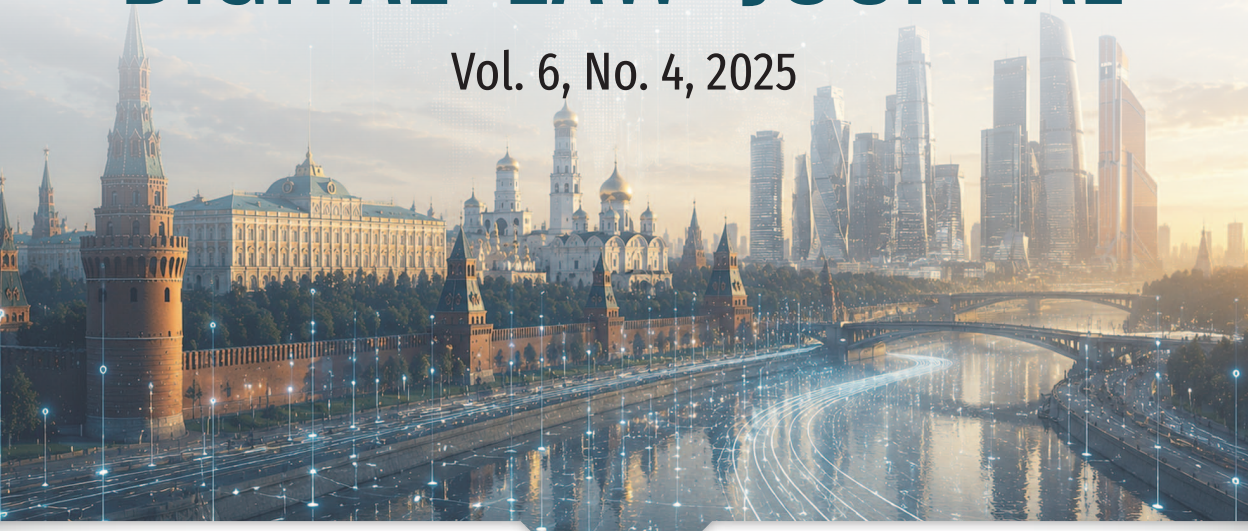
ISSN 2686-9136 (Online)

DIGITAL LAW JOURNAL

Vol. 6, No. 4, 2025



ESSAYS

8 Legal Mechanisms for Digital Content Moderation on HR Tech Platforms
Svetlana E. Shabronova

ARTICLES

21 Current Digital Dimensions of the EU Area of Freedom, Security and Justice
Vadim V. Voynikov, Alexander V. Arestov

43 Domain Name: Digital Asset, Identifier, or Some Other Kind of Object?
Ilya E. Titov, Ekaterina V. Alymova

82 Artificial Intelligence and Liability: Exploring Legal Challenges and Responsibility in AI Decision-Making and Autonomous Systems
Kolawole O. Afuwape

NOTES

101 Legal Framework of Platform Employment in Russia: Outcomes and Prospects of Reform
Iraida S. Semyonova

DIGITAL LAW JOURNAL

DIGITAL LAW JOURNAL

Journal of research and practice

Published since 2020
4 issues per year

Vol. 6, No. 4, 2025

ЦИФРОВОЕ ПРАВО

Научно-практический журнал

Журнал издается с 2020 г.
4 выпуска в год

Том 6, № 4, 2025

Contents

Essays

8 Legal Mechanisms for Digital Content Moderation on HR Tech Platforms
Svetlana E. Shabronova

Articles

21 Current Digital Dimensions of the EU Area of Freedom, Security and Justice
Vadim V. Voynikov, Alexander V. Arestov

43 Domain Name: Digital Asset, Identifier, or Some Other Kind of Object?
Ilya E. Titov, Ekaterina V. Alymova

82 Artificial Intelligence and Liability: Exploring Legal Challenges and Responsibility in AI Decision-Making and Autonomous Systems
Kolawole O. Afuwape

Notes

101 Legal Framework of Platform Employment in Russia: Outcomes and Prospects of Reform
Iraida S. Semyonova

Содержание

Эссе

8 Правовые механизмы цифровой модерации контента на HR-Tech платформах

Светлана Шабронова

Статьи

21 Цифровое измерение пространства свободы, безопасности и правосудия ЕС на современном этапе

Вадим Войников, Александр Арестов

43 Доменное имя: цифровой актив, идентификатор или иной объект?

Илья Титов, Екатерина Алымова

82 Ответственность искусственного интеллекта: правовые вызовы в процессе принятия решений с помощью ИИ и автономных систем

Колаволе Афувапе

Заметки

101 Правовое оформление платформенной занятости: итоги и перспективы реформы

Ираида Семенова

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 December 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:	30.12.2025
Копирайт:	© Цифровое право, 2025
Цена:	Бесплатное распространение

РЕГИОН ГРУППА КОМПАНИЙ При поддержке Группы компаний «РЕГИОН»

https://doi.org/10.38044/2686-9136-2025-6-19

ЭССЕ

ПРАВОВЫЕ МЕХАНИЗМЫ ЦИФРОВОЙ МОДЕРАЦИИ КОНТЕНТА НА HR-TECH ПЛАТФОРМАХ

С. Е. Шабронова

ООО «Хэдхантер»
125047, Россия, Москва, ул. Вторая Брестская, 48

Аннотация

Эссе посвящено анализу правовых механизмов цифровой модерации контента на *HR-tech*-платформах как элемента современной инфраструктуры регулирования цифрового рынка труда. В условиях цифровизации платформы перестают быть исключительно техническими посредниками и всё чаще выполняют функции частного регулирования. В этом контексте особое значение приобретает модерация контента, осуществляемая в отношении вакансий, резюме и сопутствующих информационных материалов. Целью исследования являются выявление юридической природы цифровой модерации на *HR-tech*-платформах, определение ее места в системе правового регулирования и обоснование ее роли как инструмента превентивного правоприменения в частноправовой цифровой среде. С учетом доктрины анализируются положения российского законодательства, нормы о статусе информационного посредника, а также подходы зарубежного регулирования, включая *Digital Services Act* (ЕС) и *Online Safety Act* (Великобритания). Дополнительно рассматриваются пользовательские соглашения и правила модерации конкретных платформ, что позволяет выявить практические модели премодерации, постмодерации, алгоритмической фильтрации и процедур обжалования. В эссе показано, что закрепление в российском праве специальных обязанностей владельцев сервисов размещения объявлений трансформирует традиционную модель ответственности информационного посредника и объективно предполагает внедрение активных механизмов модерации пользовательского контента. Обосновано, что цифровая модерация на *HR-tech*-платформах выходит за рамки технической фильтрации и приобретает значение механизма первичной юридической квалификации фактических обстоятельств, влекущей правовые последствия для пользователей. Особое внимание уделено дуализму правовой природы вакансий, которые в зависимости от содержания могут подпадать под различные правовые режимы, а также анализу алгоритмической модерации с учетом отраслевой специфики трудовых отношений. Аргументируется, что принцип полной прозрачности модерационных решений не является универсальным и в ряде случаев может снижать эффективность защиты прав соискателей и устойчивость платформенной экосистемы. Делается вывод о допустимости модели ограниченной прозрачности при условии сохранения механизмов апелляции и коррекции ошибок. Полученные результаты могут быть использованы при разработке пользовательских соглашений, внутренних правил модерации и алгоритмических систем *HR-tech*-платформ.

Ключевые слова

цифровая модерация, сервисы размещения объявлений, информационный посредник, вакансии, алгоритмическая модерация, цифровое правоприменение, рынок труда

Конфликт интересов Автор сообщает об отсутствии конфликта интересов.

Финансирование Исследование не имеет спонсорской поддержки.

Для цитирования Шабронова, С. Е. (2025). Правовые механизмы цифровой модерации контента на HR-Tech платформах. *Цифровое право, 6*(4), 8–20. https://doi.org/10.38044/2686-9136-2025-6-19

Поступило: 28.06.25, принято в печать: 16.11.25, опубликовано: 30.12.2025

ESSAYS

LEGAL MECHANISMS FOR DIGITAL CONTENT MODERATION ON HR TECH PLATFORMS

Svetlana E. Shabronova

Headhunter LLC
48, Vtoraya Brestskaya St., Moscow, Russia, 125047

Abstract

This essay examines the legal mechanisms of digital content moderation on *HR tech* platforms as an integral element of contemporary regulation of the digital labor market. In the context of digital transformation, online platforms increasingly move beyond the role of purely technical intermediaries and assume functions of private regulation. Within this framework, content moderation becomes a key instrument shaping the legal environment of interactions between employers and job seekers. The purpose of this study is to identify the legal nature of digital moderation on *HR tech* platforms, to determine its place within the system of legal regulation, and to substantiate its role as a form of preventive law enforcement in a private digital environment. On a doctrinal basis, the essay examines relevant provisions of Russian law, including rules on the status and liability model of the "information intermediary," and compares them with foreign regulatory approaches, notably the EU *Digital Services Act* and the United Kingdom's *Online Safety Act*. The analysis is complemented by a review of platform user agreements and moderation policies, enabling the identification of operational models of pre-moderation, post-moderation, algorithmic filtering, and appeals procedures. The essay demonstrates that the introduction of specific statutory obligations for operators of online classified services transforms the traditional model of information intermediary liability and objectively requires the implementation of proactive content moderation mechanisms. It is argued that digital moderation on HR tech platforms cannot be reduced to technical filtering; rather, it constitutes a mechanism of primary legal qualification of factual circumstances, the results of which entail legal consequences for platform users. Special attention is paid to the dual legal nature of job vacancy postings, which may fall under different legal regimes depending on their content, and to algorithmic moderation adapted to the sectoral specifics of labor relations. The study further argues that the principle of full transparency of moderation decisions is not universal and, in certain contexts, may undermine the effectiveness of fraud prevention and the stability of platform ecosystems. The essay substantiates the permissibility of limited transparency models, provided that accessible appeal mechanisms and error-correction procedures are maintained. The findings of this research may be applied in the

development of user agreements, internal moderation policies, and algorithmic moderation systems of HR tech platforms.

Keywords

digital moderation, HR tech platforms, online classified services, information intermediary, job vacancies, algorithmic moderation, digital law enforcement, labor market

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Shabronova, S. E. (2025). Legal mechanisms for digital content moderation on HR Tech platforms. *Digital Law Journal, 6*(4), 8–20. https://doi.org/10.38044/2686-9136-2025-6-19

Submitted: 28 Jun. 2025, accepted: 16 Nov. 2025, published: 30 Dec. 2025

Введение

Развитие цифровых технологий трансформировало не только способы реализации прав, но и механизмы формирования юридически значимых фактов. В научной литературе отмечается, что право в цифровой среде все чаще приобретает превентивный характер, ориентированный на упреждение конфликтов до их возникновения (Altukhov & Kashkin, 2021, pp. 86–94; Khabrieva & Chernogor, 2018, pp. 85–102).

Особую роль в этой трансформации играют цифровые платформы, которые из инструментов посредничества превращаются в субъектов частного регулирования: они устанавливают правила взаимодействия пользователей, контролируют их соблюдение и применяют меры воздействия (Casas-Cortés et al., 2023).

В контексте *HR-tech*-платформ — сервисов, обеспечивающих взаимодействие работодателей и соискателей, — ключевым инструментом такого регулирования выступает модерация контента.

Законодательство РФ не содержит легального определения термина «модерация». В Федеральном законе № 149-ФЗ[1] (далее — цитируется по номеру) он используется единожды в контексте обязанностей владельцев социальных сетей по мониторингу и удалению запрещённого контента. Однако для сервисов размещения объявлений, к которым относятся *HR-tech*-платформы, модерация приобретает специфическое значение: именно через неё реализуется обязанность владельца сервиса «не допускать использование сервиса» для распространения противоправной информации (ст. 10.7 Закона № 149-ФЗ).

В научной дискуссии акцент нередко делается на рисках для свободы выражения мнений и недостаточной прозрачности алгоритмов. Однако в контексте *HR-tech*-платформ модерация имеет иное функциональное назначение: она направлена на обеспечение качества вакансий, защиту прав соискателей и формирование безопасного цифрового пространства на рынке труда.

[1] 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).

Цель настоящего эссе — анализ правовых механизмов цифровой модерации контента на *HR-tech*-платформах в контексте российского законодательства. Основная гипотеза исследования заключается в том, что цифровая модерация на *HR-tech*-платформах представляет собой механизм первичной юридической квалификации фактов, выполняющий превентивную правоприменительную функцию, эффективность которой достигается через модель ограниченной прозрачности при сохранении механизмов апелляции.

HR-tech-платформы как сервисы размещения объявлений

В российском праве правовой статус *HR-tech*-платформ целесообразно рассматривать через призму Закона № 149-ФЗ. В частности, применима статья 10.7 указанного Закона, регулирующая обязанности владельцев сервисов размещения объявлений.

HR-tech-платформы предоставляют пользователям возможность размещения информации о предложении работы, откликов и сопутствующих сведений, что позволяет квалифицировать их именно как сервисы размещения объявлений. Такой подход соответствует функциональной природе данных платформ и позволяет избежать некорректного отождествления *HR-tech*-сервисов с социальными сетями или иными видами цифровых платформ.

Статья 10.7 Закона № 149-ФЗ возлагает на владельцев сервисов размещения объявлений обязанности по недопущению использования сервиса для совершения уголовно наказуемых деяний; предотвращению распространения экстремистских, террористических, порнографических, насильственных материалов, а также информации, содержащей нецензурную брань; пресечению распространения сведений, порочащих граждан или группы лиц. В данном контексте цифровая модерация выступает не факультативной функцией платформы, а инструментом реализации ее законодательно закрепленных обязанностей.

Эволюция конструкции информационного посредника применительно к владельцам сервисов объявлений

До появления ст. 10.7 Закона № 149-ФЗ владелец сервиса объявлений формально рассматривался как информационный посредник (ст. 1253.1 ГК РФ[2]), нес ограниченную ответственность при знании о нарушении и бездействии.

Статья 10.7 Закона № 149-ФЗ, введенная в 2022 г., изменяет эту конструкцию, поскольку прямо возлагает публично-правовые обязанности и не ограничивается моделью удаления после уведомления, что связывает ответственность не с фактом знания, а с функциональной ролью платформы.

Таким образом, статья 10.7 Закона № 149-ФЗ позволяет сделать вывод о том, что российский законодатель возлагает на владельцев сервисов размещения объявлений обязанность по обеспечению контроля за распространяемым пользователями контентом. Несмотря на отсутствие прямого указания на обязанность предварительной модерации, требование Закона не допускать использование сервиса для распространения противоправной информации предполагает необходимость выстраивания владельцем сервиса организационных и технических механизмов модерации пользовательского контента.

[2] Гражданский кодекс Российской Федерации. Часть четвертая от 18 декабря 2006 г. № 230-ФЗ. Собрание законодательства РФ, 2006 г., № 52, ст. 5496 (часть I).

Законодательство ЕС, в частности Регламент о цифровых услугах *(Digital Services Act)*[3], прямо требует от платформ внедрять механизмы контроля за распространением незаконного и вредного контента и предусматривать процессы обработки жалоб и действий по исправлению нарушений со стороны платформы.

Аналогичные тенденции наблюдаются в Великобритании: Закон об онлайн-безопасности (*Online Safety Act*) вводит обязанности для онлайн-сервисов по предотвращению распространения незаконного и опасного контента, включая защиту детей и удаление запрещенных материалов[4].

С точки зрения теории права цифровую модерацию можно рассматривать как механизм юридической квалификации фактических обстоятельств. В классической доктрине юридический факт определяется как жизненное обстоятельство, с которым норма права связывает возникновение, изменение или прекращение правоотношений (Krasavchikov, 1958, p. 5). В цифровой среде фиксация и оценка таких обстоятельств всё чаще осуществляются автоматизированными системами.

Размещение вакансии, выявление нарушения правил платформы, установление несоответствия содержания вакансии требованиям законодательства — все эти действия фиксируются в цифровой системе и приобретают значение юридически значимых фактов. Решение о блокировке или ограничении доступа пользователя представляет собой правовое последствие, наступающее в результате квалификации соответствующего факта.

Таким образом, цифровая модерация на *HR-tech*-платформах выполняет функцию первичного правоприменения в частноправовой цифровой среде. Платформа не заменяет государственные органы, однако осуществляет предварительную оценку информации и предотвращает распространение контента, потенциально нарушающего права пользователей или требования законодательства.

Типы модерации и их роль

Правовые механизмы на *HR-tech*-платформах включают элементы как обязательной, так и добровольной модерации. Обязательная модерация обусловлена требованиями законодательства, в том числе обязанностями владельца сервиса размещения объявлений по ст. 10.7 Закона № 149-ФЗ, о которых написано выше. Добровольная модерация осуществляется на основании внутренних правил платформы и направлена на повышение качества сервиса и доверия пользователей.

Внутренние стандарты модерации позволяют платформам устанавливать требования к содержанию вакансий, что прямо предусмотрено законом. Такая практика соответствует концепции сочетания правового регулирования и саморегулирования в цифровой среде, широко обсуждаемой в научной литературе (Khabrieva & Chernogor, 2018, p. 97).

Современные платформы используют премодерацию (проверку контента перед публикацией), постмодерацию (публикацию с последующей проверкой) и гибридные модели, сочетающие оба подхода[5]. Выбор конкретной модели определяется балансом между требованиями

[3] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 Oct. 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), arts. 14–17, 2022 O.J. (L 277) 1.

[4] Online Safety Act 2023, c. 50 (U.K.).

[5] Shaip. (2023, 20 сентября). *5 типов модерации контента и как масштабировать ее с помощью ИИ?* https://ru.shaip.com/blog/5-types-of-content-moderation/

к скорости взаимодействия пользователей и необходимостью минимизации юридических и репутационных рисков[6].

Алгоритмические методы модерации применяются для автоматического выявления неподходящего контента, эффективно фильтруя явные нарушения, такие как нецензурная лексика и «стоп-слова».

Этические и правовые требования к алгоритмической модерации включают принципы прозрачности, объяснимости и возможности обжалования решений.

Практическая реализация этих принципов находит отражение в пользовательских соглашениях крупных платформ. Например, правила «Авито» предусматривают запрет на регистрацию нового профиля взамен заблокированного и ограничение на повторное использование номера телефона после блокировки[7]. Такие положения демонстрируют эволюцию подходов к модерации: помимо анализа контента, платформы всё чаще применяют идентификационные и поведенческие признаки для предотвращения рецидивов нарушений.

Специфика премодерации на *HR-tech*-платформах

В отличие от универсальных платформ специализированные *HR-tech*-сервисы применяют *обязательную премодерацию работодателей* как основу доверительного пространства рынка труда. Так, согласно п. 5.1.4 правил *Rabota.ru* «Компания проходит регистрацию в Сервисе. Регистрация в Сервисе Компании признается завершенной после успешного прохождения модерации»[8]. Это демонстрирует проактивный подход к формированию экосистемы: проверка легитимности работодателя осуществляется до предоставления возможности размещения вакансий.

Постмодерация как механизм защиты прав соискателей

В то время как универсальные платформы фокусируются на общих запретах, *HR-tech*-сервисы разрабатывают специальные критерии защиты трудовых прав. Например, «Авито» как сервис объявлений общего назначения устанавливает детальные правила по запрету дискриминации, включая конкретные примеры недопустимых формулировок по признакам пола, возраста, национальности, здоровья: «Не указывайте в объявлении о вакансии ограничения или преимущества, в том числе по следующим признакам: <...> “Отсутствие инвалидности — важный критерий при приеме на работу” и т. п. “Без вредных привычек”, “только для некурящих” и т. п.»[9]

Постмодерация на *HR-tech*-платформах имеет профилактическую направленность. Согласно п. 7 правил *Rabota.ru* «все вакансии и резюме проходят постмодерацию (проверяются модераторами после размещения). Вакансии и резюме, не соответствующие настоящим Правилам, могут быть заблокированы. Компаниям, размещающим вакансии, не соответствующие настоящим Правилам, может быть приостановлен или прекращен доступ к Сервису»[10]. Это выходит

[6] Toncheva, I. (2025, February 19). *Types of content moderation: Benefits, challenges, and use cases.* Imagga. https://imagga.com/blog/types-of-content-moderation-benefits-challenges-and-use-cases/

[7] Авито. (б.д.). *Условия использования Авито.* https://www.avito.ru/legal/rules/terms-of-use/

[8] Rabota.ru. (б.д.). *Правила портала Rabota.ru.* https://www.rabota.ru/info/

[9] Авито. (б.д.). *Особенности размещения в категории «Работа».* https://www.avito.ru/legal/job/job-listings/#discrimination

[10] Rabota.ru. (б.д.). *Правила портала Rabota.ru.* https://www.rabota.ru/info/

за рамки стандартной контент-модерации и создает механизм ответственности за качество предложений на рынке труда.

Важно, что уровень глубины и строгости модерации варьируется даже между специализированными *HR-tech*-платформами, что отражает разные подходы к формированию правовой культуры рынка труда. Так, согласно п. 3.7 условий использования *HeadHunter* платформа «вправе отказать Заказчику в регистрации на Сайте либо заблокировать Регистрацию на Сайте, расторгнуть Договор с Заказчиком»[11]. Это положение демонстрирует несколько ключевых особенностей *HR-tech*-модерации.

1. Глубина верификации: *HeadHunter* не ограничивается формальной проверкой документов, а проводит комплексную оценку достоверности предоставленной информации и репутации работодателя.
2. Превентивные меры против рецидивов: особое внимание уделяется выявлению попыток обхода модерации через третьих лиц, платформа проверяет «подтверждение договорных отношений с третьими лицами (если Заказчик планирует искать персонал для третьих лиц), ранее заблокированными на Сайте».

Алгоритмическая модерация: от общих правил к отраслевой специфике

Сравнительный анализ цифровых *HR*-платформ демонстрирует качественные различия в подходах к автоматизации модерации контента, прежде всего в части выявления дискриминационных условий в вакансиях. На практике становится очевидно, что эффективная модерация не может быть сведена к формальному поиску и блокированию заранее заданных «стоп-слов» (таких как указание возраста, пола или семейного положения). Подобный подход не учитывает контекст употребления формулировок и не позволяет разграничить незаконную дискриминацию и допустимые, прямо предусмотренные законом профессиональные ограничения.

