ государства, которое могло бы установить свою юрисдикцию на основании территориального принципа (McCarthy, 1989, p. 24).

Необходимо отметить, что положение о возможности применения пассивного персонального принципа было основано на аналогичной норме Конвенции ООН против транснациональной организованной преступности (принята резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года[33]) (далее — Конвенция против транснациональной организованной преступности)[34], и Конвенции ООН против коррупции (принята резолюцией 58/4 Генеральной Ассамблеи от 31 октября 2003 года[35]) (далее — Конвенция против коррупции)[36]. Для конференций государств-участников анализируемых конвенций функции секретариата выполняет Управление Организации Объединенных Наций по наркотикам и преступности (далее — УНП ООН), которое при разработке Конвенции против киберпреступности подготовило обзор существующих источников правового регулирования в области обеспечения международной информационной безопасности[37], при этом включив туда как Конвенцию против транснациональной организованной преступности, так и Конвенцию против коррупции, отмечая, однако, что объектом их регулирования являются иные правоотношения. Так, статья 15 Конвенции против транснациональной организованной преступности закрепила возможность государств установить свою юрисдикцию в отношении любого преступления, которое совершено против гражданина этого государства[38]. Конвенция против коррупции в статье 42 также устанавливает возможность применения принципа пассивной юрисдикции, не закрепляя при этом ограничительных условий[39]. США, комментируя выбор Конвенции против коррупции в качестве основы

[32] Report of the International Law Commission to the General Assembly, 2006, U.N. GAOR Supp. No. 10, at 524 n. 23, U.N. Doc. A/61/10.

[33] G.A. Res. 55/25, United Nations Convention Against Transnational Organized Crime (Nov. 15, 2000).

[34] United Nations Convention Against Transnational Organized Crime, Nov. 15, 2000, 2225 U.N.T.S. 209.

[35] G.A. Res. 58/4, United Nations Convention Against Corruption (Oct. 31, 2003).

[36] United Nations Convention Against Corruption, Oct. 31, 2003, 2349 U.N.T.S. 41.

[37] United Nations Office on Drugs and Crime Secretariat, Overview of Existing Instruments, Recommendations and Other Documents on Countering the Use of Information and Communications Technologies for Criminal Purposes, Apr. 20, 2022, U.N. Doc. A/AC.291/CRP.10.

[38] United Nations Convention Against Transnational Organized Crime, art. 15.

[39] United Nations Convention Against Corruption, art. 42.

для разработки универсального источника регулирования проблемы обеспечения международной информационной безопасности, отмечали, что процесс разработки данного международного договора был более длительным и был инициирован на основе консенсуса государств, чего в данном случае нет[40].

При этом Э. Шер-Цагир отмечает, что Конвенция против транснациональной организованной преступности и Конвенция против коррупции все же представляют собой пример ограничительного использования пассивного персонального принципа. Так, объект регулирования Конвенции против транснациональной организованной преступности предполагает наличие таких ограничительных условий как определенная структура, период действия и цель преступных групп. Возможность применения пассивного персонального принципа в соответствии с Конвенцией против коррупции может рассматриваться как частное проявление защитного принципа установления юрисдикции, поскольку объект ее регулирования тесно связан с ключевыми интересами государства (Scher-Zagier, 2024, p. 364).

Данный принцип установления юрисдикции становится предметом критики не в первый раз. Так, Седрик Рейнгарт утверждает, что данный принцип установления юрисдикции не выполняет сдерживающей, превентивной функции, являющейся основной в уголовном праве. Это объясняется тем, что преступник не может предвидеть, какое государство установит юрисдикцию, поскольку он будет обычно не знает национальности жертвы (Ryngaert, 2015, p. 110). Еще Доннедье де Вабр подчеркивал, что применение принципа пассивной персональной юрисдикции лишь усиливает противоречия государств по вопросам установления юрисдикции (Donnedieu de Vabres, 1928, p. 170).