Трудовая дискриминация в российском праве определяется не самим фактом упоминания конкретного признака, а отсутствием его объективной связи с выполнением трудовой функции[12]. Так, требования, основанные на поле, возрасте, состоянии здоровья или семейном положении, признаются дискриминационными, если они не обусловлены характером работы и не предусмотрены Трудовым кодексом РФ или иными нормативными актами. Следовательно, автоматизированная модерация должна опираться не только на лингвистический анализ текста вакансии, но и на понимание правовой природы соответствующих ограничений, включая нормы охраны труда, требования к медицинским осмотрам, специальные запреты и допуски, установленные законом.

Примеры из практики модерации вакансий показывают, что дискриминационные условия нередко маскируются под нейтральные или оценочные формулировки и, напротив, допустимые требования могут содержать чувствительные признаки. Так, указание на разъездной характер работы или длительные командировки само по себе не является нарушением, тогда как прямое требование «только без детей» — уже очевидный пример дискриминации. Аналогично запрет на прием женщин или лиц определенного возраста может быть законным в строго ограниченных случаях, прямо закрепленных в нормативных актах (например, при выполнении тяжелых, вредных или опасных работ либо при наличии медицинских противопоказаний).

[11] HeadHunter. (б.д.). *Условия использования сайтов Хэдхантер*. https://hh.ru/terms

[12] Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ. Собрание законодательства РФ, 2002 г., № 1, ст. 3 (часть I).

Формальная фильтрация таких слов без анализа правового основания приводит либо к избыточным блокировкам, либо к пропуску незаконного контента.

Таким образом, автоматизация модерации в сфере объявлений о работе требует интеграции юридической экспертизы в алгоритмические модели. Речь идет не только о соблюдении формальных требований платформ, но и о соотнесении содержания вакансии с нормами Трудового кодекса РФ, практикой их применения и целями правового регулирования. В противном случае цифровая модерация рискует утратить превентивную функцию и превратиться в формальный инструмент фильтрации, неспособный эффективно предотвращать дискриминацию на рынке труда.

Отдельного внимания заслуживают случаи, когда одно и то же условие может быть как допустимым, так и незаконным в зависимости от содержания трудовой функции. Так, требование наличия водительского удостоверения является обоснованным для водителей или работников, использующих служебный автомобиль, но утрачивает правовой смысл при включении в вакансии, не связанные с управлением транспортом. Аналогичным образом различается оценка требований к речи, внешнему виду или документам: грамотная русская речь или опрятный внешний вид допустимы как профессиональные характеристики, тогда как требования родного языка, отсутствия акцента или презентабельной внешности формируют косвенную дискриминацию.

В результате в цифровой модерации формируется особый правоприменительный слой, в котором алгоритмы не просто фильтруют текст, а фактически воспроизводят логику трудового законодательства: отделяют деловые качества от социальных, физиологических и иных характеристик, не имеющих отношения к выполнению работы. Такой подход позволяет не только снижать риски ответственности за распространение дискриминационных вакансий, но и реализовывать превентивную функцию платформ — корректировать содержание объявлений еще до возникновения спора или жалобы со стороны соискателя.

Таким образом, кейсы модерации подтверждают, что борьба с трудовой дискриминацией в цифровой среде невозможна без интеграции норм Трудового кодекса РФ в архитектуру автоматизированных решений. Исключительно формальная фильтрация «стоп-слов» не учитывает ни сложность правового регулирования, ни многообразие допустимых исключений, что делает ее недостаточной для обеспечения законности и справедливости на цифровом рынке труда.

Процессуальные гарантии и обжалование решений модерации: пределы прозрачности и предотвращение обхода правил

В научной и правоприменительной дискуссии о цифровой модерации значительное внимание уделяется вопросу процессуальных гарантий пользователей и прозрачности решений, принимаемых операторами онлайн-платформ[13]. В то же время чрезмерное упрощение данной проблематики через призму права пользователя знать причины блокировки не учитывает функциональные особенности модерации как инструмента предотвращения незаконной и недобросовестной деятельности. В условиях *HR-tech*-платформ модерация выполняет не только регулятивную, но и превентивную функцию, направленную на пресечение системных нарушений, в том числе мошенничества и вовлечения соискателей в противоправную деятельность.

[13] См.: Kominers & Shapiro (2024). Авторы демонстрируют, что непрозрачная модерационная политика может быть более эффективной для предотвращения вредоносного контента, поскольку прозрачные правила позволяют злоумышленникам адаптировать свои сообщения для обхода фильтров.

Анализ пользовательского соглашения сервиса «Авито Подработка» для исполнителей позволяет выявить модель ограниченной процессуальной прозрачности, при которой платформа сохраняет за собой право применять меры ограничения доступа без детального раскрытия мотивов принятого решения[14]. Так, раздел 11 соглашения предусматривает возможность блокировки профиля при нарушении условий соглашения, наличии многократных жалоб, недобросовестных действиях исполнителя, а также в целях предотвращения нарушений законодательства. При этом соглашение не обязывает компанию в каждом случае раскрывать конкретные фактические основания блокировки или методологию их выявления.

В научной литературе ограниченная прозрачность модерационных решений критикуется как фактор, подрывающий процессуальные гарантии пользователей и усиливающий асимметрию власти между платформой и участниками цифровых отношений (Pasquale, 2015). Однако в контексте борьбы с обходом правил модерации она представляется функционально оправданной. Раскрытие детальных причин блокировки, особенно в случаях размещения объявлений с незаконным контентом либо скрытых форм вовлечения в противоправную деятельность, может создавать для нарушителей обратную связь, позволяющую адаптировать поведение и обходить установленные ограничения.

В этом смысле отказ от детализированного раскрытия причин блокировки выступает не как произвольное ограничение прав пользователя, а как элемент архитектуры противодействия злоупотреблениям. Речь идет о ситуациях, например, когда пользователь регистрируется как работодатель (например, известная компания), размещает вакансии с высокой зарплатой и минимальными требованиями к сотрудникам. А в ответ на запрос платформы прислать документы о регистрации этой компании отправляет поддельные документы. Такая компания представляет опасность для доверчивых соискателей, которые могут в надежде на трудоустройство дизайнером за 400 000 руб. в месяц выполнить бесплатные тестовые задания огромного объема, оплатить доставку каких-то материалов для тестового задания и стать жертвой иной мошеннической схемы. Большинство платформ в таких случаях блокируют нарушителя[15]. При повторной попытке регистрации с теми же реквизитами пользователь будет снова заблокирован во избежание повторения нарушений. Если платформа сообщит пользователю, что вакансия содержит неоправданно высокую зарплату, низкие требования к сотруднику, а представленные в подтверждение наличия компании документы откровенно поддельные, то такой нарушитель сделает вывод, как в следующий раз избежать блокировки.

Отсюда следует вывод, что платформа, обладая информацией о цифровом следе пользователя, паттернах поведения, повторяемости нарушений и использовании технических средств обхода, объективно не может раскрывать все основания принятия решения без риска компрометации механизмов модерации. Данный подход согласуется с практикой использования метаданных и поведенческих факторов в качестве самостоятельных оснований для ограничительных мер, даже при формальном соблюдении пользователем текстовых требований к размещаемому контенту.

Сравнительный анализ правил сайта *Rabota.ru* подтверждает указанную логику регулирования[16]. Правила сервиса прямо предусматривают право администрации блокировать вакансии,

[14] Авито. (б.д.). *Пользовательское соглашение сервиса «Авито Подработка»*. https://www.avito.ru/legal/job/gig_user-agreement/#blocking

[15] Авито. (б.д.). *Почему заблокировали профиль?* https://support.avito.ru/articles/4294#3432; HeadHunter. (б.д.). *Условия использования сайтов Хэдхантер*. https://hh.ru/terms

[16] Rabota.ru. (б.д.). *Правила портала Rabota.ru*. https://www.rabota.ru/info/

резюме или доступ к сервису без объяснения причин, а также устанавливать факт нарушения на основании учетных, статистических и иных данных сервиса либо при получении определенного количества жалоб. При этом пользователь фактически соглашается с тем, что оценка достаточности и обоснованности таких данных осуществляется администрацией сервиса по собственному усмотрению. Такая конструкция, с одной стороны, ограничивает возможности пользователя по немедленному оспариванию конкретных мотивов блокировки, а с другой — существенно снижает риски воспроизводства мошеннических схем за счет обучения нарушителей на результатах модерации.

Следует подчеркнуть, что речь не идет о полном отказе от процессуальных гарантий. И «Авито Подработка», и *Rabota.ru* закрепляют возможность обращения пользователя в службу поддержки и применения претензионного порядка разрешения споров. Однако данные механизмы носят преимущественно корректирующий, а не раскрывающий характер: их цель заключается не в предоставлении пользователю исчерпывающей информации о логике модерации, а в проверке обоснованности меры в конкретном случае и исправлении возможной ошибки. Таким образом, апелляция в рамках платформы ориентирована на восстановление прав добросовестного пользователя, а не на деконструкцию внутренних алгоритмов выявления нарушений.

Итого, полная прозрачность стратегий модерации создает у нарушителей инструмент для адаптации и обхода систем модерации.

Экономическая и стратегическая логика *opaque moderation*

Это подтверждается и в зарубежной научной литературе, где концепция модерации с непрозрачными правилами (*opaque policies*) обсуждается как обоснованная стратегия платформ. В исследовании С. Д. Коминерса и Дж. М. Шапиро анализируется, как стратегия модерации, при которой модератор не раскрывает правила блокировки сигнала (контента), может быть более эффективной в ограничении распространения вредоносных сведений или дезинформации (Kominers & Shapiro, 2024). Авторы показывают, что если политика модерации прозрачна, те, кто стремится разместить вредоносный контент, могут предсказать реакцию системы и адаптировать свои сообщения так, чтобы они обходили фильтры. В случае непрозрачной модерации, когда пользователи не знают, какие именно сигналы будут блокированы, уровень обхода систем значительно ниже.

В более новом проекте авторы развивают идеи *Robust Content Moderation*: модератор, который может удалять или фильтровать контент, должен действовать таким образом, чтобы максимально снижать вероятность вредоносного воздействия, даже если это означает закрытие части информации о причине таких действий (Kominers & Shapiro, 2024).

Анализ *algospeak* — языка обхода алгоритмов, когда пользователи сознательно изменяют словоформы и выражения, чтобы избежать автоматического удаления или понижения контента, — также подтверждает экономическую мотивацию ограниченной прозрачности модерации. Это эмпирически подтверждает, что злоумышленники адаптируются к известным правилам, внедряя обходные трюки в тексты, что снижает эффективность полностью прозрачных модерационных стратегий[17].

При этом зарубежное регулирование также исходит из необходимости баланса между прозрачностью и безопасностью. Так, в *Digital Services Act* закреплена обязанность онлайн-платформ

[17] Algospeak. (2025, September 21). In *Wikipedia*. https://en.wikipedia.org/wiki/Algospeak

представлять пользователям так называемые *Statements of Reasons* — уведомления о причинах удаления контента или ограничения доступа[18]. Однако данный механизм не предполагает раскрытия внутренних алгоритмов, весов критериев или технических параметров модерации.

В этом контексте положения пользовательских соглашений, допускающие отсутствие детализированного объяснения причин блокировки объявлений с незаконным или подозрительным контентом, не могут рассматриваться как произвольные или лишенные рационального основания. Напротив, они снижают возможность системного обхода ограничений. Процессуальные гарантии пользователя в такой модели смещаются с требования полного раскрытия причин блокировки на обеспечение доступных механизмов апелляции, проверки ошибок и восстановления доступа в случаях добросовестного поведения, что позволяет достичь баланса между защитой прав пользователей и устойчивостью платформенной экосистемы.

Наконец, исследования, посвященные *shadowbanning* — скрытой форме модерации, при которой пользователи не уведомляются прямо о причинах приостановки видимости их контента, показывают, что платформы сознательно создают такие непубличные подходы, чтобы не давать обратной связи, которую могли бы использовать злоумышленники для корректировки поведения (Risius & Blasiak, 2024, pp. 817–829).

Практические риски полной прозрачности

На практике раскрытие причин блокировки может дать злоумышленнику «черный ящик» с правилами, который он использует для систематического обхода модерации. В *HR-tech*-среде это может выглядеть так: если платформа указывает, что блокировка произошла из-за конкретного сочетания слов в тексте или определенной структуры объявления (например, определенные условия для соискателей, заведомо дискриминационные формулировки, призывы к незаконной деятельности и др.), то явный перечень таких критериев становится инструкцией по обходу. Пользователь может изменить номер телефона, переформулировать текст, сохранить скрытые схемы коммуникации в личных сообщениях — и таким образом обходить фильтры, не нарушая формально видимого правила.

Это особенно актуально для *HR-tech*-платформ, где целевые действия злоумышленников носят экономический характер: необходимость постоянного привлечения соискателей для незаконной деятельности, мошеннических схем или вовлечения людей в условия, противоречащие законодательству о рынке труда. В таком контексте платформа, сообщая злоумышленникам полные основания блокировки, по существу предоставляет им инструменты по обходу системы, подрывая цель модерации как защитного механизма.

Баланс между прозрачностью и безопасностью

Это не означает полного отказа от принципов прозрачности; скорее речь идет о балансе между правами пользователя и эффективностью систем защиты. Пользователь должен иметь возможность обжаловать конкретные решения и понимать, что его заблокировали, если это произошло ошибочно, но развернутые алгоритмы блокировки и внутренняя логика платформы, как правило, остаются закрытыми от публичного доступа. Такая модель согласуется с положениями *Digital Services Act* по вопросу *Statements of Reasons* — обязательных для крупных платформ объяснениях причин удаления конкретного контента. Тем не менее этот стандарт применяется в рамках строгих требований к объему и типу раскрываемой

[18] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 Oct. 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), art. 17, 2022 O.J. (L 277) 1.

информации, не обязывая показывать все внутренние алгоритмы (Drolsbach & Pröllochs, 2024, pp. 939–942).

Таким образом, условия пользовательских соглашений, которые позволяют не раскрывать причин блокировки в ряде случаев, не только не лишены здравого смысла, но и могут рассматриваться как стратегическая обязанность платформы по предотвращению обхода модерации и снижению рисков злоупотреблений. В *HR-tech*-экосистемах это особенно важно, поскольку речь идет о доступе человека к экономическим возможностям и рисках вовлечения в недобросовестные схемы. Здесь высокая адаптивность злоумышленников требует умелого сочетания ограниченной прозрачности и доступных механизмов апелляции для добросовестных пользователей.

Выводы

Цифровая модерация контента на *HR-tech*-платформах выступает самостоятельным правовым механизмом, обеспечивающим качество вакансий, защиту прав соискателей и формирование безопасного цифрового пространства на рынке труда.

HR-tech-платформы реализуют модерацию как в рамках публично-правовых обязанностей (ст. 10.7 Закона № 149-ФЗ), так и через добровольные внутренние стандарты, создавая сочетание регулирования и саморегулирования, что позволяет эффективно управлять рисками недобросовестной деятельности пользователей.

Модерация на *HR-tech*-платформах выполняет функцию первичной юридической квалификации фактов в цифровой среде: блокировка контента и ограничение доступа пользователей формируют правовые последствия, опережающие вмешательство государственных органов, и служат инструментом превентивного регулирования.

Эффективность модерации обеспечивается балансом между прозрачностью и безопасностью: ограниченное раскрытие причин блокировки снижает возможности обхода системы злоумышленниками, причем пользователи сохраняют процессуальные гарантии через апелляцию и корректирующие процедуры.

Специализированные алгоритмические и процессуальные подходы к модерации на *HR-tech*-платформах интегрируют отраслевую специфику трудовых отношений и нормы трудового законодательства, что обеспечивает дифференцированную защиту участников цифрового рынка труда и повышает доверие к платформе.

В эссе систематизировано и концептуализировано правовое значение цифровой модерации на *HR-tech*-платформах как механизма первичной юридической квалификации и опережающего регулирования. Подчеркнута роль ограниченной прозрачности модерационных решений как стратегической меры противодействия злоупотреблениям.

Список литературы / References

1. Altukhov, A. V., & Kashkin, S. YU. (2021). Pravovaya priroda tsifrovykh platform v rossiyskoy i zarubezhnoy doctrine [Legal nature of digital platforms in Russian and foreign doctrine]. *Actual Problems of Russian Law*, (7), 86–94.
2. Casas-Cortés, M., Cañedo-Rodríguez, M., & Diz, C. (2023). Platform capitalism. In M. Aldenderfer (Ed.), *Oxford research encyclopedia of anthropology*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190854584.013.597

3. Drolsbach, C., & Pröllochs, N. (2023). *Content moderation on social media in the EU: Insights from the DSA Transparency Database* (arXiv:2312.04431). arXiv. https://doi.org/10.48550/arXiv.2312.04431
4. Khabrieva, T. Ya., & Chernogor, N. N. (2018). Pravo v usloviyakh tsifrovoy real'nosti [Law in the conditions of digital reality]. *Journal of Russian Law,* (1), 85–102. https://doi.org/10.12737/art_2018_1_7
5. Kominers, S. D., & Shapiro, J. M. (2024). *Content moderation with opaque policies* (NBER Working Paper No. 32156). National Bureau of Economic Research. https://doi.org/10.3386/w32156
6. Krasavchikov, O. A. (1958). *Yuridicheskiye fakty v sovetskom grazhdanskom prave*. Gosyurizdat.
7. Pasquale, F. (2015). The black box society, the secret algorithms that control money and information. Harvard University Press. https://doi.org/10.4159/harvard.9780674736061
8. Risius, M., & Blasiak, K. M. (2024). Shadowbanning. *Business & Information Systems Engineering*, (66), 817–829. https://doi.org/10.1007/s12599-024-00905-3

Сведения об авторе:

Шабронова С. Е. — старший юрист, ООО «Хэдхантер», Москва, Россия.
s.shabronova@yandex.ru
ORCID: https://orcid.org/0009-0006-4502-7903

Information about the author:

Svetlana E. Shabronova — Senior Lawyer, HeadHunter LLC, Moscow, Russia.
s.shabronova@yandex.ru
ORCID: https://orcid.org/0009-0006-4502-7903

https://doi.org/10.38044/2686-9136-2025-6-15

СТАТЬИ

ЦИФРОВОЕ ИЗМЕРЕНИЕ ПРОСТРАНСТВА СВОБОДЫ, БЕЗОПАСНОСТИ И ПРАВОСУДИЯ ЕС НА СОВРЕМЕННОМ ЭТАПЕ

В. В. Войников[1,2,3,*], **А. В. Арестов**[1]

[1]Балтийский федеральный университет им. И. Канта
236041, Россия, Калининград, ул. А. Невского, 14

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

[3]Нижегородский государственный университет им. Н. И. Лобачевского
603022, Россия, Нижний Новгород, пр. Гагарина, 23

Аннотация

Статья посвящена анализу правовой природы и институциональных механизмов цифровых систем пограничного контроля Европейского союза на примере внедрения системы регистрации въезда/выезда и реализации проекта «Умные границы». Актуальность исследования обусловлена введением 12 октября 2025 системы регистрации въезда/выезда года — первого многоуровневого цифрового инструмента пограничного контроля, функционирующего на уровне крупного межгосударственного интеграционного объединения. Запуск данной системы знаменует переход Европейского союза к новой модели управления внешними границами, основанной на централизованной обработке данных, автоматизации контроля и глубокой цифровой интеграции, что требует комплексного правового анализа с учётом вопросов институционального развития и защиты прав человека. Цель исследования состоит в выявлении сущностных характеристик правового регулирования крупных информационных систем Европейского союза, обеспечивающих автоматизированный пограничный контроль, а также в определении институциональных и методологических основ их функционирования в рамках пространства свободы, безопасности и правосудия. Методологическую основу исследования составляет комплексный подход, включающий нормативно-правовой анализ регламентов Европейского союза, институциональный анализ развития пространства свободы, безопасности и правосудия, а также анализ архитектуры и механизмов функционирования системы регистрации въезда/выезда и связанных с ней цифровых платформ. В результате исследования установлено, что правовое регулирование крупных информационных систем Европейского союза характеризуется централизованной архитектурой управления, обязательностью унифицированных стандартов обработки биографических и биометрических данных, многоуровневым режимом доступа и приоритетом принципов защиты персональных данных и пропорциональности вмешательства. Показано, что основой функционирования таких систем является интеграция национальных компонентов в единый цифровой контур под управлением Агентства *eu-LISA*, обеспечивающего техническую эксплуатацию, правовую совместимость и устойчивость инфраструктуры. Выявлено, что проект «Умные границы» отражает переход

от фрагментарных информационных решений к комплексной модели автоматизированного пограничного контроля, а отказ от первоначальной двухсистемной конструкции был обусловлен институциональными и техническими ограничениями. Определены ключевые правовые риски функционирования системы регистрации въезда/выезда, включая последствия ошибок данных, интеграцию с иными информационными системами и влияние централизованной архитектуры на миграционные процедуры. Полученные результаты позволяют рассматривать систему регистрации въезда/выезда как структурный элемент формирования единого цифрового пространства Европейского союза и углубления интеграции в сфере пространства свободы, безопасности и правосудия. Исследование имеет прикладное значение для анализа аналогичных процессов в иных интеграционных объединениях и вносит вклад в развитие научных представлений о цифровом суверенитете и трансформации пограничного контроля в условиях информатизации.

Ключевые слова

Европейский союз, умные границы, пограничный контроль, пространство свободы, безопасности и правосудия, информационные системы, система регистрации въезда/выезда, Европейская система информации и авторизации путешествий

Конфликт интересов	Авторы сообщают об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.
Для цитирования	Войников, В. В., Арестов, А. В. (2025). Цифровое измерение пространства свободы, безопасности и правосудия ЕС на современном этапе. *Цифровое право, 6*(4), 21–42. https://doi.org/10.38044/2686-9136-2025-6-15

* Автор, ответственный за переписку

Поступила: 14.11.2025; принята в печать: 12.12.2025, опубликована: 30.12.2025

ARTICLES

CURRENT DIGITAL DIMENSIONS OF THE EU AREA OF FREEDOM, SECURITY AND JUSTICE

Vadim V. Voynikov[1,2,3,*], Alexander V. Arestov[1]

[1]Immanuel Kant Baltic Federal University
14, Alexander Nevsky St., Kaliningrad, Russia, 236041

[2]Moscow State Institute of International Relations (MGIMO University)
76, Vernadsky Ave., Moscow, Russia, 119454

[3]National Research Lobachevsky State University of Nizhny Novgorod (Lobachevsky University)
23, Gagarin Ave., Nizhny Novgorod, Russia, 603022

Abstract

The legal nature and institutional mechanisms of the digital border control systems of the European Union (EU) are analyzed based on case studies of the implementation of the Entry/Exit System and “Smart Borders”

project. The relevance of the research is due to the introduction of the Entry/Exit System on 12 October 2025, which represents the world's first multi-level digital border control instrument operating at the level of a major supranational integration entity. Such a transition to a new model of external border management based on centralized data processing, automated control, and deep digital integration necessitates a comprehensive legal analysis that takes into account issues of institutional development and the protection of fundamental rights. The purpose of the study is to identify the essential characteristics of the legal regulation of large-scale information systems of the EU that ensure automated border control, as well as to determine the institutional and methodological foundations of their functioning within the Area of Freedom, Security and Justice (AFSJ). The methodological framework of the research is based on a comprehensive approach that includes a normative legal analysis of European Union regulations, an institutional analysis of the development of the AFSJ, and an examination of the architecture and operational mechanisms of the Entry/Exit System and related digital platforms. The legal regulation of large-scale information systems of the European Union is shown to be characterized by a centralized governance architecture, the mandatory application of unified standards for the processing of biographical and biometric data, a multi-layered access regime, and the prioritization of the principles of personal data protection and proportionality of interference. It is demonstrated that the functioning of such systems is based on the integration of national components into a single digital framework under the management of the eu-LISA Agency, which ensures technical operation, legal interoperability, and infrastructure resilience. The "Smart Borders" project is further revealed to reflect a transition from fragmented information solutions to a comprehensive model of automated border control, while the abandonment of the initial two-system design was driven by institutional and technical constraints. Key legal risks associated with the operation of the Entry/Exit System, which functions as a structural element in the formation of a single digital space of the EU and deepening integration within the AFSJ, are revealed to include the consequences of data errors, integration with other information systems, and the impact of centralized architecture on migration procedures. The study, which contributes to the development of scholarly understanding of digital sovereignty and transformation of border controls, has relevance for the analysis of similar processes in other integration entities.

Keywords

European Union, Smart borders, border control, area of freedom, security and justice, information systems, Entry/Exit System (EES), European Travel Information and Authorisation System (ETIAS)

Conflict of interest	The authors declare no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Voynikov, V. V., & Arestov, A. V. (2025). Current digital dimensions of the EU area of freedom, security and justice. *Digital Law Journal*, *6*(4), 21–42. https://doi.org/10.38044/2686-9136-2025-6-15

* Corresponding author

Submitted: 14 Nov. 2025, accepted: 12 Dec. 2025, published: 30 Dec. 2025

Введение

12 октября 2025 г. в Европейском союзе произошло значимое событие. После долгих лет подготовительной работы наконец была запущена система регистрации въезда/выезда (*Entry/Exit System, EES)*[1]. Указанная система позволяет осуществлять регистрацию

[1] European Commission. (2025, October 13). *Entry/Exit System (EES).* https://home-affairs.ec.europa.eu/policies/schengen/smart-borders/entry-exit-system_en

въезда и выезда иностранных граждан, пересекающих внешние границы, в автоматическом порядке.

Запуск данной системы не является чем-то новым в мировой практике, многие страны мира уже давно используют различные цифровые сервисы при осуществлении пограничного контроля. В этом отношении ЕС скорее отстает от них. Тем не менее данное событие значимо, поскольку ЕС удалось разработать и ввести в эксплуатацию цифровую систему пограничного контроля, действующую не в рамках одного государства, а на уровне крупного межгосударственного объединения, что, безусловно, является трудной задачей.

В последнее время ЕС уделяет особое внимание цифровизации и информатизации при осуществлении своей политики. Использование современных технологий в рамках управления границами, иммиграцией и убежищем становится все более распространенным в рамках ЕС, страны — члены которого применяют и тестируют новые технологии для контроля своих границ и идентификации иностранцев (Delioglu, 2025, p. 2). В настоящее время активно ведется работа по формированию соответствующего законодательства, а также его имплементации. При этом институты ЕС пытаются играть ключевую роль в указанной деятельности, пытаясь внедрить союзные стандарты и перейти от национального регулирования к регламентации на уровне союза.

Внедрение общесоюзной системы регистрации въезда/выезда выступило в качестве очередного этапа построения цифрового пространства ЕС. Особое развитие цифровое измерение получило в рамках пространства свободы, безопасности и правосудия (далее — ПСБП).

Начало развитию цифрового компонента ПСБП было положено еще несколько десятилетий тому назад, когда в рамках шенгенского процесса участвующие в нем государства приняли решение о создании Шенгенской информационной системы (далее — ШИС)[2], играющей ключевую роль в вопросах контроля въезда иностранцев и борьбы с преступностью в масштабах всего союза.

С тех пор количество и качество информационных систем ПСБП существенно возросли, они стали выступать в качестве неотъемлемого элемента, обеспечивающего реализацию визовой, иммиграционной политики, политики предоставления убежищ, пограничного контроля и борьбы с преступностью (Alsaleh, 2024, p. 7).

В настоящий момент работа по развитию цифрового компонента ПСБП продолжается: помимо вышеупомянутой системы регистрации въезда/выезд идет подготовка к внедрению Европейской системы информации и авторизации путешествий (*European Travel Information and Authorisation System, ETIAS*)[3]. Обе информационные системы выступают ключевыми элементами проекта «Умные границы» (*Smart Borders*)[4]. Таким образом, посредством запуска системы регистрации въезда/выезда, Европейской системы регистрации и авторизации путешествий вместе с уже действующей визовой системой в рамках ЕС должна быть сформирована целостная цифровая составляющая, направленная на обеспечение пограничного контроля в масштабах всего союза.

[2] The Schengen acquis — Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at Their Common Borders, 2000 O.J. (L 239) 19.

[3] Министерство Европы и иностранных дел Франции. (2025). *Въезд в Шенгенскую зону: будущее внедрение систем EES и ETIAS*. https://www.diplomatie.gouv.fr/ru/dobro-pozhalovat-vo-franciyu/v-ezd-v-shengenskuyu-zonu-buduschee-vnedrenie-sistem-ees-i-etias/

[4] Investment visa. (2025, November 26). *EU Smart Borders: EES & ETIAS explained*. Harland & Poston Group. https://www.investmentvisa.com/news-and-media/eu-smart-borders

Цель настоящей статьи заключается в том, чтобы выявить сущностные характеристики правового регулирования цифровых систем в рамках ЕС, обеспечивающих осуществление пограничного контроля на внешних границах.

Правовые и институциональные основы цифрового измерения ПСБП

В условиях цифровизации особое значение приобретает информационное измерение ПСБП ЕС, представляющее собой совокупность крупных информационных систем и установленных на уровне союза механизмов их взаимодействия (Voynikov, 2019b, p. 100). Эти системы обеспечивают сбор, обработку и обмен данными, необходимыми для пограничного контроля и выполнения правоохранительных функций.

Нормативная архитектура ПСБП предусматривает дифференциацию информационных систем по их задачам и по степени централизации. По функциональному назначению они делятся на системы, ориентированные на пограничный контроль, на правоохранительные цели, а также на смешанные системы, которые обслуживают обе сферы[5]. На практике большинство из них относится именно к смешанному типу.

По институциональному устройству информационные системы подразделяются на централизованные и децентрализованные. В централизованных системах союз не только устанавливает правовые рамки их функционирования, но и создает наднациональную управляющую составляющую. В децентрализованных же ответственность за эксплуатацию лежит преимущественно на государствах-членах при минимальном нормативном вмешательстве ЕС.

Четыре ключевые системы ПСБП: ШИС, Визовая информационная система (далее — ВИС), Европейская дактилоскопическая система (*European Dactyloscopy, Eurodac*) и система регистрации въезда/выезда, образуют цифровой контур ПСБП. Эти системы не привязаны к отдельному институту союза, их задача — обеспечивать информационную взаимосвязанность всех участников ПСБП. Поскольку внесение данных осуществляется на национальном уровне, государства-члены сохраняют контроль над предоставленной ими информацией, а доступ третьих стран возможен лишь в исключительных случаях и на договорной основе.

Для управления централизованными системами в 2011 г. было создано Агентство по оперативному управлению крупномасштабными информационными системами в области ПСБП (*European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice*, далее — Агентство *eu-LISA*), действующее на основании Регламента (ЕС) 2018/1726[6]. Агентство отвечает за техническое и оперативное управление ШИС, ВИС и *Eurodac*, а также уполномочено разрабатывать и администрировать новые ИТ-системы ПСБП. С 2012 г. Агентство *eu-LISA* осуществляет деятельность, обеспечивая институциональную стабильность и технологическую интеграцию цифровой инфраструктуры ПСБП.

[5] Dumbrava, C. (2017). *European information systems in the area of justice and home affairs: An overview* (Report No. PE 603.923; p. 9). European Parliamentary Research Service. http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/603923/EPRS_IDA(2017)603923_EN.pdf

[6] Regulation 2018/1726, of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and Amending Regulation (EC) No. 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No. 1077/2011, 2018 O.J. (L 295) 99.

Проект «Умные границы»

Одним из ключевых цифровых проектов в рамках ПСБП являются «Умные границы» (*Smart Borders*). Сегодня указанный проект включает в себя две инициативы: *EES* и *ETIAS*.

Впервые о возможности внедрения составляющих инициативы «Умные границы» было заявлено в 2008 г., когда Европейская комиссия подготовила сообщение об управлении границами в ЕС[7].

25 октября 2011 г. Комиссия подготовила сообщение для Совета и Парламента, в котором предложила перечень законодательных мер, направленных на повышение безопасности границ в ЕС посредством технологизации и гармонизации[8]. Первоначально этот проект предусматривал две составляющих: систему въезда/выезда и программу регистрации путешественников, однако впоследствии Комиссия отказалась от идеи формирования двух отдельных информационных систем; таким образом, программа регистрации путешественников была включена в систему регистрации въезда/выезда.

Основная идея проекта «Умные границы» состояла в том, чтобы модернизировать управление внешними границами Шенгенской зоны с помощью передовых технологий[9]. Цель проекта — цифровизация границ для увеличения эффективности контроля, предотвращения мошенничества, более точного учета сроков пребывания и одновременно повышения удобства для добросовестных путешественников. Помимо этого, проект «Умные границы» был направлен на упрощение идентификации нелегальных иммигрантов, пытающихся въехать или уже находящихся на территории ЕС.

В 2016 году Комиссия подготовила сообщение для Европейского парламента и Совета «Более сильные и интеллектуальные информационные системы для границ и безопасности»[10]. Основная идея состояла в том, чтобы обеспечить повышение эффективности пограничного контроля посредством развития существующих и создания новых информационных систем.

Несмотря на технологическую проработку, запуск системы многократно откладывался. Среди причин сложность адаптации национальных систем, задержки в закупках, технические риски и опасения, что одновременный запуск во всех странах может нарушить устойчивость общей ИТ-инфраструктуры. В мае 2025 г. Совет ЕС и Европарламент согласовали постепенный запуск *EES* в течение шести месяцев, что должно смягчить нагрузку и дать государствам-членам больше времени на интеграцию[11]. 12 октября 2025 г. состоялся официальный старт *EES*, причем страны будут подключаться поэтапно, а полностью система должна заработать к 10 апреля 2026 г.[12]

[7] Commission Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Preparing the Next Steps in Border Management in the European Union, COM (2008) 69 final (Feb. 13, 2008).

[8] Commission Communication to the European Parliament and the Council, Smart Borders — Options and the Way Ahead. COM (2011) 680 final (Oct. 25, 2011).

[9] eu-Lisa. (2015). *Smart Borders Pilot Project: Interim report on the technical conclusions of the Pilot project*. https://www.statewatch.org/media/documents/news/2015/sep/eu-e-lisa-smart-borders-pilot-interim-report.pdf

[10] Commission Communication to the European Parliament and the Council, Stronger and Smarter Information Systems for Borders and Security, COM/2016/0205 final (Apr. 6, 2016).

[11] eu-Lisa. (2025, May 12). *EU readies for phased launch of Entry/Exit System*. https://www.eulisa.europa.eu/news-and-events/news/eu-readies-phased-launch-entryexit-system

[12] European Commission. (2025, October 17). *Smart borders*. https://home-affairs.ec.europa.eu/policies/schengen/smart-borders_en

Система регистрации въезда/выезда

Правовая архитектура системы регистрации въезда/выезда

Правовой основой системы регистрации въезда/выезда являются два регламента: Регламент 2017/2226[13], устанавливающий систему регистрации въезда/выезда, и Регламент 2017/2225[14] о внесении соответствующих изменений в Шенгенский кодекс о границах. *EES* представляет собой централизованную информационную систему, содержащую данные о пересечении иностранцами внешних границ союза и используемую для подсчета продолжительности их пребывания, выявления случаев превышения разрешенного периода пребывания, а также для иных целей (Voynikov, 2019a, p. 110).

В *EES* компетентные органы вносят данные о дате, времени и месте въезда и выезда иностранного гражданина, а сама система позволяет осуществлять автоматизированную обработку информации, в том числе с целью подсчета продолжительности разрешенного пребывания иностранца на территории Шенгенского пространства.

EES направлена на повышение безопасности внешних границ союза и упрощение пересечения границ путем все большего использования автоматизированного обмена информацией и бесконтактных устройств (Lehtonen & Aalto, 2019, p. 208).

Посредством введения *EES* решается сразу несколько задач по обеспечению безопасности и повышению эффективности пограничного контроля. Эффективность пограничного контроля увеличивается посредством того, что *EES* избавляет сотрудников пограничных служб от необходимости вручную производить подсчет общего периода пребывания иностранца на территории ЕС (Entin et al., 2018, p. 106), а безопасность обеспечивается благодаря тому, что система сама генерирует сообщение о превышении разрешенного срока пребывания иностранца на территории Шенгенского пространства.

Кроме того, *EES* создаст дополнительные удобства для самих путешественников благодаря использованию специального электронного ресурса, при помощи которого иностранец в любой момент сможет проверить оставшийся период разрешенного пребывания на территории Шенгенского пространства (*short-stay calculator*)[15].

Регламент 2017/2226 не только закрепляет обязательность регистрации данных о въезде, выезде и отказах во въезде граждан третьих стран, но и определяет категории персональных данных, включая биометрические, цели их обработки и порядок доступа для компетентных органов, «уполномоченных запрашивать такой доступ для конкретных целей» (п. 27 Преамбулы)[16].

[13] Regulation 2017/2226, of the European Parliament and of the Council of 30 November 2017 Establishing an Entry/Exit System (EES) to Register Entry and Exit Data and Refusal of Entry Data of Third-Country Nationals Crossing the External Borders of the Member States and Determining the Conditions for Access to the EES for Law Enforcement Purposes, and Amending the Convention Implementing the Schengen Agreement and Regulations (EC) No. 767/2008 and (EU) No. 1077/2011, 2017 O.J. (L 327) 20.

[14] Regulation 2017/2225, of the European Parliament and of the Council of 30 November 2017 Amending Regulation (EU) 2016/399 as Regards the Use of the Entry/Exit System, 2017 O.J. (L 327) 1.

[15] European Commission. (2025, October 27). *Short-stay calculator.* https://home-affairs.ec.europa.eu/policies/schengen/border-crossing/short-stay-calculator_en

[16] Regulation 2017/2226, of the European Parliament and of the Council of 30 November 2017 Establishing an Entry/Exit System (EES) to Register Entry and Exit Data and Refusal of Entry Data of Third-Country Nationals Crossing the External Borders of the Member States and Determining the Conditions for Access to the EES for Law Enforcement Purposes, and Amending the Convention Implementing the Schengen Agreement and Regulations (EC) No. 767/2008 and (EU) No. 1077/2011, 2017 O.J. (L 327) 20, 24.

В рамках системы регистрации въезда/выезда уполномоченные правоохранительные органы получают доступ к агрегированной статистике, например о количестве нарушителей сроков пребывания, через защищенное хранилище данных, управляемое Агентством *eu-LISA*. Для обеспечения безопасности предусмотрена обязательная защита персональных данных, а Комиссия принимает исполнительные акты, регулирующие функционирование веб-сервиса, в том числе требования к защите данных и безопасному обмену через зашифрованный канал (*Trans European Services for Telematics between Administrations, TESTA*)[17].

Регламент 2017/2225 также обеспечивает техническую и правовую совместимость системы регистрации въезда/выезда с иными инструментами союза, вводя в Шенгенский кодекс понятия *self-service system*, *e-gate* и «автоматизированная система пограничного контроля» (*Automated Border Control system*)[18], а также устанавливая сроки внедрения соответствующих институтов.

Автоматическая система пограничного контроля позволяет проходить пограничный контроль в пунктах пропуска в автоматическом порядке и состоит из двух частей: 1) системы самостоятельной регистрации (*self-service system*), представляющей собой совокупность технических устройств, посредством которых осуществляются все или некоторые виды пограничного контроля; 2) электронного пункта пропуска (*e-gate*) — специальной аппаратуры, управляемой с помощью электронных средств, посредством которой осуществляется пересечение границы.

В соответствии со ст. 8b Регламента 2016/399 граждане третьих стран, подлежащие регистрации в *EES*, могут проходить проверку через такие устройства при наличии электронного паспорта, возможности биометрической идентификации и выполнении технических требований[19]. Работа *e-gate* сопровождается обязательной биометрической проверкой (как минимум лица) и верификацией подлинности и целостности данных чипа паспорта. Эксплуатация автоматизированных систем осуществляется под визуальным контролем сотрудника пограничной службы, который должен вмешаться при любых подозрительных обстоятельствах.

На техническом уровне *EES* разрабатывается как централизованная система: государства-члены подключаются через национальный единый интерфейс (*National Uniform Interface, NUI*), что обеспечивает унификацию передачи данных и их обработку на уровне Агентства *eu-LISA*.

Особое внимание уделено соблюдению прав человека. Регламент требует, чтобы использование *EES*, включая сбор биометрии, соответствовало гарантиям Европейской конвенции о защите прав человека и основных свобод[20], Хартии ЕС об основных правах[21] и Конвенции о правах ребенка[22] (Kontak, 2024, p. 623).

По оценкам Комиссии, ежегодно в системе будут регистрироваться данные примерно о 300 млн пересечениях граждан третьих стран. Хотя внедрение *EES* предполагает значительные

[17] Regulation 2017/2226, of the European Parliament and of the Council of 30 November 2017 Establishing an Entry/Exit System (EES) to Register Entry and Exit Data and Refusal of Entry Data of Third-Country Nationals Crossing the External Borders of the Member States and Determining the Conditions for Access to the EES for Law Enforcement Purposes, and Amending the Convention Implementing the Schengen Agreement and Regulations (EC) No. 767/2008 and (EU) No. 1077/2011, art. 68, 2017 O.J. (L 327) 78.

[18] Regulation 2017/2225, of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as Regards the Use of the Entry/Exit System, art. 1, 2017 O.J. (L 327) 4.

[19] Regulation 2016/399, of the European Parliament and of the Council of 9 March 2016 on a Union Code on the Rules Governing the Movement of Persons Across Borders (Schengen Borders Code), 2016 O.J. (L 77), 1, 12.

[20] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221.

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

[22] Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.

операционные преимущества, оно одновременно порождает риски для основных прав граждан третьих стран и требует применения компенсаторных механизмов[23]. *EES* позволяет вести электронные записи обо всех иностранцах, въезжающих в Шенгенскую зону, это влечет за собой изменение характера политики ЕС в отношении иностранцев, предполагающее развитие массового наблюдения, или массовой слежки, как центрального элемента пограничного контроля (Jeandesboz, 2016, p. 293).

Воздействие *EES* затрагивает ключевые положения Хартии ЕС об основных правах: человеческое достоинство (ст. 1), право на частную жизнь (ст. 7), защиту данных (ст. 8), запрет дискриминации (ст. 21), а также защиту уязвимых групп: детей, пожилых людей и лиц с ограниченными возможностями (ст. 24–26). Возможны косвенные последствия для права на убежище (ст. 18) и принципа невысылки (ст. 19). Существенное значение имеет обеспечение эффективных средств правовой защиты (ст. 47), поскольку даже при низкой вероятности ошибки биометрической идентификации массовый характер обработки данных повышает риск неправомерных решений. Права, закрепленные в Хартии ЕС об основных правах и эквивалентные им, предусмотренные Европейской конвенцией о защите прав человека и основных свобод, подлежат толкованию с учетом практики Европейского суда по правам человека (ст. 52(3) Хартии)[24], что требует применения ее стандартов при оценке вмешательства *EES* в частную жизнь[25].

Регламент 2017/2226 предусматривает комплекс гарантий: обеспечение точности данных и их защиты (ст. 35, 39), право граждан третьих стран на доступ к информации (ст. 50), а также механизмы исправления данных и возмещения ущерба (ст. 52). Для уязвимых категорий лиц должны применяться меры, исключающие непропорциональное бремя при прохождении пограничного контроля[26].

Поскольку *EES* является частью архитектуры крупных информационных систем ЕС, ее данные будут доступны через механизм совместимости, в том числе для систем миграции и предоставления убежища. Это означает, что ошибки в *EES* могут негативно отразиться на процедурах предоставления убежища или иных миграционных решениях. Контроль за системой, включая мониторинг надежности, доступов и статистики, осуществляется Агентством *eu-LISA*, обязующимся публиковать отчеты и предоставлять агрегированные данные[27].

Проблемы и риски внедрения системы

Дополнительного анализа требуют несколько групп вопросов и рисков, связанных с внедрением и функционированием *EES*. Одной из ключевых тем является операционная устойчивость системы: централизованная архитектура предъявляет повышенные требования к надежности

[23] European Union Agency for Fundamental Rights. (2025, October 8). *Entry/Exit system: Fundamental rights guidance for managers*. https://fra.europa.eu/lv/publication/2025/entryexit-system-guidance-managers

[24] Charter of Fundamental Rights of the European Union, art. 1, 7–8, 18–19, 21, 24–26, 47, 53, 2012 O.J. (C 326) 391, 396–397, 399–401, 405, 407.