Однако критика использования пассивного персонального принципа представляется недостаточно обоснованной. Данный принцип не противоречит превентивной функции уголовного права, поскольку она связана в первую очередь с наличием ответственности за совершенное противоправное деяние, а невозможность спрогнозировать формы ее реализации может служить лишь дополнительным усиливающим сдерживающий характер фактором. При этом, интерес государства гражданства жертвы представляется обоснованным и правомерным, поскольку является следствием факта нарушения прав его гражданина. Что касается ограничительных условий применения пассивного персонального принципа, Конвенция против киберпреступности в качестве обязательств государств-участников устанавливает криминализацию указанных в ней деяний, что представляет собой требование двойной криминализации, являющееся одним из проявлений ограничительных условий[41]. Кроме того, перечень деяний, которые государства должны признать в качестве уголовного правонарушения в соответствии с Конвенцией против киберпреступности, является ограниченным и не может толковаться расширительно. Наличие таких ограничительных положений, а также закрепленное в договоре требование выполнения обязательств в соответствии с принципами суверенного равенства и территориальной целостности государств и принципом невмешательства во внутренние дела других государств[42] позволяют сделать вывод о чрезмерности опасений противников применения такого принципа.

---

40 United States of America, “Implementation of Operative Paragraph 3 of General Assembly Resolution 74/247 and Next Steps”, Apr. 20, 2020, U.N. Doc. A/AC.291/CRP, (Ad Hoc Comm. to Elaborate a Comprehensive Int’l Convention on Countering the Use of ICTs for Criminal Purposes), available at https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/USA.pdf

41 U.N. Convention against Cybercrime, art. 7–17.

42 Ibid., art. 5.

Что касается защиты персональных данных, предметом критики выступили положения Конвенции о сборе доказательств: предлагалось закрепить возможность передачи данных только «в случае наличия серьезных оснований полагать, что преступление носит "серьезный характер"» (Shtodina, 2025, p. 122). Однако необходимо отметить, что существующая в Конвенции формулировка, позволяющая сбор доказательств по уголовным правонарушениям в соответствии с Конвенцией[43], решает проблему Будапештской конвенции, закрепляющей возможность доступа к данным без согласия другой стороны[44]. Соответствующее положение Будапештской конвенции с точки зрения отечественной доктрины «фактически представляет собой норму, регламентирующую не что иное, как обыск в компьютерных сетях (или в среде для хранения компьютерных данных) за рубежом с целью обнаружения и изъятия искомой компьютерной информации» (Volevodz, 2007, p. 25), а также влечет риск нарушения фундаментальных прав и свобод человека в цифровой среде (Danel'yan, 2020, p. 265).

Существенным недостатком Конвенции является отсутствие контрольного механизма, который предлагала закрепить Российская Федерация. С целью эффективного контроля за исполнением положений документа представляется оптимальным создание договорного органа или специальной процедуры Совета по правам человека. В качестве примера эффективно функционирующих договорных механизмов можно привести десять органов ООН по правам человека (Abashidze & Koneva, 2015, p. 14). Среди них, в частности, Комитет по правам ребенка, который наблюдает за выполнением Конвенции о правах ребенка 1989 г.[45] и двух факультативных протоколов к ней, касающихся сексуальной эксплуатации детей, их участия в вооруженных конфликтах, а также торговли детьми[46]. Однако, помимо договорных органов, мониторинг и привлечение внимания к актуальным нарушениям прав человека также может эффективно осуществляться посредством деятельности специальных процедур Совета по правам человека. Так, деятельность специального докладчика по вопросу о рабстве способствовала привлечению внимания международного сообщества к проблеме создания незаконного онлайн-рынка рабского труда крупными технологическими компаниями[47]. Создание подобного механизма в рамках принятой Конвенции против киберпреступности позволило бы отслеживать существующую ситуацию в области международной информационной безопасности, контролировать соблюдение государствами-участниками Конвенции и выявлять соответствующие нарушения.