[25] Yang, Y., Zuiderveen Borgesius, F., Beckers, P., & Brouwer, E. (2024). *Automated decision-making and artificial intelligence at European borders and their risks for human rights* (p. 32). Social Sciences Citation Network. http://dx.doi.org/10.2139/ssrn.4790619

[26] Regulation 2017/2226, of the European Parliament and of the Council of 30 November 2017 Establishing an Entry/Exit System (EES) to Register Entry and Exit Data and Refusal of Entry Data of Third-Country Nationals Crossing the External Borders of the Member States and Determining the Conditions for Access to the EES for Law Enforcement Purposes, and Amending the Convention Implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, art. 35, 39, 50, 52, 2017 O.J. (L 327) 20, 51, 56, 61, 62.

[27] Ibid., art. 27.

ИТ-инфраструктуры и стабильности каналов связи между национальными интерфейсами и центральным узлом. В этой связи необходимо оценить вероятность отказов, перебоев в коммуникации, а также достаточность мер по резервному копированию и восстановлению данных.

Не менее значимой является проблема согласования *EES* с другими крупными информационными системами ЕС, такими как *ETIAS* и ШИС. Обеспечение их полноценной совместимости требует устранения технических расхождений, связанных со стандартами, форматами данных и различиями в нормативном регулировании, что усложняет интеграцию.

Введение системы регистрации въезда/выезда будет иметь определенные последствия и для граждан Российской Федерации как граждан третьей страны, подпадающей под общее действие шенгенского пограничного режима. Это влияние следует рассматривать в контексте действующих визовых ограничений, введенных государствами — членами ЕС в отношении российских граждан после 2022 г., включая приостановление действия Соглашения об упрощении выдачи виз между ЕС и РФ, запрет на выдачу виз со стороны целого ряда стран ЕС, увеличение сроков рассмотрения заявлений и расширение практики отказов во въезде по соображениям общественного порядка и безопасности[28].

С правовой точки зрения *EES* применяется ко всем гражданам третьих стран, въезжающим на территорию государств-членов для краткосрочного пребывания, независимо от гражданства, при условии, что они не относятся к специально исключенным категориям. Таким образом, российские граждане, получающие шенгенские визы либо въезжающие на иных законных основаниях, в общем порядке подлежат регистрации в *EES* с фиксацией биографических данных, даты и места пересечения границы, а также биометрических идентификаторов. Это означает, что даже при сокращении реальных потоков въезда система будет аккумулировать данные о перемещениях тех российских граждан, которые сохраняют доступ к Шенгенскому пространству, включая лиц с гуманитарными визами, членов семей граждан ЕС или обладателей служебных и дипломатических документов (за исключением прямо освобожденных категорий).

Отдельного анализа требует вопрос калининградского транзита, который исторически представляет собой особый режим передвижения граждан РФ через территорию ЕС. Общий принцип действия *EES* предполагает регистрацию факта пересечения внешней границы Шенгенской зоны, независимо от формы въезда. Однако согласно ст. 6а Шенгенского кодекса о границах в редакции Регламента 2017/2225 не подлежат внесению в *EES* данные в отношении

[28] Agreement between the European Community and the Russian Federation on the Facilitation of the Issuance of Visas to the Citizens of the European Union and the Russian Federation, 2007 O.J. (L 129), 27. См. версию на русском языке: Соглашение между Российской Федерацией и Европейским сообществом об упрощении выдачи виз гражданам Российской Федерации и Европейского союза (г. Сочи, 25 мая 2006 г.), Бюллетень международных договоров, август 2007 г., № 8. *Частично* приостановлено Указом Президента РФ «Об ответных мерах визового характера в связи с недружественными действиями иностранных государств» от 04 апреля 2022 № 183, Собрание законодательства РФ, 11.04.2022, № 15, ст. 2452 и Федеральным законом «О приостановлении Российской Федерацией действия отдельных положений международных договоров Российской Федерации с Европейским сообществом, Королевством Дания, Исландией, Княжеством Лихтенштейн, Королевством Норвегия, Швейцарской Конфедерацией об упрощении выдачи виз гражданам Российской Федерации и Европейского союза, Королевства Дания, Исландии, Княжества Лихтенштейн, Королевства Норвегия, Швейцарской Конфедерации» от 1 мая 2022 г. № 119-ФЗ (в ред. от 25.12.2023 № 646-ФЗ), Собрание законодательства РФ, 02.05.2022, № 18, ст. 3005. Приостановлено *полностью* со стороны Европейского союза решением Совета ЕС, см.: Proposal for a Council Decision on the Suspension in Whole of the Application of the Agreement between the European Community and the Russian Federation on the Facilitation of the Issuance of Visas to the Citizens of the European Union and the Russian Federation, COM/2022/661 final (Sept. 6, 2022).

лиц, которые при пересечении границы предъявляют действующий упрощенный транзитный документ для железнодорожного транспорта (*Facilitated Rail Transit Document, FRTD*)[29], выданный в соответствии с Регламентом (ЕС) 693/2003[30], либо упрощенный транзитный документ (*Facilitated Transit Document, FTD*) при условии транзита исключительно поездом и отсутствия высадки на территории государства-члена. Тем самым законодатель ЕС прямо вывел калининградский железнодорожный транзит из сферы действия *EES*, подтвердив сохранение его особого правового режима даже в условиях цифровизации пограничного контроля.

Это исключение имеет принципиальное значение, поскольку на практике для транзитных пассажиров, следующих по упрощенному транзитному документу для железнодорожного транспорта, уже на протяжении длительного времени штампы проставляются не в паспорта, а в транзитный документ, который не вклеивается в паспорт. Введение *EES* без указанного исключения привело бы к фактическому пересмотру всей логики калининградского транзита и его приравниванию к обычному краткосрочному въезду, чего законодатель сознательно избегает.

В случае калининградского транзита на автомобильном транспорте через территорию ЕС на основании упрощенного транзитного документа применяются специальные правила внесения данных в *EES* в соответствии с приложением II к Регламенту 2017/2226[31].

Помимо калининградского транзита, Регламент о *EES* содержит и иные исключения, которые потенциально затрагивают российских граждан, хотя и в ограниченном числе случаев. В частности, в систему не вносятся данные о лицах, обладающих видом на жительство или разрешением на долгосрочное пребывание в государстве-члене, а также о некоторых иных категориях иностранцев.

В совокупности влияние *EES* на российских граждан носит дифференцированный характер. С одной стороны, система усиливает цифровой контроль и снижает пространство для дискреции при повторных въездах, что в условиях политически мотивированных визовых ограничений может иметь сдерживающий эффект. С другой стороны, сохранение специальных исключений, прежде всего в отношении калининградского транзита, свидетельствует о том, что даже в условиях деградации отношений с РФ ЕС стремится формально соблюдать ранее взятые международно-правовые обязательства и избегать автоматического распространения новых цифровых инструментов на чувствительные вопросы транзита.

Европейская система информации и авторизации путешествий

ETIAS представляет собой систему предварительной авторизации въезда на территорию ЕС граждан третьих стран, освобожденных от визовых требований. *ETIAS* можно назвать аналогом[32]

[29] Schengen Borders Code, 2016 O.J. (L 77), 1; Regulation 2017/2225, of the European Parliament and of the Council of 30 November 2017 Amending Regulation (EU) 2016/399 as Regards the Use of the Entry/Exit System, art. 1, 2017 O.J. (L 327) 1, 4–7.

[30] Council Regulation No. 693/2003, of 14 April 2003 Establishing a Specific Facilitated Transit Document (FTD), a Facilitated Rail Transit Document (FRTD) and Amending the Common Consular Instructions and the Common Manual, 2003 O.J. (L 99) 8.

[31] Regulation 2017/2226, of the European Parliament and of the Council of 30 November 2017 Establishing an Entry/Exit System (EES) to Register Entry and Exit Data and Refusal of Entry Data of Third-Country Nationals Crossing the External Borders of the Member States and Determining the Conditions for Access to the EES for Law Enforcement Purposes, and Amending the Convention Implementing the Schengen Agreement and Regulations (EC) No. 767/2008 and (EU) No. 1077/2011, 2017 O.J. (L 327) 20, 24.

[32] ETIAS. (2025, November 26). *ETIAS visa waiver security: How ETIAS compares to ESTA, Canada's eTA, and the UK ETA in protecting borders and travelers.* https://etias.com/articles/etias-visa-waiver-security-how-etias-compares-to-esta,-canada%E2%80%99s-eta,-and-the-uk-eta-in-protecting-borders-and-travelers

Электронной системы авторизации путешествий (*Electronic System for Travel Authorization (ESTA*), действующей в США и введенной в качестве ответа на террористические атаки 11 сентября 2001 г.[33].

Правовой основой *ETIAS* служат Регламент 2018/1240[34], учреждающий данную систему, а также Регламент 2018/1241[35]. Согласно указанным правовым актам система призвана укрепить и усовершенствовать ИТ-системы союза, архитектуру данных и обмен информацией в области управления границами, обеспечение правопорядка и борьбу с терроризмом путем внедрения более сильных и интеллектуальных информационных систем.

Ключевой особенностью *ETIAS* является возможность перепроверки данных, предоставленных путешественником, по другим крупным системам ЕС, занимающимся вопросами границ, безопасности и миграции, таким как ШИС, ВИС, *EES* и *Eurodac*, а также базы данных Европола и Интерпола. Кроме того, *ETIAS* будет включать специальный список наблюдения и индикаторы риска. Таким образом, ожидается, что *ETIAS* устранит информационные пробелы и укрепит внутреннюю безопасность ЕС.

ETIAS должна давать разрешение на поездку гражданам третьих стран, освобожденным от визовых требований, исходя из того, не представляет ли их присутствие на территории государств-членов или не будет ли представлять угрозу безопасности, риск нелегальной иммиграции или высокий эпидемический риск. Заявки подаются онлайн (через веб-сайт или мобильное приложение), и в них заявитель указывает персональные данные, реквизиты проездного документа, сведения о родстве, профессии, криминальном прошлом и т. п. (ст. 15 Регламента 2018/1240), а система, в свою очередь, проводит автоматическую проверку подаваемых данных по ряду баз: ШИС, *EES*, ВИС, базе Европола, чтобы выявить «подозрительные случаи, требующие дополнительного анализа» (ст. 20 Регламента 2018/1240). Если система находит совпадения, заявление обрабатывается вручную ответственным национальным подразделением *ETIAS* государства-члена, с возможностью дополнительного запроса информации (ст. 21 Регламента 2018/1240)[36]. Услуга авторизации является платной и стоит 20 евро (ст. 18 Регламента 2018/1240 в редакции делегированного регламента 2025/1411)[37].

По сути *ETIAS* выступает механизмом предварительного разрешения на въезд в страны Шенгенского пространства, т. е. неким аналогом шенгенской визы, только выдаваемым в электронном виде. Фактически *ETIAS* позволяет осуществлять пограничный контроль дистанционно, еще до того, как иностранец окажется на внешней границе Союза (Skleparis, 2016, p. 107). Иными словами, *ETIAS* можно рассматривать в качестве некого аналога электронной визы. Мировая практика свидетельствует о том, что электронная виза оформляется онлайн, без посещения консульских учреждений и визовых центров, и высылается заявителю в цифровом виде,

[33] Implementing Recommendations of the 9/11 Commission Act, Pub. L. No. 110–53, 121 Stat. 266 (2007), https://www.govinfo.gov/content/pkg/PLAW-110publ53/pdf/PLAW-110publ53.pdf

[34] Regulation 2018/1240, of the European Parliament and of the Council of 12 September 2018 Establishing a European Travel Information and Authorisation System (ETIAS) and Amending Regulations (EU) No. 1077/2011, (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, 2018 O.J. (L 236) 1.

[35] Regulation 2018/1241, of the European Parliament and of the Council of 12 September 2018 Amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS), 2018 O.J. (L 236) 72.

[36] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R1240

[37] Commission Delegated Regulation (EU) 2025/1411, of 16 July 2025 amending Regulation (EU) 2018/1240 of the European Parliament and of the Council as regards the amount of the European Travel Information and Authorisation System (ETIAS) travel authorisation fee, art. 1, 2025 O.J. (L 2025/1411), 1, 2.

часто по электронной почте или через специализированный портал, после чего предъявляется при пересечении границы[38]. *ETIAS* же не заменяет традиционную шенгенскую визу, а служит инструментом для разрешения (авторизации) на въезд для граждан стран с безвизовым режимом для краткосрочных поездок. При этом в отличие от шенгенской визы разрешение на въезд (авторизация) принимается не на национальном уровне, а на уровне ЕС. Однако разработчики законопроекта намеренно отказались от использования слова «виза» с тем, чтобы почеркнуть отличие визы от разрешения на въезда (авторизации) и сохранить иллюзию открытости ЕС при ужесточении правил въезда иностранцев. Это, в частности, следует из того, что в соответствии регламентом 2018/1240 (ст. 1) система *ETIAS* распространяется на иностранных граждан, освобожденных от визовых требований. Более того, согласно п. 9 преамбулы Регламента 2018/1240 разрешение на въезда (авторизация) по своей природе не является визой, поскольку она не потребует дополнительной информации и не станет более тяжелым бременем для заявителей, чем виза[39].

С точки зрения защиты прав человека Регламент 2018/1240 акцентирует внимание на балансе между эффективностью предварительного анализа рисков и гарантиями основных свобод. Согласно данному документу, выдача или отказ в авторизации не гарантируют автоматическое право въезда или запрет на него[40]. Заявители сохраняют право подать апелляцию, которая должна быть подана в государстве-члене, принявшем решение по заявке, и в соответствии с национальным законодательством этой страны. Заявители также имеют право на возмещение ущерба, если считают, что с ними обошлись «несправедливо»[41].

Если данные не соответствуют действительности и в ходе автоматизированной обработки не было зарегистрировано других совпадений, Центральное подразделение ETIAS удаляет ложное совпадение из файла заявления, а центральная система *ETIAS* автоматически выдает разрешение на поездку. Центральное подразделение *ETIAS* должно завершить ручную обработку в течение не более 12 часов с момента получения файла заявления[42]. Кроме того, введены гарантии прав субъектов данных: предусмотрена юридическая возможность обжалования отказа, а также ограничение по сроку действия авторизации — три года или до истечения

[38] Объединённые Арабские Эмираты (ОАЭ): *e*-виза подается полностью онлайн, не требует посещения посольства или консульства, привязывается к номеру паспорта и направляется заявителю в электронном виде. Япония: государство ввело систему *eVisa*, где иностранцы подают заявку через официальный веб-портал, а электронное разрешение высылается без визовых наклеек в паспорт. Казахстан: туристические, деловые и медицинские электронные визы оформляются через официальный визово-миграционный портал в интернете, без посещения консульских учреждений, и действуют для граждан более чем 100 стран.

[39] То, что разрешение на въезд (авторизация) не является визой подчеркивается в официальных разъяснениях: «ETIAS authorisation is not a visa. Nationals of visa liberalisation countries will still be able to travel without a visa but will be required... to obtain a travel authorisation prior to their travel» (См.: Diplomatic Service of the European Union. (2016, November 17). *Security Union: A European travel information and authorisation system — questions & answers*. https://www.eeas.europa.eu/node/15205_en).

[40] Regulation 2018/1240, of the European Parliament and of the Council of 12 September 2018 Establishing a European Travel Information and Authorisation System (ETIAS) and Amending Regulations (EU) No. 1077/2011, (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, 2018 art. 40 (1) O.J. (L 236) 39.

[41] Wahl, T. (2018, October 20). *European Travel Information and Authorisation System (ETIAS): Legislation adopted*. eucrim. https://eucrim.eu/news/european-travel-information-and-authorisation-system-etias-legislation-adopted/

[42] Regulation 2018/1240, of the European Parliament and of the Council of 12 September 2018 Establishing a European Travel Information and Authorisation System (ETIAS) and Amending Regulations (EU) No. 1077/2011, (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, art. 22(6), 2018 O.J. (L 236) 27.

срока действия проездного документа[43]. При этом в Регламенте 2018/1240 заложены строгие нормы конфиденциальности. Обработка данных должна соответствовать стандартам защиты персональных данных, а система проектируется с учетом фундаментальных прав. Также предусмотрены специальные поправки в Регламенте (EU) 2021/1152 с целью регулирования доступа *ETIAS* к другим ИТ-системам ЕС и обеспечения законного, но ограниченного обмена данными[44].

Регламент 2018/1240 (п. 27 Преамбулы) предусматривает создание специального независимого Совета по основным правам *ETIAS* (*The ETIAS Fundamental Rights Guidance Board*), который объединяет представителей агентства «Фронтекс», Европейского инспектора по защите данных, Европейского совета по защите данных и Агентства по основным правам (*Fundamental Rights Agency, FRA*)[45]. Совет по основным правам оценивает соблюдение прав человека в системе, прежде всего конфиденциальность, защиту данных и недискриминацию.

В первом годовом отчете Совет по основным правам отметил, что в 2023 г. его работа была сосредоточена на подготовке к первоначальному запуску системы: разработке правил проверки, формировании списка наблюдения *ETIAS*, создании процедур обработки заявлений и взаимодействии с национальными подразделениями, Центральным подразделением *ETIAS* и Рабочей группой по операциям проверки рисков[46]. Институционально *ETIAS* должна функционировать в рамках Центрального подразделения агентства «Фронтекс» и национальных подразделений в 30 странах.

С точки зрения институциональной и правовой устойчивости *ETIAS* содержит риски, требующие анализа. Операционная надежность зависит от сложной ИТ-инфраструктуры и высокой загруженности при массовом заполнении заявок — необходимо оценить возможность перегрузок, сбоя связи и отказов. Совместимость с другими системами ЕС (ШИС, *EES*) может стать вызовом из-за разницы в стандартах и протоколах обмена данными. Потенциальные проблемы *ETIAS* включают значительные задержки запуска, вызванные техническими проблемами, вопросами конфиденциальности данных и необходимостью обновления системы безопасности. Официальный запуск *ETIAS* неоднократно откладывался (в настоящее время предполагаемый срок — конец 2026 г.)[47] из-за сложности интеграции баз данных и координации работы во многих странах.

---

[43] Regulation 2018/1240, of the European Parliament and of the Council of 12 September 2018 Establishing a European Travel Information and Authorisation System (ETIAS) and Amending Regulations (EU) No. 1077/2011, (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, 2018 art. 24 (6c (ii)) O.J. (L 236) 29.

[44] Regulation 2021/1152, of the European Parliament and of the Council of 7 July 2021 Amending Regulations (EC) No. 767/2008, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861 and (EU) 2019/817 as Regards the Establishment of the Conditions for Accessing Other EU Information Systems for the Purposes of the European Travel Information and Authorisation System, 2021 O.J. (L 249) 15.

[45] Regulation 2018/1240, of the European Parliament and of the Council of 12 September 2018 Establishing a European Travel Information and Authorisation System (ETIAS) and Amending Regulations (EU) No. 1077/2011, (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, 2018 O.J. (L 236) 1, 5.

[46] ETIAS Fundamental Rights Guidance Board, *Annual Report 2023* (2024), https://www.frontex.europa.eu/assets/fundamental/Annual_Report_EFRGB_2023.pdf

[47] Министерство Европы и иностранных дел Франции. (2025, сентябрь). *Въезд в Шенгенскую зону: будущее внедрение систем EES и ETIAS*. https://www.diplomatie.gouv.fr/ru/dobro-pozhalovat-vo-franciyu/v-ezd-v-shengenskuyu-zonu-buduschee-vnedrenie-sistem-ees-i-etias/

После запуска системы могут возникнуть такие проблемы, как длинные очереди на границах, путаница при первоначальном внедрении соответствующей *EES* и отказы по таким причинам, как наличие судимости или неточные данные в заявке[48].

Кроме того, важен аспект защиты прав человека: автоматизация проверки, использование алгоритмов оценки риска могут оказать непропорциональное воздействие на лиц с меньшей цифровой грамотностью или на уязвимые категории (например, пожилые люди или лица с особыми потребностями). Мошеннические сайты, имитирующие официальные ресурсы *ETIAS*, приводят к риску передачи денежных средств мошенникам, кражи персональных данных и дезинформации о процессе подачи заявки.

Международные и европейские рекомендации по защите прав, а также требования прозрачности решений и обжалования отказов должны лежать в основе технического дизайна и процедур[49]. Важнейшей задачей для лиц, которым необходимо подать заявление в *ETIAS*, является обеспечение доступа к эффективным средствам судебной защиты в случае, если они хотят оспорить решение, вынесенное по их заявлению. Например, отказ в выдаче разрешения на поездку может быть вызван ошибкой обработки данных, которая может привести к неправомерному отказу во въезде в ЕС. В таких случаях лица могут ссылаться на свое право на эффективные средства судебной защиты, закрепленное в ст. 47 Хартии ЕС об основных правах[50]. Она распространяется на органы ЕС и национальные органы власти при применении законодательства ЕС и позволяет лицам оспаривать в суде законность любого решения, неблагоприятно влияющего на них. Особая осторожность может потребоваться в случаях, когда отказ связан с конфиденциальными данными правоохранительных органов или конфиденциальной информацией, касающейся угрозы безопасности[51].

Визовая информационная система

ВИС формально не входит в состав проекта «Умные границы», однако является важнейшей составляющей цифровизации пограничного контроля в рамках Шенгенской зоны. Система представляет собой централизованную электронную базу данных, предназначенную для аккумулирования и обмена информацией о выдаче виз гражданам третьих стран между государствами — членами ЕС. Взаимный обмен визовой информацией обеспечивает основу для создания единого визового пространства и повышает эффективность работы визовых и пограничных служб. После внедрения ШИС и системы *Eurodac* разработка ВИС стала следующим логичным шагом в рамках борьбы с нелегальной иммиграцией (Broeders, 2007, p. 85).

Цели создания ВИС многоаспектны. Во-первых, система выполняет правоохранительные функции, снижая угрозы внутренней безопасности и способствуя борьбе с организованной преступностью. Во-вторых, она направлена на предотвращение незаконной миграции

[48] ETIAS. (2025, Oct. 17). *Technical glitches, long queues mark EU's Entry/Exit System rollout.* https://etias.com/articles/technical-glitches,-long-queues-mark-eu%E2%80%99s-entry/exit-system-rollout

[49] Jones, C. (2019). *Data protection, immigration enforcement and fundamental rights: What the EU's regulations on interoperability mean for people with irregular status.* StateWatch & PICUM. https://picum.org/wp-content/uploads/2019/11/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf

[50] Charter of Fundamental Rights of the European Union, art. 47, 2012 O.J. (C 326) 391, 405.