В зарубежной доктрине Конвенция подверглась критике преимущественно в части положений, посвященных международному сотрудничеству (Tropina, 2024, p. 220; Tennant & Oliveira, 2024, p. 238). Так, К. Родригес характеризует данную главу документа как «главу о трансграничном шпионаже» и отмечает, что сфера действия статьи 24 Конвенции, устанавливающей обязанность государств обеспечивать защиту прав человека и действовать в соответствии с принципом соразмерности[48], ограничивается областью применения процессуальных мер

[43] U.N. Convention against Cybercrime, art. 23.

[44] Convention on Cybercrime, art. 32(b), Mar. 1, 2002, ETS No. 185, 2296 U.N.T.S. 167, https://treaties.un.org/doc/Publication/UNTS/Volume%202296/v2296.pdf

[45] Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.

[46] *See,* Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict, May 25, 2000, 2173 U.N.T.S. 222; Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, May 25, 2000, 2171 U.N.T.S. 227.

[47] Совет по правам человека. (б.д.). *Результаты работы Специальных процедур: предупреждение и/или прекращение нарушений прав человека.* По обращению 24 июля 2025 к https://www.ohchr.org/ru/special-procedures-human-rights-council/impact-work-special-procedures-prevention-andor-cessation-human-rights-violations

[48] U.N. Convention against Cybercrime, art. 24.

согласно Конвенции и не распространяется на международное сотрудничество государств[49]. Следует подчеркнуть, что данный довод представляется необоснованным: необходимость уважения и защиты прав человека, в том числе в ходе международного сотрудничества государств в рамках исполнения обязательств, вытекающих из Конвенции, закреплена в ст. 6 Конвенции[50]. В ходе переговорного процесса ряд стран, в том числе Новая Зеландия, Вануату, Норвегия и Лихтенштейн, предлагали внести в статью 35 Конвенции, посвященную общим принципам международного сотрудничества[51], положение, которое могло бы стать дополнительной гарантией защиты прав человека[52]. Предложение содержало формулировку, позволяющую государству отказать в исполнении запроса о международном сотрудничестве, если есть веские основания полагать, что такой запрос был сделан с целью преследования или наказания лица по признаку пола, расы, языка, религии, национальности, этнического происхождения или политических убеждений или что выполнение запроса нанесет ущерб положению этого лица по любой из этих причин. Однако указанное предложение не было учтено в финальной редакции Конвенции.

Следует также отметить иной недостаток Конвенции, которому уделяет внимание К. Родригес[53]. Конвенция не содержит определений ключевых для данной сферы понятий: «данные» и «информация». Их отсутствие может повлечь расширительное толкование положений документа, что несет в себе риски для обеспечения надлежащего уровня защиты персональных данных и конфиденциальной информации.

Скорость разработки документа выделяется в качестве одной из причин существующих недостатков Конвенции: поскольку участники переговорного процесса были вынуждены сосредоточить внимание на согласовании наиболее дискуссионных условий договора, ряд положений не был надлежащим образом разработан. Так, Э. Шер-Цагир обращает внимание на процесс разработки анализируемого международного договора: график включал всего семь сессий переговоров менее чем за два года (Scher-Zagier, 2024, p. 346). Так, именно с этим автор связывает проблему применения пассивного персонального принципа установления юрисдикции в соответствии с Конвенцией. Однако мы не можем согласиться с данной позицией, поскольку работа по разработке международного договора в области обеспечения международной информационной безопасности ведется на протяжении длительного периода времени, и разногласия государств обусловлены не недостаточной продолжительностью дискуссий, а концептуальными различиями подходов и конфликтом политических интересов.

На момент написания статьи работа по созданию системы регламентации в области обеспечения международной безопасности продолжается. В Нью-Йорке 7 июля 2025 г. открылась финальная сессия РГОС, по результатам который должен быть подготовлен доклад, отражающий общую позицию международного сообщества в области обеспечения международной

---

[49] Rodriguez, K. (2023, August 22). *Proposed UN Cybercrime Treaty threatens to be an expansive global surveillance pact*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2023/08/proposed-un-cybercrime-treaty-threatens-be-expansive-global-surveillance-pact

[50] U.N. Convention against Cybercrime, art. 6.

[51] Ibid., art. 35.

[52] Draft text of the convention with the amendments made by Member States. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Sixth session. New York, 21 August — 1 September 2023. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_01.09.2023_PM.pdf

[53] Rodriguez, K. Op. cit.

информационной безопасности[54]. Работа РГОС приведет к принятию доклада, нового акта рекомендательного характера, лишь косвенно способствуя формированию системы юридически обязывающего регулирования в данной сфере.

Заключение

Таким образом, гипотеза исследования подтвердилась. Конвенция стала первым международным юридически обязывающим актом в сфере международной информационной безопасности, выступая в роли необходимого, но промежуточного этапа, поскольку присущие ей существенные недостатки не позволяют ей полностью решить комплексные вызовы безопасности в динамично развивающемся киберпространстве. Как результат длительной дискуссии, она является компромиссом между позициями Российской Федерации и иных государств, выступающих за необходимость универсального регулирования в данной области, и их оппонентов, которые видят в этом риск нарушения прав человека и злоупотреблений государствами. Несмотря на то, что опасения государств, связанные с возможностью использования документа как инструмента слежки, представляются преувеличенными, принятый в 2024 г. международный договор все же обладает рядом недостатков.

Во-первых, Конвенция отличается трудностью внесения изменений, что, в свою очередь, порождает риск неактуальности положений договора в связи с развитием информационных технологий.

Во-вторых, недостатком является возможность расширительного толкования отдельных положений Конвенции, к числу которых относятся, в частности, отсутствие определений понятий «данные» и «информация» и вопросы сбора доказательств. Вероятно, причина этому — необходимость согласования разнополярных позиций договаривающихся государств. Однако широта формулировок не может считаться решением данной проблемы, поскольку позволяет государствам самостоятельно толковать указанные положения, что препятствует достижению цели Конвенции — закреплению единообразной практики.

В-третьих, существенным недостатком данного международного договора является отсутствие механизмов контроля за исполнением его положений.

В-четвертых, можно поставить под сомнение само вступление Конвенции в силу в связи с необходимостью внесения 40 ратификационных грамот или документов о принятии, утверждении или присоединении на фоне не устраненных до конца противоречий в позициях договаривающихся государств.

Несовершенство Конвенции, продолжительность дискуссий, полярность позиций, обилие критики приводят к возникновению более глобального вопроса, способного послужить предметом отдельного исследования, — о том, каким должно быть регулирование международной информационной безопасности. В результате анализа существующего регулирования можно предположить, что наиболее эффективным путем его развития стало бы сочетание рамочного международного договора и актов рекомендательного характера. Эффективное регулирование недостижимо без закрепления обязательств, что реализуемо именно посредством заключения международного договора. Однако с учетом быстроты изменений в данной сфере представляется невозможным исчерпывающим образом охватить

[54] Черненко, Е. (2025, 7 июля). Цифровую ответственность оформят докладом. На площадке ООН вновь обсудят правила поведения государств в киберпространстве. *Коммерсантъ*. https://www.kommersant.ru/doc/7871382

все требующие регламентации области посредством заключения международного договора. Акты рекомендательного характера представляют собой более гибкий механизм, способный отражать актуальные тенденции отрасли. Так, Конвенция не стала финалом дискуссии о регулировании информационной безопасности на универсальном уровне, но выступила важнейшим шагом в этом направлении.