[51] European Data Protection Supervisor, *Opinion 3/2017: EDPS Opinion on the Proposal for a European Travel Information and Authorisation System (ETIAS)* (Mar. 6, 2017), https://www.edps.europa.eu/sites/default/files/publication/17-03-070_etias_opinion_en.pdf

и упрощение контроля на внешних границах. В-третьих, ВИС повышает эффективность регулирования въезда иностранцев: упрощает выдачу виз, предотвращает практику *visa shopping*[52] и обеспечивает обоснованность принимаемых решений о визах.

Правовая основа ВИС содержится в нескольких нормативных актах ЕС: решении Совета 2004/512/ЕС[53], Регламенте Совета и Европейского парламента 767/2008[54], а также решении Комиссии 2006/648/ЕС[55]. ВИС состоит из двух частей: центральной базы данных (*Central Visa Information System, CS-VIS*) и национальных интерфейсов (*National Interface, NI-VIS*). Информация о визах вносится через национальные интерфейсы и хранится в центральной базе. Передача данных осуществляется посредством специально разработанной коммуникационной инфраструктуры, обеспечивающей надежный и безопасный обмен информацией между государствами.

Согласно Регламенту 767/2008 в систему вносятся сведения обо всех заявлениях на краткосрочные (шенгенские) визы, а также о решениях по этим заявлениям: выдача, отказ, аннулирование или продление виз[56]. Кроме того, в систему вносятся данные о национальных долгосрочных визах, действительных для краткосрочных поездок. Для каждого заявителя сохраняются буквенно-цифровые данные, фотографии, отпечатки пальцев и ссылки на предыдущие обращения или совместных путешественников.

Основной информационной единицей ВИС является файл визового заявления. Любое решение, принимаемое в отношении визы, вносится в соответствующий файл. При этом система не ограничивает внесение информации конкретным государством: файл, сформированный одной визовой службой, может быть дополнен компетентным органом другого государства, например при аннулировании визы. Срок хранения визовых файлов составляет до пяти лет после окончания действия визы или после принятия решения об отказе в ее выдаче[57].

Доступ к ВИС возможен в двух режимах: активном и пассивном. Активный доступ позволяет вносить, изменять и удалять данные и предоставляется исключительно визовым службам, включая консульства и другие уполномоченные органы. Пассивный доступ дает возможность только просмотра информации и предназначен для пограничных служб, полиции, иммиграционных органов и органов, участвующих в процедуре предоставления убежища[58].

ВИС не предусматривает введение на уровне ЕС электронных шенгенских виз. Исходя из открытой информации, указанный вопрос пока даже не обсуждается. При этом в мировой практике электронные визы получают все большее распространение как способ упрощения въезда иностранных граждан. Например, в России уже несколько лет действует единая электронная виза, доступная гражданам более 50 государств (включая все страны ЕС), с возможностью однократного въезда и пребывания до 30 суток; заявление подается онлайн на официальном портале без необходимости прикрепления дополнительных документов, кроме паспорта

[52] *Visa-shopping* — явление, означающее заведомое нарушение заявителем установленного порядка определения государства, ответственного за выдачу визы, посредством обращения в консульское учреждение, где при существующих условиях легче всего получить визу.

[53] Council Decision 2004/512/EC of 8 June 2004 Establishing the Visa Information System (VIS), 2004 O.J. (L 213) 5.

[54] Regulation No. 767/2008, of the European Parliament and of the Council of 9 July 2008 Concerning the Visa Information System (VIS) and the Exchange of Data Between Member States on Short-Stay Visas (VIS Regulation), 2008 O.J. (L 218) 60.

[55] Commission Decision 2006/648/EC of 22 September 2006 Laying down the Technical Specifications on the Standards for Biometric Features Related to the Development of the Visa Information System, 2006 O.J. (L 267) 41.

[56] VIS Regulation, art. 8-14, 2008 O.J. (L 218) 60, 65-68.

[57] VIS Regulation, art. 5, 6(2), 9, 10, 23(1), 2008 O.J. (L 218) 64-66, 71.

[58] VIS Regulation, art. 6-7, 18-22, 2008 O.J. (L 218) 65, 69-71.

и фотографии[59]. Практика выдачи электронных виз распространена в целом ряде стран Азии[60], Африки и Латинской Америки и облегчает визовые процедуры для туристических и деловых путешествий.

Как было отмечено выше, неким аналогом электронной визы выступает авторизация, выдаваемая в рамках системы *ETIAS*, хотя в традиционном понимании такая авторизация не приравнивается к визе.

Таким образом, ВИС представляет собой ключевой инструмент цифрового пограничного контроля, обеспечивая интеграцию национальных и наднациональных процедур, поддержку правоохранительных функций, контроль над миграцией и эффективное управление визовыми данными на уровне всего ЕС.

Дальнейшие шаги: обеспечение совместимости информационных систем

С целью повышения эффективности существующих и потенциальных информационных систем еще в 2016 г. Комиссия предложила обеспечить совместимость и взаимодействие между информационными системами с целью устранения структурных недостатков, препятствующих работе национальных органов власти. Обеспечение совместимости существенно повышает возможности указанных систем и упрощает работу компетентных органов с ними.

Правовой основой совместимости информационных систем служат два регламента: Регламент 2019/818[61], касающийся совместимости информационных систем в области полицейского и судебного сотрудничества, миграции и убежища, и Регламент 2019/817[62] об обеспечении совместимости информационных систем в области визовой политики и пограничного контроля.

Регламент 2019/817 устанавливает правовые рамки для обеспечения совместимости существующих и перспективных информационных систем (ВИС, *Eurodac*, ШИС, *EES*, *ETIAS*, а также Европейской системы информации о судимостях граждан третьих стран (*European Criminal Records Information System — Third Country Nationals, ECRIS-TCN*).

Совместимость информационных систем базируется на четырех основных составляющих (*ESP, sBMS, CIR, MID*), которые выступают так называемыми инструментами взаимодействия (Baceiredo Macho, 2025, p. 22). Во-первых, создается единый поисковый портал (*European search portal, ESP*), который позволяет компетентным органам одновременно осуществлять поиск в нескольких информационных системах, используя как биографические, так и биометрические данные. Во-вторых, создается общий сервис сравнения биометрических данных (shared Biometric Matching Service, sBMS), который включает биометрические данные (отпечатки пальцев и изображения

[59] Распоряжение Правительства РФ «О перечне иностранных государств, гражданам которых оформляется единая электронная виза» № 2571-р от 06.10.2020 (ред. от 05.12.2024), Собрание законодательства РФ, 2020, № 41, ст. 6495; 2023, № 32, ст. 6407, http://publication.pravo.gov.ru/document/0001202412070006

[60] Immigration Department. (n.d.). *Viet Nam e-Visa for foreigners outside Viet Nam applying for an e-Visa personally*. Ministry of Public Security. Retrieved October 18, 2025 from https://evisa.gov.vn/

[61] Regulation 2019/818, of the European Parliament and of the Council of 20 May 2019 on Establishing a Framework for Interoperability between EU Information Systems in the Field of Police and Judicial Cooperation, Asylum and Migration and Amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, 2019 O.J. (L 135) 85.

[62] Regulation 2019/817, of the European Parliament and of the Council of 20 May 2019 on Establishing a Framework for Interoperability between EU Information Systems in the Field of Borders and Visa and Amending Regulations (EC) No. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, 2019 O.J. (L 135) 27.

лиц) из нескольких информационных систем ЕС. Посредством *sBMS* власти смогут проверять, являются ли граждане третьих стран теми лицами, за которых себя выдают, с помощью биометрической верификации, а затем гарантировать, что они не просрочат срок пребывания (Martins et al., 2022, p. 489). В-третьих, формируется общее хранилище идентификационных данных (a common identity repository, CIR), которое включает биографические и биометрические данные граждан стран, не входящих в ЕС, доступные в нескольких информационных системах ЕС. В-четвертых, предусматривается создание детектора множественных идентификационных данных (*multiple identity detector, MID*), который направлен на выявление множественных идентификационных данных в различных информационных системах ЕС.

Обеспечение совместимости информационных систем опирается на несколько базовых принципов, прямо вытекающих из регламентов 2019/817 и 2019/818. Среди них ключевыми являются унификация форматов данных, взаимная техническая согласованность алгоритмов обработки биометрии и биографических данных, а также гарантированный уровень кибербезопасности и контроля доступа. Эти элементы необходимы для того, чтобы вышеупомянутые инструменты (*ESP, sBMS, CIR* и *MID*) функционировали в единой архитектуре и могли обеспечивать обмен информацией в режиме реального времени. Немаловажен и принцип целевой допустимости обработки данных: каждая ИТ-система продолжает функционировать в пределах собственных правовых задач, а общие модули совместимости не расширяют круг целей обработки за пределы прямо установленных в соответствующих регламентах, а также предполагают обработку как можно меньшего количества данных для достижения назначенных целей[63].

Вместе с тем анализ нормативной базы и технических характеристик обозначенных систем показывает, что практическая реализация совместимости сталкивается с рядом проблем. Остается существенным риск несоответствия стандартов, поскольку системы создавались в разные периоды, в рамках различных технических требований и под руководством различных агентств: ВИС и ШИС имеют иную архитектуру по сравнению с новыми системами проекта «Умные границы». Это приводит к сложности интеграции баз данных, отличиям в способах и объеме хранимой информации, а также к необходимости многоуровневой консолидации при сопоставлении профилей в *CIR* или при работе общего сервиса сравнения данных.

Техническая нагрузка также представляет собой значимый вызов: внедрение *CIR* и *sBMS* предполагает значительное увеличение объемов данных, включая биометрию высокого разрешения, что требует устойчивой сети коммуникации между национальными интерфейсами и центральными модулями. Риск в том, что сбой в одном из компонентов способен повлиять на доступность информации сразу в нескольких системах, поскольку они будут связаны через *ESP* и общую биометрическую службу. Поэтому вопросы резервирования, отказоустойчивости и непрерывности обмена данными становятся критически важными в условиях возрастающего трафика, прежде всего после полного запуска *EES* и *ETIAS*.

Дополнительного внимания требует правозащитный аспект совместимости. Концентрация биографических и биометрических данных в едином хранилище повышает эффективность контроля, однако одновременно усиливает потребность в строгом соблюдении принципов пропорциональности, минимизации данных и недискриминации. Как ранее отмечалось в отношении *ETIAS*, автоматизация риск-оценки и централизованная обработка информации могут оказывать непропорциональное воздействие на определенные категории лиц. В условиях

[63] European Data Protection Board, *Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects* (Oct. 8, 2019), https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

интеграции систем эти риски усиливаются: ошибки в одной базе данных могут транслироваться в другие, а алгоритмы сопоставления идентичностей — влиять на решения пограничных служб. В этой связи соблюдение требований по контролю за доступом, обновлению данных, а также по механизму исправления ошибок и обжалования решений должно стать неотъемлемой частью практической реализации стратегии совместимости.

Проект «Умные границы» может представлять для России определенный интерес с точки зрения использования положительного опыта в рамках возможного формирования межгосударственного информационного пространства. В частности, в настоящий момент в рамках Союзного государства продолжается формирование правовой базы, обеспечивающей отсутствие регулярного паспортного контроля на внутренних границах. Указанная работа также включает в себя информационную составляющую, связанную с обменом сведениями, используемыми при осуществлении пограничного контроля. Пока вопрос не стоит о создании централизованной союзной информационной системы, однако идет процесс интеграции соответствующих национальных систем. Иными словами, в рамках Союзного государства используется иной подход к межгосударственному информационному взаимодействию. Тем не менее некоторые положительные наработки ЕС в области межгосударственного информационного взаимодействия могут быть использованы в рамках Союзного государства.

Заключение

Проведенный анализ показывает, что запуск *EES* в 2025 г. стал важным этапом в формировании цифрового измерения ПСБП ЕС. Цифровизация ПСБП является не разовым проектом, а долгосрочной политико-правовой стратегией, направленной на интеграцию и унификацию пограничного контроля. В политическом лексиконе ЕС закрепилось понятие «цифровая граница» (*Digital Border*) (Chouliaraki & Georgiou, 2019), а в науке заявляют о дематериализации физических границ посредством цифровизации процесса пограничного контроля (Bigo, 2022, p. 229).

Развитие ПСБП базируется на расширяющейся архитектуре взаимосвязанных информационных систем, которые обеспечивают пограничный контроль, правоохранительное взаимодействие и миграционные процедуры. Эти системы различаются по назначению и степени централизации, однако в целом образуют единый цифровой контур союза, благодаря которому осуществляются обмен и обработка данных в масштабах ЕС. Центральную роль в его функционировании играет Агентство *eu-LISA*, которое обеспечивает техническую эксплуатацию инфраструктуры и служит основным интеграционным институтом. Таким образом, ЕС последовательно формирует наднациональный режим управления информационными системами, что усиливает единство ПСБП и снижает фрагментарность национальных подходов (Zaloilo, 2024, p. 523).

Инициатива «Умные границы» стала концептуальной основой для модернизации пограничного контроля ЕС. Несмотря на многочисленные задержки, вызванные сложностями межгосударственной технической интеграции, проект «Умные границы» сформировал основу двух ключевых систем: *EES* и *ETIAS*. Из этого можно сделать вывод о том, что ЕС выбрал модель централизованного подхода, что позволяет обеспечить совместимость инфраструктуры, но одновременно требует более глубокого наднационального вмешательства (Klimburg-Witjes & Huettenrauch, 2021). Для России интерес представляет возможность использования отдельных

элементов этого опыта при формировании аналогичных механизмов в рамках Союзного государства, где также осуществляется политика по либерализации трансграничного передвижения лиц.

EES представляет собой систему автоматизированной фиксации всех въездов, выездов и отказов во въезде граждан третьих стран. Она призвана повысить эффективность пограничного контроля и сроков пребывания, облегчить работу пограничных служб и создать прозрачный режим доступа путешественников к информации о собственном статусе. Особое внимание уделено балансу между публичной безопасностью и защитой прав иностранцев, особенно уязвимых групп. Однако, несмотря на очевидные преимущества, внедрение *EES* сопровождается целым рядом рисков: централизованная архитектура предъявляет повышенные требования к устойчивости ИТ-инфраструктуры, возможны ошибки биометрической идентификации, а совместимость с другими системами требует технологической доработки.

ETIAS дополняет *EES*, устраняя информационные пробелы в отношении граждан третьих стран, освобожденных от визовых требований. Система осуществляет автоматизированную предварительную проверку по всем ключевым базам данных ЕС и международных организаций, что позволяет выявлять рисковые случаи до пересечения границы. Таким образом, *ETIAS* формирует новый уровень превентивной безопасности, одновременно сохраняя баланс между эффективностью и соблюдением прав человека. В совокупности *ETIAS* и *EES* образуют единый многоуровневый механизм управления перемещением иностранных граждан, в котором цифровизация выступает основным инструментом повышения прозрачности, оперативности и предсказуемости решений.

ETIAS, безусловно, представляет собой шаг по ужесточению правил въезда иностранцев. После введения указанной системы практически все иностранцы обязаны будут получать предварительное разрешение на въезд в Шенгенскую зону: граждане одних государств — в виде электронной авторизации, граждане других — в виде бумажной визы.

Резюмируя, хотелось бы отметить, что цифровые системы ПСБП — это не набор разрозненных ИТ-проектов, а структурированная наднациональная модель управления границами, основанная на:

- единых правовых стандартах;
- централизованной технической архитектуре;
- интеграции данных в масштабах всего Союза;
- приоритетности защиты прав человека;
- постепенном переходе от национального к союзному регулированию.

Запуск *EES* и предстоящее внедрение *ETIAS* завершат формирование цифровой составляющей пограничного контроля ЕС. После запуска *ETIAS* новые цифровые системы ЕС будут охватывать все категории иностранцев, включая законопослушных граждан из безвизовых стран. Таким образом, страны ЕС будут покрыты цифровыми сетями идентификации, которые будут непрерывно классифицировать и сортировать людей на основе их цифровых данных (Topak, 2014, p. 28).

Эти системы смогут стать фундаментом для дальнейшей интеграции ПСБП, обеспечив более высокую степень управляемости миграционных процессов, оперативность обмена информацией и согласованность решений государств-членов. Фактически цифровизация ПСБП затрагивает не только вопросы миграции — это фундаментальный вектор всей архитектуры безопасности ЕС (Martins et al., 2022, p. 490).

Список литературы / References

1. Alsaleh, A. (2024). The impact of technological advancement on culture and society. *Scientific Reports, 14*, Article 32140. https://doi.org/10.1038/s41598-024-83995-z
2. Baceiredo Macho, I. (2025). Shaping EU borders: An analysis of the technological and institutional developments in border management in the European Union. *Peace & Security – Paix et Sécurité Internationales*, (13), Article 1203. http://dx.doi.org/10.25267/Paix_secur_int.2025.i13.1203
3. Bigo, D. (2022). The digitalisation of border controls and their corporate actors. In M. Bosworth, & L. Zedner (Eds.), *Privatising border control: Law at the limits of the sovereign state* (pp. 229–247). Oxford University Press. https://doi.org/10.1093/oso/9780192857163.003.0013
4. Broeders, D. (2007). The new digital borders of Europe: EU databases and the surveillance of irregular migrants. *International Sociology, 22*(1), 71–92. https://doi.org/10.1177/0268580907070126
5. Chouliaraki, L., & Georgiou, M. (2019). The digital border: Mobility beyond territorial and symbolic Divides. *European Journal of Communication, 34*(6), 594–605. https://doi.org/10.1177/02673231198861
6. Delioglu, F. (2025). Technology at the borders: Surveillance, control and resistance in EU migration governance. *Balsillie Papers*, *6*(6). https://doi.org/10.51644/bap66
7. Entin, M. L., Voynikov, V. V., & Torkunova, E. A. (2018). Novyy etap v institutsional'no-pravovom obustroystve prostranstva svobody, bezopasnosti i pravosudiya ES [The new stage of institutional and legal foundation of the EU area of freedom, security and justice]. *Moscow Journal of International Law,* (2), 102–114. https://doi.org/10.24833/0869-0049-2018-2-102-114
8. Jeandesboz, J. (2016). Smartening border security in the European Union: An associational inquiry. *Security Dialogue, 47*(4), 292–309. https://doi.org/10.1177/0967010616650226
9. Klimburg-Witjes, N., & Huettenrauch, C. F. (2021). Contextualizing security innovation: Responsible research and innovation at the smart border? *Science and Engineering Ethics, 27*, Article 13. https://doi.org/10.1007/s11948-021-00292-y
10. Kontak, M. (2024). Biometric borders envisaged by Frontex: Fundamental rights in the backseat. *European Papers, 9*(2), 621–640. https://doi.org/10.15166/2499-8249/773
11. Lehtonen, P., & Aalto, P. (2017). Smart and secure borders through automated border control systems in the EU? The views of political stakeholders in the Member States. *European Security, 26*(2), 207–225. https://doi.org/10.1080/09662839.2016.1276057
12. Martins, B. O., Lidén, K., & Jumbert, M. G. (2022). Border security and the digitalisation of sovereignty: Insights from EU borderwork. *European Security, 31*(3), 475–494. https://doi.org/10.1080/09662839.2022.2101884
13. Skleparis, D. (2016). (In)securitization and illiberal practices on the fringe of the EU. *European Security, 25*(1), 92–111. https://doi.org/10.1080/09662839.2015.1080160
14. Topak, O. E. (2014). The new borders of the European Union: Digital surveillance and social sorting. In M. Okyayuz, P. Herrmann, & C. Dorrity (Eds.), *Migration global processes caught in national answers* (pp. 17–35). Wiener Verlag für Sozialforschung.
15. Voynikov, V. V. (2019a). Pravovoye osnovy prostranstva svobody, bezopasnosti i pravosudiya Evropeyskogo Soyuza [The legal basis of the EU area of freedom, security and justice] (Dr. Sci. dissertation, MGIMO University). https://mgimo.ru/upload/diss/2019/voynikov-diss.pdf
16. Voynikov, V. V. (2019b). Pravovoye regulirovaniye informatsionnykh sistem prostranstva svobody, bezopasnosti i pravosudiya ES [Legal regulation of the information systems within the EU' area of freedom, security and justice]. *Vestnik Saratovskoy Gosudarstvennoy Yuridicheskoy Akademii*, (4), 99–111.

17. Zaloilo, M. V. (2024). Pravovyye problemy obespecheniya tekhnologicheskogo suvereniteta [Legal issues of ensuring technological sovereignty]. *Journal of Digital Technologies and Law, 2*(3), 500–520. https://doi.org/10.21202/jdtl.2024.26

Сведения об авторах:

Войников В. В. — доктор юридических наук, профессор, Высшая школа права, Институт управления и территориального развития, Балтийский Федеральный университет им. И. Канта, Калининград, Россия; профессор, кафедра интеграционного права и прав человека, международно-правовой факультет, МГИМО МИД России, Москва, Россия; ведущий научный сотрудник, Центр европейских и евразийских правовых исследований, Нижегородский государственный университет им. Н. И. Лобачевского, Нижний Новгород, Россия.
voinicov@yandex.ru
ORCID: https://orcid.org/0000-0003-1495-3227

Арестов А. В. — магистр юриспруденции, аспирант, Высшая школа права, Балтийский Федеральный университет им. И. Канта, аналитик Института геополитических и региональных исследований, Балтийский Федеральный университет им. И. Канта, Калининград, Россия.
a.arestov.work@yandex.ru
ORCID: https://orcid.org/0009-0001-2455-8100

Information about the authors:

Vadim V. Voynikov — Dr. Sci. in Law, Professor, Higher School of Law, Institute of Management and Territorial Development, Immanuel Kant Baltic Federal University, Kaliningrad, Russia; Professor, Department of Integration and Human Rights Law, International Law School, MGIMO University, Moscow, Russia; Leading Researcher, Center for European and Eurasian Legal Studies, Lobachevsky University, Nizhny Novgorod, Russia.
voinicov@yandex.ru
ORCID: https://orcid.org/0000-0003-1495-3227

Alexander V. Arestov — LL.M., Post-Graduate Student, Higher School of Law, Analyst, Institute of Geopolitical and Regional Studies, Immanuel Kant Baltic Federal University, Kaliningrad, Russia.
a.arestov.work@yandex.ru
ORCID: https://orcid.org/0009-0001-2455-8100

https://doi.org/10.38044/2686-9136-2025-6-18

СТАТЬИ

ДОМЕННОЕ ИМЯ: ЦИФРОВОЙ АКТИВ, ИДЕНТИФИКАТОР ИЛИ ИНОЙ ОБЪЕКТ?

И. Е. Титов[1,*], **Е. В. Алымова**[2]

[1]Российский университет дружбы народов имени Патриса Лумумбы
117198, Россия, Москва, ул. Миклухо-Маклая, 6

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

Аннотация

Настоящая статья посвящена комплексному исследованию правовой природы доменного имени как особого объекта, функционирующего в цифровой среде и активно участвующего в гражданском обороте. Актуальность работы обусловлена отсутствием единообразного подхода к квалификации доменных имен в законодательстве и судебной практике различных правопорядков, что затрудняет формирование эффективных механизмов их правовой охраны и защиты. Целью исследования является выявление преобладающих доктринальных и правоприменительных подходов к определению правовой природы доменного имени в правовых системах России, Германии и США, а также определение возможных способов правовой защиты соответствующих прав. В качестве материалов использованы нормативные правовые акты, судебная практика и научные источники указанных правопорядков. В статье анализируются основные концепции правовой природы доменного имени: как средства адресации, цифрового актива, идентификатора и объекта интеллектуальной собственности. Показано, что узкотехническое понимание доменного имени не отражает его фактической роли в цифровой экономике. Выявлено, что в российском праве преобладает фрагментарный и противоречивый подход, в то время как германская и американская правовые системы демонстрируют более гибкие модели правовой квалификации, допускающие использование существующих правовых институтов для защиты прав администраторов доменных имен. Особое внимание уделено анализу доменного имени как объекта имущественных прав и цифрового актива, обладающего самостоятельной экономической ценностью и оборотоспособностью. Авторы приходят к выводу о гибридной правовой природе доменного имени, сочетающей в себе признаки различных правовых категорий, и обосновывают необходимость дифференцированного подхода к его правовой квалификации в зависимости от выполняемых функций, что позволяет обеспечить баланс интересов участников гражданского оборота и повысить эффективность правовой защиты.

Ключевые слова

доменное имя, адресация, цифровые активы, коммерческие обозначения, названия произведений, товарные знаки, средства индивидуализации, имущественное право, идентификатор, правовой гибрид

Конфликт интересов Настоящая статья отражает личную позицию авторов. Содержание и результаты данного исследования не следует рассматривать либо цитировать в каких-либо изданиях как официальную позицию международной юридической фирмы ADVANT Beiten. Настоящая статья ни при каких обстоятельствах не может считаться юридической консультацией международной юридической фирмы ADVANT Beiten.

Финансирование Исследование не имеет спонсорской поддержки.

Для цитирования Титов, И. Е., Алымова, Е. В. (2025). Доменное имя: цифровой актив, идентификатор или иной объект? *Цифровое право, 6*(4), 43–81. https://doi.org/10.38044/2686-9136-2025-6-18

* Автор, ответственный за переписку

Поступила: 08.10.2025; принята в печать: 10.12.2025, опубликована: 30.12.2025

ARTICLES

DOMAIN NAME: DIGITAL ASSET, IDENTIFIER, OR SOME OTHER KIND OF OBJECT?

Ilya E. Titov[1,*], Ekaterina V. Alymova[2]

[1] RUDN University
6, Miklukho-Maklaya St., Moscow, Russia, 117198

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

Abstract

This article is dedicated to a comprehensive analysis of the legal nature of a domain name as a special object functioning in the digital environment and proactively involved in civil commerce. The relevance of this work is attributable to the lack of a uniform approach used to qualify domain names in the legislation and judicial practices of different legal systems, which complicates the establishment of effective legal remedies. The goal of this analysis is to identify the prevailing doctrinal and law enforcement approaches applied to determine the legal nature of a domain name in the Russian, German and American legal systems and also to determine possible legal remedies in the respective countries. The authors have used as materials here the regulatory and legal acts, judicial practices and sources of academic research of the indicated legal systems. The underlying concepts of the legal nature of a domain name are analysed in the article: as address facilities, as a digital asset, identifier and item of intellectual property. They demonstrate that a limited technical understanding of a domain name does not reflect its actual role in the digital economy. The authors highlight the prevalence of a fragmented and contradictory approach in Russian law—by contrast, the German and American legal systems provide more flexible models of legal qualification, which enable the use of existing legal institutes to protect the rights of a domain name administrator. Particular attention is paid to analysis of a domain name as a subject of property

rights and as a digital asset that has independent economic value and is capable of generating turnover. The authors conclude that a domain name has a hybrid legal nature, combining features of different legal categories, and substantiate the need to adopt a differentiated approach to its legal qualification, depending on the functions being performed, which makes it possible to ensure a balance of the interests of participants in civil commerce and enhance the effectiveness of the legal protection that is provided.

Keywords

domain names, addressing, digital asset, trade names, titles of works, trademarks, means of identification, proprietary rights, identifiers, legal hybrid, USA, Germany, Russia

Conflict of interest	The views expressed herein are solely those of the authors. The content and results of this research should not be considered or referred to in any publications as representing the official position of the International Law Firm ADVANT Beiten. Under no circumstances should this article be considered legal advice from the International Law Firm ADVANT Beiten.
Financial disclosure	The study has no sponsorship.
For citation	Titov, I. E. & Alymova, E. V. (2025). Domain name: Digital asset, identifier, or some other kind of object? *Digital Law Journal, 6*(4), 43–81. https://doi.org/10.38044/2686-9136-2025-6-18

* Corresponding author

Submitted: 8 Oct. 2025, accepted: 10 Dec. 2025, published: 30 Dec. 2025

Введение

Постпандемийный период мирового развития характеризуется цифровизацией экономики, перемещением привычных бизнес-процессов в цифровую среду, созданием моделей ведения бизнеса онлайн, стиранием привычных физических территориальных границ ведения предпринимательской деятельности.

Увеличение интереса к электронной коммерции как со стороны потребителей, так и со стороны предпринимателей, по оценкам аналитиков, обеспечит стабильный ежегодный рост рынка доменных имен на 4,5% в год, что позволит в 2032 г. достигнуть объема в 3,41 млрд долл. США по сравнению с текущим (2,4 млрд долл. США)[1]. Некоторые доменные имена, как, например, *.ai*, в 2025 г. показали рост популярности на 46% в отношении к предыдущему году[2], что обусловлено повышением интереса к сервисам, организациям и проектам, связанным с искусственным интеллектом (*AI — Artificial Intelligence*). При этом объем всего рынка *e-commerce* к 2028 г. должен приблизиться к 28 трлн долл. США, что означает рост более чем в два раза по сравнению с 2021 г.[3]

1 Market Data Forecast. (2025). *Domain name market size, share, trends & growth, 2033.* https://www.marketdataforecast.com/market-reports/domain-name-market

2 Mohan, R. (2025, February 20). *.ai's dramatic growth: A future-proof domain for the AI era. Identity Digital.* https://www.identity.digital/newsroom/ais-dramatic-growth-a-future-proof-domain-for-the-ai-era

3 Zion Market Research. (2025, June). *Global e-commerce market size, share, growth analysis report — forecast 2034.* https://www.zionmarketresearch.com/report/global-ecommerce-market-size

Подобный переход от аналоговой экономики к цифровой невозможен без развитой системы правовых механизмов, обеспечивающих защиту прав и законных интересов предпринимателей и иных участников гражданского оборота. Особую роль при этом играют доменные имена, выступающие базой для создания различных проектов в цифровой экономике.

В то же время законодательство Российской Федерации, как представляется, не готово к обеспечению стабильного роста цифровой экономики и предсказуемого развития интернет-проектов. Связано это прежде всего с неопределенностью в отношении правовой природы доменного имени, а значит, и с ограниченностью средств правовой защиты, которые администратор доменного имени может использовать.

Архаичность законодательного регулирования в рассматриваемой сфере является особенностью не только российского правового ландшафта, но и законодательства других ведущих мировых государств — Германии и США — в части определения правовой природы доменных имен. Подобная ситуация, однако, вынуждает правоприменителя искать ответы в уже имеющихся правовых институтах и находить способы применения знакомых правовых категорий при разрешении споров в сфере доменных имен.

Настоящее исследование опирается на труды ведущих российских ученых-цивилистов в сфере правового регулирования доменных имен: М. А. Рожковой, С. А. Копылова, К. В. Гееца, А. И. Савельева и др. Германская доктрина представлена авторами, чьи научные труды формируют теоретическую основу современного германского права — так называемое господствующее мнение (*herrschende Meinung*) — и часто ложатся в основу мотивировочных частей судебных актов германских судов: *K.-H. Fezer*, *P. Axer*, *M. Viefhues*, *R. Heine*, *R. Ingerl*, *C. Rohnke* и др. США, где Интернет был изобретен, представлены также плеядой ученых, в частности *M. Leaffer, H. H. Perritt, J. H. Rechman, J. Story* и др.

Впервые в истории отечественной науки в настоящей статье предпринята попытка структурированного сравнительно-правового исследования всего объема научной и практической информации о доменных именах в трех рассматриваемых правопорядках. Несмотря на известные различия правовых систем России, Германии и США, ставится цель установления универсальных подходов к определению правовой природы доменного имени.

Для достижения данной цели определяются следующие задачи: анализ нормативно-правового регулирования в сфере доменных имен; изучение правоприменительной практики и доктрины в указанной сфере; выявление пробелов правового регулирования; установление правовых институтов, используемых в одном правопорядке, но безосновательно игнорируемых в другом; выработка правовых механизмов охраны и защиты прав на доменные имена.

Правовая природа доменного имени: российский подход

Российский подход к определению правовой природы доменных имен представляет собой во многом уникальный и ценный опыт. Связано это прежде всего с глубокой теоретической проработкой данного вопроса и с широким осмыслением проблематики цифровых объектов в системе гражданского права[4]. В отечественной доктрине установлению правовой природы доменных имен было уделено значительное внимание, в результате чего была сформирована

[4] В данном контексте под цифровым объектом понимается объект, не обладающий овеществленной формой, существующий исключительно в информационно-цифровой среде. К числу таких цифровых объектов, не имеющих материального носителя, но при этом обладающих определенной и реальной ценностью, функциональностью и возможностью участия в гражданском обороте, относятся и доменные имена.

обширная концептуальная база, включающая три ключевых подхода к пониманию доменного имени: как результата оказания услуги, как средства индивидуализации и как разновидности имущественного права.

Впрочем, несмотря на столь детальную теоретическую разработку, законодательное регулирование и судебная практика в части правовой природы доменных имен остаются крайне фрагментарными и ограниченными. Законодатель не дает прямого ответа на вопрос о месте доменного имени в системе объектов гражданских прав, а правоприменитель, в свою очередь, воздерживается от квалификации доменного имени как самостоятельного объекта права, ограничиваясь лишь прикладными вопросами защиты исключительных прав на средства индивидуализации в доменных спорах.

В результате возникает явный перекос между уровнем проработанности данного вопроса в российской доктрине и судебной практике, что препятствует формированию стабильного правового режима для доменных имен и замедляет интеграцию этого цифрового объекта в гражданско-правовую систему Российской Федерации. В связи с указанным рассмотрение российского подхода к определению правовой природы доменных имен будет строиться прежде всего на анализе и осмыслении доктринально выработанных позиций, поскольку именно научная литература содержит наиболее системные и обоснованные подходы к установлению места доменных имен. Судебные акты, как правило, лишь эпизодически затрагивают вопрос правовой природы домена и зачастую делают это постольку, поскольку это необходимо для разрешения конкретного спора, не углубляясь в теорию.

Доменное имя как средство адресации

В Российской Федерации имеется легальная дефиниция доменного имени. В пункте 15 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации»[5] (далее — Закон об информации) доменное имя определено как «обозначение символами, предназначенное для адресации сайтов в сети “Интернет” в целях обеспечения доступа к информации, размещенной в сети “Интернет”». Особенность данной дефиниции заключается в том, что законодатель отразил лишь техническую составляющую доменного имени. Это вызвано тем, что общее понимание сущности домена на момент введения данного термина в законодательство (начало действия редакции Федерального закона с 15 ноября 2014 г.)[6] заключалось в его основном предназначении как средства адресации на искомый сайт или иной информационный ресурс (Kopylov & Rozhkova, 2022, pp. 106–107).

При этом принятие Федерального закона от 28 июля 2012 г. № 139-ФЗ, которым термин «доменное имя» был закреплен, было мотивировано прежде всего необходимостью совершенствования законодательства о защите детей от нежелательной информации в сети Интернет, на что обращают внимание его разработчики[7]. Вместе с тем целью законопроекта,

[5] 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).

[6] Федеральный закон «О внесении изменений в Федеральный закон “О защите детей от информации, причиняющей вред их здоровью и развитию” и отдельные законодательные акты Российской Федерации» от 28 июля 2012 г. № 139-ФЗ. Собрание законодательства РФ, 2012 г., № 31, ст. 4328.

[7] Пояснительная записка к проекту Федерального закона «О внесении изменений в Федеральный закон “О защите детей от информации, причиняющей вред их здоровью и развитию” и отдельные законодательные акты Российской Федерации» № 89417-6 (по вопросу ограничения доступа к противоправной информации в сети Интернет). https://sozd.duma.gov.ru/bill/89417-6

а соответственно, и включения определения понятия «доменное имя» в федеральное законодательство было внедрение возможности «принудительного блокирования интернет-страниц, содержащих информацию, распространение которой запрещено»[8]. Очевидно, что ввиду указанных публично-правовых целей на первый план выходят именно технические характеристики доменного имени как средства адресации к контенту, доступ к которому при необходимости следует заблокировать. Частноправовая природа доменного имени уходит на второй план, и, как видно из определения рассматриваемой категории, а также из пакета документов при внесении законопроекта в Государственную Думу ФС РФ, в данном случае она не была предметом анализа в принципе.

Аналогичное узкое понимание было заложено ранее как в ст. 1484, 1519 Гражданского кодекса РФ[9] (далее — ГК РФ), где доменное имя прямо названо одним из способов адресации в сети Интернет, с помощью которого могут быть реализованы исключительное право на товарный знак и географическое указание соответственно, так и в определении доменного имени в Правилах регистрации доменных имен в доменах *.RU* и .РФ (ред. от 02.07.2025)[10] (далее — Правила регистрации).

В научной литературе данное определение неоднократно критиковалось за излишнюю узость и односторонность, поскольку оно делает акцент на одной функции доменного имени — адресации в сети Интернет. Нельзя отрицать, что такой подход игнорирует комплексный характер доменного имени, которое в современных условиях выполняет не только техническую, но также экономическую и идентифицирующую функции. Так, Д. В. Кожемякин указывал, что законодательная дефиниция «охватывает лишь внешнюю (техническую) составляющую доменного имени и не характеризует ни природу прав администратора доменного имени, ни их соотношение с правами на иные объекты гражданских прав» (Kozhemyakin, 2019, p. 22). М. А. Рожкова в свою очередь указывала на абстрактность определения доменного имени, содержащегося в Законе об информации (Rozhkova, 2024, p. 211), а В. И. Еременко — на отсутствие отличий данной трактовки от используемых в мировой практике (Eremenko, 2013, p. 2). Аналогичная оценка законодательной дефиниции доменного имени содержится в работах Н. А. Новиковой (Novikova, 2018) и Е. И. Гладкой (Gladkaya, 2014, p. 33).

Иная оценка была дана К. В. Геецом, который, в отличие от критиков узкотехнического подхода, обосновал уместность акцента на природе доменного имени как средства адресации именно в контексте законодательства об информации. Как далее указывает автор, целью дефиниции доменного имени в Законе об информации не является определение его места в системе объектов гражданских прав, поскольку определение носит публично-правовой характер и направлено, прежде всего, на регулирование технических аспектов функционирования Интернета (Geets, 2023, p. 33).

Тем не менее определение доменного имени исключительно через выполнение им функции адресации не способно объяснить правовую природу этого объекта. Такое определение не позволяет раскрыть правовую сущность доменного имени как объекта, участвующего

[8] Там же.

[9] Гражданский кодекс Российской Федерации. Часть первая от 30 ноября 1994 г. № 51-ФЗ. Собрание законодательства РФ, 1994 г., № 32, ст. 3301; часть вторая от 26 января 1996 № 14-ФЗ. Российская газета, 10 февраля 1996 г.; часть четвертая от 18 декабря 2006 г. № 230-ФЗ. Собрание законодательства РФ, 2006 г., № 52, ст. 5496 (часть I).

[10] Координационный центр национального домена сети Интернет, *Правила регистрации доменных имен в доменах .RU и .РФ,* утв. решением № 2011-18/81 от 5 октября 2011 г., в ред. решения № 05-35 от 2 июля 2025 г., дата введения в действие: 11 августа 2025 г., https://cctld.ru/files/pdf/docs/rules_ru-rf.pdf

в обороте, и не объясняет, как такой объект эффективнее и целесообразнее регулировать. Более того, если подобное узкофункциональное определение доменного имени закрепляется как единственное в законодательстве, оно искусственно сужает область возможной правовой квалификации доменного имени.

Понимание доменного имени исключительно как средства адресации послужило основанием для вывода ряда исследователей о том, что доменное имя не обладает признаками объекта гражданских прав и, соответственно, полностью исключено из гражданского оборота (Yukhnova et al., 2020, pp. 110–112; Rozhkova, 2018, p. 208; Kozhemyakin, 2019, p. 53).

Интересным и одновременно показательным является тот факт, что сам российский правоприменитель до настоящего времени не выработал единой и четкой позиции относительно доменного имени как средства адресации. Так, в деле «Ассоциация владельцев транспорта “Ответственность” против ЗАО “РСИЦ”» и пр.» суд прямо указал, что доменное имя лишь средство адресации, сравнимое с номером телефона в сети Интернет, и не является ни средством индивидуализации, ни вещью, ни объектом интеллектуальной собственности. В обоснование своей позиции суд указал, что в действующем законодательстве отсутствуют понятие права на адресацию и, следовательно, сам правовой объект, подлежащий защите[11].

Схожая позиция воспроизводилась и в других судебных актах, где подчеркивалось, что доменные имена не указаны в числе объектов гражданских прав (ст. 128 ГК РФ), не обладают признаками вещи (ст. 216 ГК РФ) и не относятся к объектам интеллектуальной собственности (ст. 1225 ГК РФ)[12]. Аналогичный формальный подход был применен и в деле «ФГАУ “Государственный научно-исследовательский институт информационных технологий” против ООО “Университетские телекоммуникации”» (дело № А56-12177/2016), где суд отказался признать *IP*-адрес, который также выполняет функцию адресации в сети Интернет, объектом гражданских прав (подробнее см. Rozhkova, 2024, pp. 212–214).

Такой подход, однако, вызывает обоснованные сомнения, поскольку вступает в противоречие с фактической ролью доменных имен в обороте: они активно вовлечены в сделки, становятся предметом споров, передаются по соглашениям, в судебной практике признаются элементы недобросовестного поведения при их регистрации и использовании.

На этом фоне в судебной практике встречаются и прямо противоположные решения, подтверждающие возможность доменных имен выступать в качестве объекта гражданских прав и не фокусирующиеся исключительно на их функции адресации. Так, в деле «ЗАО “Управляющая компания ‘Висма’” против ООО “Архыз”» в рамках завершения конкурсного производства суд указал, что доменное имя как информационная технология представляет собой определенную экономическую ценность, может быть предметом сделки и, следовательно, относится к объектам гражданских прав[13].

Таким образом, узкое понятие доменного имени, закрепленное в законодательстве в единственном числе, привело к тому, что российские суды либо вовсе игнорируют вопрос правовой природы доменного имени, либо отказывают в его квалификации в качестве объекта гражданских прав, ссылаясь на его исключительно техническую функцию. Именно закрепление такого определения породило фрагментарность и противоречивость судебной практики

[11] Решение Арбитражного суда г. Москвы от 10 июня 2011 г. по делу № А40-136893/2010; постановление Федерального арбитражного суда Московского округа от 16 декабря 2011 г. по делу № А40-136893/10-6-1133 (оставить вышеуказанное решение АСГМ без изменения).

[12] Постановление Одиннадцатого арбитражного апелляционного суда от 9 июня 2018 г. по делу № А55-12866/2017.

[13] Постановление Шестнадцатого арбитражного апелляционного суда от 11 сентября 2018 г. по делу № А25-851/2015.

в Российской Федерации, при которой значение доменного имени в экономическом и гражданском обороте не находит отражения в правовой плоскости и создает очевидную правовую неопределенность.

Доменное имя как идентификатор

Другой важной функцией доменного имени является его способность идентифицировать деятельность организаций или частных лиц в сети Интернет. Благодаря этому доменное имя приобретает статус виртуального идентификатора, выполняющего в интернет-пространстве роль, сходную со средствами индивидуализации.

Действительно, в сущность доменного имени, в отличие от иных средств адресации (прежде всего IP-адреса), изначально заложена идея о более простом и удобном способе навигации в сети Интернет, который бы позволял отделить один ресурс от другого. Именно эта человекоориентированность обусловила естественное смещение акцента с технической функции доменного имени на его роль виртуального идентификатора.

Описывая доменное имя в качестве идентификатора, надо отметить следующее. Понятие «идентификатор» является более широким, чем юридическая категория «средство индивидуализации», закрепленная в гражданском законодательстве. Если средства индивидуализации предполагают наличие специального правового режима, то идентификатором может выступать любой элемент, позволяющий выделить, опознать или соотнести объект с конкретным лицом или деятельностью.

Впервые в российской правовой плоскости на индивидуализирующую функцию доменных имен указал Высший Арбитражный Суд РФ в деле «Корпорация "Истман Кодак Компани" против ПБОЮЛ Грундула А. В.» о доменном имени *kodak.ru:* «Доменные имена фактически трансформировались в средство, выполняющее функцию товарного знака, который дает возможность отличать соответственно товары и услуги одних юридических или физических лиц от однородных товаров и услуг других юридических или физических лиц»[14]. Как видно из приведенной цитаты, Суд не отождествляет доменные имена с товарными знаками, а лишь сравнивает их функциональные характеристики, делая акцент на сходстве выполняемых задач.

Доменное имя действительно может использоваться для ведения коммерческой деятельности, выступать в качестве элемента брендинга, средства коммуникации, площадки для электронной коммерции, рекламы, иметь самостоятельную экономическую ценность и выполнять иные функции. Как указывает М. А. Рожкова, роль виртуального идентификатора присуща доменным именам, которые используются не только в коммерческих целях, но и в рамках некоммерческой деятельности, включая, например, ведение персонального сайта (Rozhkova, 2015a, p. 62).