Список литературы / References

1. Abashidze A. Kh., & Koneva A. E. (2015). *Dogovornye organy po pravam cheloveka: uchebnoe posobie* [Human rights treaty bodies: A study guide] (2nd ed.). RUDN.
2. Assaf, A. (2023). Violations of sovereignty in "cyberspace" under the United Nations Charter. *Zhurnal VSHÉ po Mezhdunarodnomu Pravu* [*HSE University Journal of International Law*], *1*(3), 4–20. https://doi.org/10.17323/jil.2023.18848
3. Boyko, S. M. (2023). Mezhdunarodnaya informatsionnaya bezopasnost': Rossiya v OON. Nachalo istorii (1998-2009 gg.) [International information security: Russia at the United Nations. The beginning of the story (1998–2009)]. *Mezhdunarodnaya Zhizn'*, (11), 8–23.
4. Danel'yan, A. A. (2020). Mezhdunarodno-pravovoe regulirovanie kiberprostranstva [International legal regulation of cyberspace]. *Obrazovanie i Pravo*, (1), 261–269. https://doi.org/10.24411/2076-1503-2020-10140
5. Donnedieu de Vabres, H. (1928). *Les principes modernes du droit pénal international* [Modern principles of international criminal law]. Librairie du Recueil Sirey.
6. Gorelik, I. B. (2022). Rol' mezhdunarodnykh organizatsiy v protsesse protivodeystviya kiberprestupnosti [The role of international organizations in the process of countering cybercrime]. *Mezhdunarodnoe Pravo*, (3), 28–41. https://doi.org/10.25136/2644-5514.2022.3.38585
7. Krutskikh, A. V., Biryukov A. V., Boyko, S. M., Volkova, S. G., Zinovieva, E. S., Zinchenko, A. V., Matyukhin, D. V., & Smirnov, A. I. (2021). *Mezhdunarodnaya informatsionnaya bezopasnost': Teoriya i praktika: Uchebnik v trekh tomakh. T. 2.* [*International information security: Theory and practice: Textbook* (Vol. 2; 2nd ed.)]. Aspekt Press.
8. McCarthy, J. G. (1989). The passive personality principle and its use in combatting international terrorism. *Fordham International Law Journal*, *13*(3), 298–327.
9. Ryngaert, C. M. J. (2015). *Jurisdiction in international law* (2nd ed.). Oxford University Press.
10. Scher-Zagier, E. (2025). Jurisdictional creep: The UN Cybercrime Convention and the expansion of passive personality jurisdition. *Yale Journal of Law & Technology, 27*(1), 327–389.
11. Shtodina, D. D. (2025). Konventsiya Organizatsii Ob'yedinennykh Natsiy protiv kiberprestupnosti 2024 goda — itog "kiberkompromissa"? [United Nations Convention against Cybercrime, 2024 — the outcome of «cyber compromise»?] *Moskovskij Zhurnal Mezhdunarodnogo Prava*, (1), 110–124. https://doi.org/10.24833/0869-0049-2025-1-110-124
12. Tennant, I., & Oliveira, A. P. (2024). Applying the right lessons from the negotiation and implementation of the UNTOC and the UNCAC to the implementation of the newly agreed UN 'cybercrime' treaty. *Journal of Cyber Policy*, *9*(2), 221–238. https://doi.org/10.1080/23738871.2024.2428655
13. Tropina T. (2024). 'This is not a human rights convention!': The perils of overlooking human rights in the UN cybercrime treaty. *Journal of Cyber Policy*, *9*(2), 200–220. https://doi.org/10.1080/23738871.2024.2419517
14. Volevodz, A. G. (2007). Konventsiya o kiberprestupnosti: novatsii pravovogo regulirovaniya [The Convention on cybercrime: Innovations in legal regulation]. *Pravovye Voprosy Svyazi*, (2), 17–25.
15. Watson, G. R. (1993). The passive personality principle. *Texas International Law Journal*, *28*(1), 1–46.

Сведения об авторе:

Божко Л. В. — магистрант, международно-правовой факультет, МГИМО МИД России, юрист отдела сопровождения корпоративного бизнеса и банковской деятельности, АО «Райффайзенбанк», Москва, Россия.
lada-bozhko@mail.ru
ORCID: https://orcid.org/0009-0002-2637-170X

Information about the author:

Lada V. Bozhko — Master's student, International Law Faculty, Moscow State Institute of International Relations, lawyer in the Corporate Business and Banking Support Department, Raiffeisenbank JSC, Moscow, Russia.
lada-bozhko@mail.ru
ORCID: https://orcid.org/0009-0002-2637-170X