В настоящее время рассмотрение доменного имени как виртуального идентификатора производится преимущественно на доктринальном уровне. Несмотря на активное развитие научной мысли в этом направлении и убедительное обоснование идентифицирующей функции доменных имен, судебная практика, за редким исключением, не уделяет этому аспекту должного внимания. Так, например, в деле «ПАО "Сбербанк" против А. Р. Курбангалиева» о банкротстве суд лишь указал, что «доменное имя представляет собой уникальный идентификатор... Доменное имя выполняет функцию уникального имени в Интернете и представляет собой более

[14] Постановление Президиума Высшего Арбитражного Суда РФ от 16 января 2001 г. по делу № 1192/00.

простой вариант записи [*IP*-адреса. — *И. Т., Е. А.*][15]». В данном случае термин «идентификатор» был использован без раскрытия правовой и экономической значимости соответствующей категории. В недавнем решении по делу «ООО "Бесогон" против Р. С. Ерохина» о доменном имени *besogon.tv* суд также указал: «Основными функциями доменного имени являются обеспечение доступа к определенной информации, а также индивидуализация информационного ресурса, содержащего эту информацию, и его владельца»[16].

Следовательно, даже в тех случаях, когда суды упоминают идентифицирующую роль домена, они, как правило, не рассматривают ее как основание для признания за доменом самостоятельного правового режима.

Доменное имя как средство индивидуализации

Более радикальным отражением теории о доменном имени как виртуальном идентификаторе является подход, согласно которому доменное имя рассматривается в качестве средства индивидуализации. Суть данной позиции заключается в том, что при определенных условиях доменное имя фактически выполняет ту же функцию, что и товарный знак или иное средство индивидуализации.

Идея о том, что доменное имя может индивидуализировать лиц, товары и услуги, высказанная на заре российского права интеллектуальной собственности, так понравилась юридическому сообществу и даже законодателю, что в проекте четвертой части ГК РФ присутствовал параграф под названием «Право на доменное имя» (гл. 76), в котором доменные имена рассматривались в качестве одного из средств индивидуализации. Как указывает А. И. Савельев, одной из причин отказа от данного проекта в итоге стало отсутствие опыта законодательного регулирования доменных имен в качестве средств индивидуализации за рубежом (Savelyev, 2020, p. 531).

Несмотря на полный отказ от данного параграфа в проекте четвертой части ГК РФ, несколько лет в действующей статье 1483 ГК РФ среди оснований для отказа в государственной регистрации товарного знака указывалось тождество обозначения не только классическим объектам интеллектуальной собственности, но и доменному имени, права на которое возникли ранее даты приоритета регистрируемого товарного знака. Указанное положение было исключено из ГК РФ уже в 2010 г. (Savelyev, 2020, p. 531).

В настоящее время нельзя отрицать отсутствие доменного имени в закрытом перечне охраняемых результатов интеллектуальной деятельности и средств индивидуализации в ГК РФ. Заслуживают внимания аргументы Д. В. Кожемякина о том, что доменное имя может не индивидуализировать информационный ресурс в случае, когда домен зарегистрирован администратором без намерения использовать его в качестве средства адресации (Kozhemyakin, 2019). В таком случае не будет важнейшего свойства средства индивидуализации — наличия индивидуализируемого объекта, связи между ним и средством индивидуализации, что в конкретном

[15] Постановление Семнадцатого арбитражного апелляционного суда от 19 декабря 2022 г. по делу № А60-2544/2021; определение Верховного Суда РФ от 28 июня 2023 г. № 309-ЭС23-11305 (отказ в передаче дела № А60-2544/2021 в Судебную коллегию по экономическим спорам Верховного Суда РФ для пересмотра в порядке кассационного производства данного постановления).

[16] Решение Арбитражного суда Московской области от 9 апреля 2025 г. по делу № А41-68198/2021. Также см. аналогичную судебную практика вышестоящих судов: постановления Суда по интеллектуальным правам от 20 октября 2022 г. № С01-1735/2022 по делу № А41-40447/2020; от 3 марта 2022 г. № С01-717/2021 по делу № А45-15457/2020; от 29 июня 2021 г. № С01-850/2021 по делу № А40-162975/2020; от 13 мая 2019 г. № С01-331/2019 по делу № А40-77364/2018; от 18 октября 2018 г. № С01-968/2017 по делу № А53-1941/2017 и т. д.

случае исключает возможность квалификации доменного имени как средства индивидуализации. Однако отсутствие индивидуализируемого объекта в один момент не означает, что он не может появиться в будущем в случае, когда администратор доменного имени настроит адресацию на какой-либо веб-сайт, где расположит интернет-магазин.

Правовая охрана доменного имени в составе фирменного наименования

Заслуживают внимания и альтернативные варианты, которые, хотя и не получили широкого обсуждения в доктрине, потенциально могут применяться на практике в качестве возможного способа охраны и защиты доменных имен. Так, в ряде случаев доменное имя может выступать в качестве составного элемента или полного фирменного наименования. В соответствии с п. 1 ст. 1483 ГК РФ юридическое лицо — коммерческая организация — выступает в гражданском обороте под фирменным наименованием, которое определяется в его учредительных документах и включается в Единый государственный реестр юридических лиц при государственной регистрации юридического лица. Кроме того, согласно п. 3 ст. 1483 ГК РФ юридическое лицо должно иметь одно полное фирменное наименование и вправе иметь одно сокращенное наименование на русском языке.

Данный подход особенно актуален для домена верхнего уровня .РФ, где регистрация доменных имен осуществляется на кириллице, что позволяет активно использовать формат доменного имени для фирменного наименования юридических лиц, например ООО «РУБЛЁВКА.РФ»[17], АО «ВЕЗУМАТЕРИАЛЫ.РФ»[18], АО «ДОМ.РФ»[19].

В подобных случаях фирменное наименование, совпадающее с доменным именем, очевидно выполняет функцию индивидуализации юридического лица. Однако следует подчеркнуть, что охраняется не само доменное имя как технический идентификатор, а только лишь словесное обозначение, зарегистрированное в качестве фирменного наименования юридического лица.

Хотя Суд по интеллектуальным правам отмечает, что «коммерческая организация вправе указывать свое фирменное наименование в доменном имени в сети Интернет и запрещать иным владельцам доменов использовать тождественное или сходное до степени смешения с фирменным наименованием обозначение в доменных именах»[20], правовую сущность доменного имени это не проясняет, так как доменное имя попадает в рассматриваемом случае в сферу правовой охраны иного объекта — охраняемого в силу закона средства индивидуализации, фирменного наименования.

Правовая охрана доменного имени в составе и в качестве товарного знака

Аналогичная проблематика на первый взгляд прослеживается и при рассмотрении доменных имен с точки зрения законодательства о товарных знаках. Сегодня не возникает сомнений, что при соблюдении требований законодательства обозначение, используемое в качестве доменного имени, может быть зарегистрировано как товарный знак[21].

Товарные знаки, содержащие в себе доменные имена, мы можем найти среди международных регистраций, например № 1830227 *domain.com* (охраняется для услуг классов 35, 38, 42,

[17] ИНН 5032236537.

[18] ИНН 9111028470.

[19] ИНН 7729355614.

[20] Постановление Суда по интеллектуальным правам от 16 июня 2023 г. № С01-915/2023 по делу № А14-9738/2022.

[21] Далее в настоящем разделе под термином «товарный знак» понимаются также и знаки обслуживания, если не указано иное.

45 Международной классификации товаров и услуг (далее — МКТУ)), № 1851376 *traveling.com* (охраняется как для товаров класса 09, так и для услуг класса 39 МКТУ) или № 1778622 *komus.com* (также охраняется для большого перечня товаров и услуг) и пр. При этом зачастую элемент *.com* в рассматриваемых случаях выделен в качестве неохраняемого.

Анализ реестра российских товарных знаков Федеральной службы интеллектуальной собственности (Роспатента)[22] также показывает наличие большого количества доменных имен, зарегистрированных в качестве товарных знаков, например № 265062 *Amazon.com* (охраняется для услуг классов 38, 39 и 41 МКТУ), № 931965 *Alibaba.com* (охраняется для большого перечня товаров и услуг) и многих других.

Таким образом, само обозначение, используемое в качестве доменного имени, при соблюдении известных требований может быть зарегистрировано в качестве товарного знака. Однако данное обстоятельство правовой природы доменного имени не раскрывает, так как в законодательстве о регистрации товарных знаков представляемые на регистрацию обозначения рассматриваются не с точки зрения их правовой природы, а с точки зрения соответствия требованиям, установленным законом для регистрации в качестве товарных знаков.

Больший интерес с научной точки зрения и с точки зрения анализа правовой природы доменного имени представляет возможность получения в отношении доменного имени правовой охраны как общеизвестного товарного знака.

Российское гражданское законодательство предполагает, что лицо, использующее обозначение в качестве товарного знака, должно обратиться в Роспатент с соответствующим заявлением для рассмотрения Роспатентом вопроса о признании такого обозначения общеизвестным товарным знаком (п. 1 ст. 1508 ГК РФ). Следует отметить, что такое обозначение может как быть зарегистрировано в качестве товарного знака, так и не иметь такой регистрации. Следовательно, не исключена ситуация, когда администратор доменного имени, которое не охраняется в качестве товарного знака, получит правовую охрану в отношении такого доменного имени в связи с его широкой известностью в России среди соответствующих потребителей в отношении определенных товаров по решению Роспатента.

При этом среди общеизвестных товарных знаков без труда можно найти и товарные знаки со словесными элементами, состоящими из доменных имен, например № 176 *ozon.ru*, № 168 *auto.ru*, № 87 *@mail.ru* и пр.[23]

Конституционный Суд РФ разъяснил, что «общеизвестность товарного знака (используемого в качестве товарного знака обозначения) является фактом объективной действительности и процедура признания такого товарного знака (обозначения) общеизвестным товарным знаком имеет целью подтверждение или опровержение данного факта, а не его возникновение»[24].

Таким образом, доменное имя может использоваться в качестве товарного знака и в определенный момент приобрести статус общеизвестного товарного знака формально без какой-либо регистрации, поскольку возникновение такого статуса от регистрации не зависит, но подтверждается Роспатентом в рамках соответствующей процедуры.

---

[22] Ведение реестра осуществляется Федеральным институтом промышленной собственности.

[23] Все указанные знаки являются словесно-изобразительными. Для целей настоящей статьи мы приводим только словесные элементы указанных знаков. С полными версиями знаков можно ознакомиться в Перечне общеизвестных в Российской Федерации товарных знаков Роспатента.

[24] Пункт 3.2 определения Конституционного Суда РФ «По запросу Суда по интеллектуальным правам о проверке конституционности подпункта 3 пункта 6 статьи 1483 и статьи 1508 Гражданского кодекса Российской Федерации» от 19 сентября 2019 г. № 2145-О.

С точки зрения установления правовой природы доменного имени это означает, что в рамках российской правовой системы не исключается правовая квалификация доменного имени в качестве общеизвестного товарного знака, т. е. обозначения, обладающего функциями отделения товаров одного производителя от другого, указания на источник происхождения товара, рекламной и иными функциями, которые характерны именно для товарных знаков, а не средств адресации.

Правовая охрана доменного имени в составе и в качестве коммерческого обозначения

Другим альтернативным способом охраны доменного имени теоретически может выступать использование доменного имени в составе коммерческого обозначения. ГК РФ не содержит четкого определения коммерческого обозначения, что придает данному механизму гибкость и адаптивность на практике. Вместе с тем законодатель установил определенные требования к охраняемому коммерческому обозначению: оно должно обладать достаточными различительными признаками и его использование для индивидуализации предприятия должно быть известно в пределах определенной территории (п. 1 ст. 1539 ГК РФ). Отдельно законодатель прямо указывает на возможность применения обозначения в сети Интернет. Это свидетельствует о том, что функция коммерческого обозначения как средства индивидуализации распространяется и на цифровую среду, а само обозначение может быть интегрировано, например, в доменное имя.

Но может ли само доменное имя получить правовую охрану в качестве коммерческого обозначения?

Согласно позиции Суда по интеллектуальным правам «для того, чтобы обозначение, входящее в состав доменного имени, приобрело статус коммерческого обозначения, оно должно отвечать требованиям, предъявляемым действующим законодательством к коммерческим обозначениям»[25]. Однако далее Суд заключает, что доменное имя не является средством индивидуализации, исключительное право на само по себе доменное имя как на коммерческое обозначение возникнуть не может[26].

Представляется, что данное однозначное суждение Суда по интеллектуальным правам существенно сужает правовые границы коммерческого обозначения как такового и носит дискуссионный характер. В то же время, как правильно указал Суд, для того чтобы доменное имя приобрело статус коммерческого обозначения, оно должно соответствовать критериям, установленным пунктом 1 ст. 1539 ГК РФ, которые мы упомянули ранее. Рассмотрим их более подробно.

Критерий 1: обладание достаточными различительными признаками. Законодательно не определены конкретные достаточные различительные признаки, тем не менее *per analogiam* возможно применение критериев для определения различительной способности обозначений, регистрируемых в качестве товарных знаков (ст. 1483 ГК РФ).

Таким образом, отсутствуют правовые препятствия для приобретения в конкретной ситуации различительных признаков обозначением, используемым в качестве доменного имени.

Критерий 2: известность в пределах определенной территории. Как отмечает Суд по интеллектуальным правам, «[в] этом проявляется связь правообладателя с потребителями: только известное обозначение может претендовать на признание его коммерческим обозначением и, соответственно, только на такое обозначение возникает исключительное право. ...[О]

[25] Постановление Суда по интеллектуальным правам от 28 апреля 2017 г. № С01-301/2017 по делу № А60-1837/2016.

[26] Там же.

собенность правового режима коммерческого обозначения как средства индивидуализации состоит в том, что оно охраняется не на всей территории Российской Федерации, а в пределах границ своей известности»[27].

Может ли доменное имя приобрести известность в пределах определенной территории? Представляется, что очевидные препятствия для этого отсутствуют. Среди критериев для оценки такой известности Суд по интеллектуальным правам называет (1) длительное и интенсивное использование обозначения на определенной территории; (2) произведенные затраты на рекламу; (3) значительные объемы реализации товаров и оказания услуг под этим обозначением; (4) результаты опроса потребителей товаров относительно известности[28]. Данные критерии представляют собой *numerus apertus*, т. е. открытый перечень, и могут быть дополнены и другими в конкретной ситуации.

Доменное имя может приобрести известность в пределах определенной территории, например, если предприниматель ведет коммерческую деятельность по продаже товаров потребителям на ней. Возможность доступа к веб-сайту предпринимателя из любого уголка страны или из-за рубежа, безусловно, не является основанием для распространения правовой охраны на все такие территории. В данной ситуации могут быть применены другие критерии: география показов и геотаргетинг при размещении рекламы соответствующего веб-сайта, территория фактических продаж товаров, количество отзывов о товарах на веб-сайте[29] и пр.

Таким образом, критерий известности на определенной территории в отношении доменного имени в конкретной ситуации может быть соблюден.

Критерий 3: употребление для своего предприятия. В пункте 1 ст. 1538 ГК РФ при перечислении видов предприятий, в отношении которых может использоваться коммерческое обозначение, дана отсылка на ст. 132 ГК РФ, где предусмотрено легальное определение предприятия как имущественного комплекса, используемого для осуществления предпринимательской деятельности.

Согласно сложившейся практике Суда по интеллектуальным правам «государственная регистрация предприятия в качестве объекта недвижимости, исходя из характера правоотношений, не является необходимым условием возникновения права на коммерческое обозначение»[30]. Например, в одном из дел Суд по интеллектуальным правам признал достаточным наличие договора аренды помещений, также указав, что «заявителем заключен... договор аренды нежилого помещения», а «головными офисами продаж заявителя по производству лежаков для животных, через которые продукция вводится в гражданский оборот под обозначением *"Pet's Love"*, являются виртуальные магазины ответчика на сайтах маркетплейсов *https://www.wildberries.ru/* и *https://www.ozon.ru/*»[31].

Подобное толкование правовой категории предприятия предоставляет широкие возможности для правовой охраны и защиты коммерческих обозначений всех предпринимателей, а не только тех, которые имеют зарегистрированные предприятия как объекты недвижимого имущества. Фактически суд пошел даже дальше данной идеи признав виртуальные магазины на маркетплейсах «головными офисами продаж».

---

27 Постановление Суда по интеллектуальным правам от 4 апреля 2025 г. № С01-178/2025 по делу № А63-22156/2023.

28 Там же.

29 Решение Суда по интеллектуальным правам от 16 января 2025 г. по делу № СИП-759/2024.

30 Постановления Суда по интеллектуальным правам от 22 ноября 2019 г. № С01-778/2019 по делу № А33-2388/2018, от 24 июля 2018 г. № С01-547/2018 по делу № А79-11966/2017.

31 Решение Суда по интеллектуальным правам от 16 января 2025 г. по делу № СИП-759/2024.

Таким образом, анализ практики Суда по интеллектуальным правам показывает, что обозначения, которые используются в интернет-магазинах на маркетплейсах, признаются судом коммерческими обозначениями, например *Pet's Love* при реализации товаров для животных на платформах *Wildberries* или *Ozon*[32].

Несмотря на то что российский правоприменитель в настоящее время не готов рассматривать доменное имя в качестве самостоятельного коммерческого обозначения, представляется, что гибкость данного правового механизма позволяет при соблюдении установленных в п. 1 ст. 1539 ГК РФ критериев прийти к выводу о принципиальной возможности квалификации доменного имени в качестве коммерческого обозначения по российскому праву.

Тем не менее из этого следует, что не любое доменное имя может претендовать на такую правовую квалификацию. Только те доменные имена, которые обладают достаточными различительными признаками и стали известными в результате фактического использования для индивидуализации предприятия в пределах определенной территории, могут быть рассмотрены в качестве коммерческих обозначений.

Доменное имя как результат услуги

Отнесение доменных имен к результатам услуг базируется на идее, что процесс создания и использования доменного имени неразрывно связан с деятельностью регистратора, который является стороной договора об оказании услуг регистрации, принимает заявку на регистрацию, вносит соответствующие изменения в реестр доменных имен и принимает оплату за регистрацию и ежегодное продление регистрации доменного имени (Kozhemyakin, 2019, p. 72).

Эта позиция нашла отражение в судебной практике. Так, в самом, пожалуй, известном до настоящего времени наследственном споре о праве на доменные имена[33] суд пришел к выводу о том, что доменное имя представляет собой услугу, оказываемую регистратором на основании договора оказания услуг, и сделал заключение о невозможности наследования доменного имени (подробнее см. Kozhemyakin, 2019, p. 34–37). В практике арбитражных судов можно встретить аналогичную позицию: «Приобретение прав на доменное имя означает приобретение прав и обязанностей администратора доменного имени, возникших из договора об оказании услуг регистрации доменного имени. Продажа прав на доменное имя означает замену стороны в правоотношении по договору об оказании услуг регистрации доменного имени, в результате которой прежний пользователь выбывает из правоотношений с регистратором, на его место становится приобретатель прав на доменное имя. Договор о передаче прав на доменное имя, заключаемый между прежним и новым пользователями, представляет собой договор, содержанием которого является одновременная уступка права требования и перевод долга в обязательства между пользователем и регистратором доменного имени»[34]. На ошибочность такого подхода в судебной практике указывает Д. В. Кожемякин (Kozhemyakin, 2023, p. 41).

Концепция, рассматривающая доменное имя исключительно как услугу, а право на него — как обязательственное, возникшее в силу договора оказания услуг регистрации и существующее исключительно между регистратором и администратором, не объясняет и не может объяснить высокую стоимость того или иного домена на вторичном рынке. Если домен действительно был бы лишь услугой, логично предположить, что само существование

[32] Решение Суда по интеллектуальным правам от 16 января 2025 г. по делу № СИП759/2024.

[33] Решение Мытищинского городского суда Московской области от 30 ноября 2011 г. по делу № 2-4006/2011.

[34] Постановление Суда по интеллектуальным правам от 2 апреля 2024 г. по делу № А40-160906/2022.

вторичного рынка теряло бы смысл, поскольку право на доменное имя в таком случае не имело бы самостоятельной ценности для лиц, не участвующих в договоре регистрации.

Доменное имя как имущественное право

Согласно ст. 128 ГК РФ к имуществу может быть отнесено иное имущество, включая имущественные права. Перечень имущественных прав в российском законодательстве открытый, что позволяет гибко подходить к квалификации различных объектов и явлений в качестве имущества в гражданско-правовом смысле.

Эта особенность правового регулирования позволяет рассматривать доменные имена в качестве объектов имущественных прав, поскольку они обладают признаками оборотоспособности, экономической ценности и возможностью участия в гражданском обороте.

В российской гражданско-правовой доктрине отсутствуют серьезные аргументы против признания права на доменное имя имущественным. Единственным основанием, заставляющим сомневаться в этой концепции, является ограниченный срок регистрации домена. Тем не менее, по мнению некоторых ученых, срочный характер регистрации доменов не имеет в данном случае определяющего значения в том числе потому, что регистрация домена может быть продлена неограниченное количество раз (Danilenkov, 2018, p. 98).

Тем не менее в судебной практике на данный момент отсутствует устоявшийся подход к квалификации доменного имени в качестве объекта имущественных прав, что, однако, не мешает выделить господствующее мнение по данному вопросу.

С одной стороны, суды не признают доменные имена объектами имущественных прав, что наглядно продемонстрировано в постановлении по делу «А. С. Грачев против ООО “Сантехпласт”»[35]. В рамках данного дела апелляционный суд, анализируя требования о распределении обнаруженного имущества ликвидированного юридического лица в виде доменного имени *pnd.ru,* не признал доменное имя объектом, обладающим полноценным имущественным содержанием. Несмотря на то что доменное имя продолжало быть зарегистрированным за ликвидированным обществом, суд фактически исходил из того, что право администрирования домена вытекает из договорных отношений между администратором и регистратором.

С другой стороны, в актуальной российской судебной практике отражен и противоположный подход, который поддерживается многими кассационными судами, в том числе Судом по интеллектуальным правам. В частности, в постановлении по делу «*Rado Uren AG, Longines Watch Co. Franciion Ltd., Certina AG* против ООО “Аквамарин”» Суд по интеллектуальным правам, сохраняя в силе судебные акты нижестоящих инстанций, согласился с выводами арбитражного суда первой инстанции о том, что «право администрирования доменного имени является имущественным правом, имеющим денежную стоимость и участвующим в обороте, на которое может быть обращено взыскание в рамках исполнительного производства для удовлетворения денежных требований о взыскании»[36].

К тождественному выводу Суд по интеллектуальным правам пришел и в другом постановлении по спору тех же сторон[37].

---

[35] Постановление Первого арбитражного апелляционного суда от 24 марта 2025 г. по делу № А43-4370/2024.

[36] Постановление Суда по интеллектуальным правам от 9 декабря 2015 г. № С01-502/2015 по делу № А56-83807/2014; определение Верховного Суда РФ от 2 марта 2016 г. № 307-ЭС16-380 (отказано в передаче дела № А56-83807/2014 в Судебную коллегию по экономическим спорам Верховного Суда РФ для пересмотра в порядке кассационного производства данного постановления).

[37] Постановление Суда по интеллектуальным правам от 1 июля 2015 г. № С01-502/2015 по делу № А56-83807/2014.

Квалификацию доменного имени в качестве объекта имущественных прав подтверждают и иные кассационные арбитражные суды: в деле «А.С. Хартманн против "Экес АГ"»[38], в деле «ООО "Мэлт" против ООО "Сальвадор"»[39], в деле о несостоятельности ООО «Заяка.ру» по заявлению ООО «Аренда-Т»[40], в деле «А. Т. Ханеев против ООО "Мэлт", ООО "Сальвадор", АО "РСИЦ"»[41], в деле о несостоятельности ИП Макарычева А. Ф.[42] и пр. В частности, в постановлении по делу ИП Макарычева А. Ф. Арбитражный суд Московского округа указал, что «право на доменное имя должно квалифицироваться именно как имущественное право, заключающееся в возможности лица, зарегистрировавшего доменное имя, разместить в сети Интернет информационный ресурс, доступ к которому осуществляется пользователем сети Интернет путем набора определенных символов, составляющих доменное имя»[43].

Таким образом, анализ актуальной судебной практики позволяет сделать вывод о наличии господствующего мнения о возможности квалификации доменного имени в качестве объекта имущественных прав.

Доменное имя в составе имущественного комплекса

В настоящее время в российском законодательстве отсутствует легальное определение понятия «имущественный комплекс», однако в ГК РФ предусмотрено всего две его разновидности: предприятие (ст. 132 ГК РФ) и единый недвижимый комплекс (ст. 133.1 ГК РФ). Поскольку последний представляет собой совокупность зданий, сооружений и иных неразрывно связанных с ними вещей, рассмотрим правовое положение доменного имени в составе первого вида имущественного комплекса, т. е. предприятия.

В соответствии с п. 2 ст. 132 ГК РФ в состав предприятия как имущественного комплекса могут входить, в частности, все виды имущества, права требования, а также права на обозначения, индивидуализирующие предприятие, его продукцию, работы и услуги, и другие исключительные права. При этом норма является диспозитивной и предполагает возможность изменения и расширения данного перечня договором.

Как видно из приведенного положения, законодатель отдельно не включил доменное имя в рассматриваемую норму ГК РФ.

В то же время право на доменное имя может входить в состав имущественного комплекса и передаваться вместе с предприятием от одного лица другому, что находит подтверждение и в судебной практике. Например, в деле «ИП Ефимов М. Д. против ИП Сидляренко И. В.» суд

[38] Постановление Арбитражного суда Московского округа от 18 декабря 2023 г. № Ф05-31515/2023 по делу № А40-11288/2023; определение Верховного Суда РФ от 18 апреля 2024 г. № 305-ЭС24-3735 (отказано в передаче дела № А40-11288/2023 в Судебную коллегию по экономическим спорам Верховного Суда РФ для пересмотра в порядке кассационного производства данного постановления).

[39] Постановление Арбитражного суда Поволжского округа от 27 мая 2021 г. № Ф06-3779/2021 по делу № А65-5166/2020.

[40] Постановление Арбитражного суда Московского округа от 23 декабря 2020 г. № Ф05-21866/2020 по делу № А40-279321/2019.

[41] Постановление Арбитражного суда Поволжского округа от 24 января 2020 г. № Ф06-54089/2019 по делу № А65-39419/2018; определение Верховного Суда РФ от 14 апреля 2020 г. № 306-ЭС20-4385 (отказано в передаче дела № А65-39419/2018 в Судебную коллегию по экономическим спорам Верховного Суда РФ для пересмотра в порядке кассационного производства данного постановления).

[42] Постановление Арбитражного суда Московского округа от 21 февраля 2023 г. № Ф05-27243/2021 по делу № А40-70751/2018.

[43] Там же.

согласился с тем, что ответчик передал истцу «доменное имя»[44]. Зачастую при такой передаче стороны не всегда вникают в суть правовой природы доменного имени и указывают не право на доменное имя, которое подлежит передаче (передача договора), а именно доменное имя, воспринимая его как цифровой актив (об этом см. далее). Безусловно, на действительность такого договора данное обстоятельство по общему правилу влияния оказывать не должно, если воля сторон была направлена именно на смену администратора домена и передачу контроля над соответствующим веб-сайтом (если применимо).

Возможность включения *права* на доменное имя как нематериального имущества в состав предприятия отмечается и в российской доктрине (Rozhkova, 2015b, para. 1.1, 2).

Кроме того, как показано ранее в подразд. 1.3.3, при соблюдении критериев, указанных в п. 1 ст. 1539 ГК РФ, не исключены квалификация доменного имени в качестве коммерческого обозначения и, соответственно, включение его в имущественный комплекс в таком правовом статусе. При этом возможна ситуация, когда одно доменное имя будет охраняться в рамках предприятия в качестве коммерческого обозначения, а остальные, не соответствующие критериям п. 1 ст. 1539 ГК РФ, с учетом того, что у предприятия может быть только одно коммерческое обозначение (п. 2 ст. 1538 ГК РФ), будут охраняться как иные объекты.

Доменное имя как цифровой актив и объект инвестирования

Отдельные доменные имена могут обладать значительной коммерческой ценностью[45], которая формируется в условиях ограниченности ресурса в рамках конкретного домена верхнего уровня: каждое доменное имя является уникальным, а значит, в пределах одного домена верхнего уровня может быть зарегистрировано лишь один раз.

М. А. Рожкова разделяет цифровые объекты и цифровые активы, указывая, что к числу цифровых объектов относятся объекты, вращающиеся в цифровой среде; в то же время в качестве цифровых активов могут быть квалифицированы некоторые цифровые объекты, если они получили дополнительное к первоначальному самостоятельное назначение и допускают денежную оценку (Rozhkova, 2025, p. 155). С учетом сказанного доменное имя следует признать не только цифровым объектом, неовеществленным и существующим исключительно в информационно-цифровой среде, но и цифровым активом, т. е. таким цифровым объектом, который обладает определенной и реальной ценностью, функциональностью и возможностью участия в гражданском обороте.

Несмотря на отсутствие в российском законодательстве прямого регулирования вторичного рынка доменных имен, действующее правовое поле допускает существование такого оборота. Следовательно, указанная передача может быть оформлена и реализована в рамках гражданско-правового договора.

---

[44] Постановление Тринадцатого арбитражного апелляционного суда от 19 января 2015 г. № 13АП-23305/2014 по делу № А56-22296/2014; постановление Суда по интеллектуальным правам от 8 июня 2015 г. № С01-439/2015 (указанное постановление № 13АП-23305/2014 оставлено без изменения).

[45] Под коммерческой ценностью в контексте данной работы понимается стоимость отдельных доменов на вторичном рынке. Такая стоимости формируется за счет узнаваемости, лаконичности, соответствия ключевым поисковым запросам или присутствия в домене популярных слов, аббревиатур и пр. Согласно обзору доменного аналитика Боба Хоукса, в 2024 г. общий объем сделок с доменными именами на вторичном рынке превысил 185 млн долл. (Hawkes, B. (2024). *Domain name market dollar volume trends.* https://www.namepros.com/blog/2024-domain-name-market-dollar-volume-trends.1343492/). Положения о высокой стоимости отдельных доменов в полной мере применимы и к национальным доменам верхнего уровня .*RU*/.РФ.

Среди крупнейших доменных сделок в зоне *.ru* (от первых двух букв *Russia*) в средствах массовой информации отмечают сделки по домену *sms.ru* (550 тыс. долл. США), *casino.ru* (250 тыс. долл. США), *games.ru* (1 млн долл. США), *dom.ru* (120 млн руб.), *vk.ru* (от 70 млн до 300 млн руб.) и пр.[46]

«Продажа» доменного имени не запрещена и осуществляется, как правило, через заключение договора уступки прав и обязанностей администратора (передача договора).

О правомерности таких сделок свидетельствуют и положения Правил регистрации, которые прямо предусматривают возможность смены администратора, при этом не устанавливая запрета на ее возмездность[47].

В то же время ни регистратор доменного имени, ни координатор не требуют представления самого договора между текущим администратором и администратором будущим, выступающего правовым основанием передачи домена от одного лица другому. Регистратору направляется прежде всего заявление о передаче прав на доменное имя[48]. Анализ конкретных сделок показывает, что стороны, как правило, именуют их «договор на передачу прав на доменное имя», «договор уступки прав на доменное имя», «договор передачи права администрирования доменного имени» и т. д.

Анализ соответствующих договоров позволяет прийти к выводу, что к рассматриваемой сделке могут быть применены пункты 1 и 2 ст. 382 ГК РФ, согласно которым право (требование), принадлежащее на основании обязательства кредитору, может быть передано им другому лицу по сделке. Для перехода к другому лицу прав кредитора по общему правилу согласие должника не требуется, если иное не определено законом и договором либо соответственно применяются статья 392.3 ГК РФ («Передача договора») и, следовательно, правила о переводе долга, которые даже предусматривают ничтожность перевода должником своего долга на другое лицо без согласия кредитора.

Помимо законодательных ограничений, анализ, например, договора об оказании услуг с регистратором доменных имен ООО «Рег.ру» показывает, что также и договор содержит запрет на уступку администратором своих прав и обязанностей по договору без согласия регистратора. В то же время представляется, что такое согласие может быть выражено в форме одобрения регистратора в момент выполнения заявки текущего администратора на передачу права администрирования новому администратору.

В соответствии с п. 6.2 Правил регистрации, которые носят обязательный характер как для регистраторов, так и для администраторов доменных имен, лицо, которому передается право администрирования, должно заключить с регистратором, осуществляющим поддержку сведений об этом доменном имени, договор об оказании услуг регистрации доменных имен и подтвердить свое согласие на получение права администрирования в соответствии с указанным договором.

---

[46] Воробьев, А. (2023, 26 февраля). *Именем прибыли: почему на доменном рынке непросто заработать.* https://www.forbes.ru/mneniya/485304-imenem-pribyli-pocemu-na-domennom-rynke-neprosto-zarabota

[47] В текущей редакции Правил регистрации передача права администрирования регулируется разделом 6. В нем, в частности, содержатся требования к процедуре и условиям передачи права администрирования: лицо, которому передается право, должно заключить с регистратором договор об оказании услуг регистрации доменных имен и подтвердить свое согласие на получение права администрирования. Пунктом 6.5 Правил установлены условия, при которых передача права администрирования не допускается, например в случае установления ограничений на действия с доменными именами в случае возникновения доменного спора.

[48] Руцентр. (б.д.). *Передача прав на домен по заявлению.* https://www.nic.ru/help/peredacha-prav-na-domen-po-zayavleniyu_9106.html

Из данного положения следует, что на момент передачи доменного имени от одного лица другому как у текущего администратора, так и у администратора будущего должны быть заключены самостоятельные договоры об оказании услуг регистрации доменных имен с регистратором или регистраторами, если одновременно с передачей домена происходит и смена его регистратора. При этом, например, в соответствии с проанализированным договором об оказании услуг с регистратором доменных имен ООО «Рег.ру» в случае передачи новому администратору права администрирования доменного имени акцептом договора на оказание услуг с регистратором (оферты) будет направленное в адрес регистратора письменное волеизъявление нового администратора принять права администрирования домена.

В связи с этим Л. В. Санникова и Ю. С. Харитонова отмечают, что «такая связанность права на домен... с пользовательским соглашением... позволяет говорить о специальном правовом свойстве данного актива по сравнению с иными — ограниченности права пользовательским соглашением» (Sannikova & Kharitonova, 2020, ch. II, para. 2.2).

Для рынка доменных имен важным аспектом является и то, что сама по себе регистрация доменного имени без последующего его использования для адресации по общему правилу не признается нарушением.

Всё вышесказанное дает основания для вывода о том, что по общему правилу при условии добросовестности администратора при регистрации и использовании доменного имени и соблюдении прав и законных интересов третьих лиц особенно ценные доменные имена могут рассматриваться как полноценные цифровые активы и объекты инвестирования.

Впрочем, следует иметь в виду ограниченный потенциал доменных имен как объектов инвестирования с учетом правовых инструментов защиты правообладателей товарных знаков от так называемых киберсквоттеров и применения судами, в частности, Единообразной политики по разрешению споров в связи с доменными именами, одобренной интернет-корпорацией по присвоению названий и номеров (*Internet Corporation for Assigned Names and Numbers, ICANN*).

Если администратор зарегистрировал доменное имя «с основной целью его продажи, сдачи в аренду или передачи использования другим способом истцу, являющемуся правообладателем исключительного права на товарный знак, либо конкуренту истца за денежную сумму, превышающую подтвержденные расходы администратора доменного имени, прямо относящиеся к приобретению доменного имени»[49], то такие действия могут быть признаны недобросовестными, что может привести к потере администратором права администрирования спорного доменного имени в случае судебного спора с правообладателем тождественного или сходного до степени смешения товарного знака.

Вывод по российскому подходу

Таким образом, несмотря на наличие в российском законодательстве легального определения понятия «доменное имя», очевидно, что оно носит технический характер, направлено

[49] Постановление Суда по интеллектуальным правам от 30 августа 2023 г. № С01-1456/2023 по делу № А40-206164/2021. Аналогичная практика: постановление Суда по интеллектуальным правам от 30 ноября 2016 г. № С01-943/2016 по делу № А35-9858/2015 и определение Верховного Суда РФ от 3 февраля 2017 г. № 310-КГ16-20110 (отказано в передаче дела № А35-9858/2015 в Судебную коллегию по экономическим спорам Верховного Суда РФ для пересмотра в порядке кассационного производства данного постановления); постановление Суда по интеллектуальным правам от 24 ноября 2015 г. № С01-951/2015 по делу № А41-83776/2014 и пр.

изначально на решение конкретных прикладных публично-правовых задач и не отражает правовой природы доменного имени.

В то же время нельзя отрицать и возрастающую роль доменного имени в качестве идентификатора, которая выражается, помимо прочего, как в использовании доменных имен в фирменных наименованиях, товарных знаках и коммерческих обозначениях, так и в не получившей в настоящий момент поддержки в судебной практике идее о возможности квалификации доменного имени как такового в качестве коммерческого обозначения или общеизвестного товарного знака, что заслуживает внимания судебных органов.

Особый интерес в современной цифровой экономике, безусловно, уделяется доменному имени как цифровому активу и объекту инвестирования, объекту имущественных прав, поскольку доменные имена, ввиду их уникальности и невозможности существования двух одинаковых доменных имен, могут обладать существенной коммерческой ценностью. Тем не менее, рассматривая доменное имя в качестве объекта инвестирования и цифрового актива, следует учитывать актуальную российскую судебную практику, в которой приобретение права администрирования доменного имени исключительно для целей его «продажи» правообладателю сходного до степени смешения или тождественного товарного знака, как правило, квалифицируется как недобросовестное деяние и может повлечь потерю такого цифрового актива.

Правовая природа доменного имени: германский подход

Законодательное определение доменного имени в настоящий момент в Германии отсутствует.

В качестве отправной точки в германской доктрине доменное имя определяется как буквенно-цифровое дополнение к техническим цифровым *IP*-адресам, которое выполняет, с одной стороны, функцию адресации, что позволяет идентифицировать конкретное устройство в Сети, а с другой — интернет-представительства или идентификации собственника такого имени, а следовательно, выступает идентификатором (Koos, 2004, para. 359). Исходную функцию адресации доменного имени подчеркивает и М. Фифхюс, трактуя его в качестве обозначения адреса веб-сайта и обозначения, используемого для отличия одного веб-сайта от другого, для чего технические адреса веб-сайтов переводятся в «наименования» (*Namen*), благодаря которым такие веб-сайты пользователю проще идентифицировать (Viefhues, 2024, para. 1).

Многофункциональность доменного имени не несет в себе противоречия. В зависимости от выбранного администратором конкретного доменного имени правовые последствия такого выбора, как и юридическая квалификация самого доменного имени, могут различаться.

Использование доменного имени исключительно для целей адресации к конкретному ресурсу в сети Интернет, как, например, номер телефона для адресации к соответствующему абоненту в сети связи, функции идентификации администратора домена как участника экономической деятельности или идентификации его предприятия (*betriebliche Herkunft*) само по себе не выполняет[50].

В то же время следует учитывать, что зачастую обозначения, используемые в доменных именах, уже обеспечены правовой охраной, например посредством регистрации такого обозначения как товарного знака либо в случае совпадения доменного имени и имени администратора – физического лица (Heine, 2025, para. 245) или фирменного наименования, поэтому данные случаи мы исключим из дальнейшего анализа.

[50] Bundesgerichtshof [BGH] [Федеральный суд Германии] 22.07.2004, *Gewerblicher Rechtsschutz und Urheberrecht* [GRUR] 262, 263 (2005), I ZR 135/01, § 2 абз. 4.

Правовая охрана доменного имени как коммерческого обозначения

Несмотря на свою изначальную природу в качестве средства адресации, доменное имя может получить самостоятельную правовую охрану, если в результате его использования в обороте оно приобретает функцию идентификации администратора домена (Heine, 2025, para. 246) по аналогии с товарным знаком, выступающим средством индивидуализации товаров или услуг и одновременно идентификации, т. е. установления в глазах потребителя связи товара с конкретным производителем (*Herkunftsfunktion*).

В соответствии с абз. 1 § 5 «Коммерческие обозначения» Закона о защите товарных знаков и прочих обозначений от 25 октября 1994 г.[51] (далее — Закон о защите товарных знаков) в качестве коммерческих обозначений (*geschäftliche Bezeichnungen*) охраняются наименования предприятий (*Unternehmenskennzeichen*) и названия произведений (*Werktitel*). Согласно предл. 2 абз. 2 § 5 названного Закона под термином «наименование предприятия» понимаются обозначения, которые используются в деловом обороте в качестве наименования, фирменного наименования или особого обозначения бизнеса или предприятия. Конкретный перечень особых обозначений в Законе не определен, однако под ними подразумеваются *de facto* любые обозначения, которые в соответствующих предпринимательских и потребительских кругах воспринимаются в качестве обозначений соответствующего бизнеса.

Может ли доменное имя получить охрану в качестве такого особого обозначения?

Да, такое возможно, но при соблюдении ряда условий, выработанных судебной практикой и доктриной:

1) доменное имя должно использоваться посредством адресации на действующий веб-сайт (Heine, 2025, para. 246);
2) доменное имя и расположенный на нем веб-сайт должны применяться в предпринимательских целях[52];
3) доменное имя должно использоваться как указание на конкретный бизнес администратора домена (*Hinweis auf einen Geschäftsbetrieb*)[53].

Таким образом, сам факт регистрации доменного имени предпринимателем не позволяет квалифицировать такое доменное имя в качестве особого обозначения по смыслу предл. 2 абз. 2 § 5 Закона о защите товарных знаков, поскольку в любом случае между моментом регистрации доменного имени и осуществлением делегирования, созданием собственно веб-сайта, к которому будет адресовать такой домен, проходит определенное время. Однако после совершения всех необходимых действий, которые приведут к выполнению вышеназванных требований, т. е., по сути, к возможности третьим лицам посредством доменного имени обратиться к веб-сайту предпринимателя, администратор домена может рассчитывать на защиту доменного имени как особого, а значит, коммерческого обозначения по смыслу указанного законоположения.

Правовая охрана доменного имени как названия произведения

Помимо квалификации в качестве «особого обозначения» доменное имя при некоторых условиях может получить правовую охрану в качестве названия произведения (*Werktitel*). Согласно абз. 3 § 5 Закона о защите товарных знаков названием произведения признаются

---

[51] Markengesetz [Закон о защите товарных знаков] от 25 октября 1994 г., *Bundesgesetzblatt Teil I* [BGBl. I] 2357, с изм., § 5 абз. 1.

[52] BGH 29.10.1992, *GRUR* 404 (1993), I ZR 264/90.

[53] BGH 24.04.2008, *Neue Juristische Wochenschrift* [NJW] 3716, 3717 (2008), I ZR 159/05.

наименование или особые обозначения печатных изданий, кинофильмов, звукозаписей, сценических или других аналогичных произведений. В частности, согласно германской судебной практике по общему правилу доменное имя может быть квалифицировано в качестве названия «другого аналогичного произведения» и, соответственно, получить правовую охрану при соблюдении следующих критериев:

1) речь должна идти о готовом произведении, а не о планах по его созданию или совершению каких-либо подготовительных действий для этого[54];
2) регистрации доменного имени как таковой для указанных целей недостаточно, так как название произведения должно соотноситься «потребителем» с конкретным произведением[55];
3) само содержание веб-сайта должно отвечать критериям «другого аналогичного произведения» (Heine, 2025, para. 247).

Таким образом, правовая охрана доменному имени в качестве названия произведения, согласно германской судебной практике, может быть предоставлена, однако только в том случае, когда само доменное имя позволяет отличить произведение, размещенное на веб-сайте, от иных и не выступает простым средством адресации[56].

Правовая охрана доменного имени как товарного знака

В соответствии с п. 2 § 4 Закона о защите товарных знаков правовая охрана в качестве товарного знака может быть получена не только обозначением, которое зарегистрировано как товарный знак или приобрело общеизвестный характер, но и, в частности, обозначением, которое использовалось в деловом обороте и в результате такого использования получило признание в виде товарного знака среди участников оборота (*Verkehrskreise*)[57].

Такие товарные знаки в германской практике обозначаются термином *Benutzungsmarke*[58], т. е. «товарные знаки в силу использования».

В отличие от товаров повседневного спроса, где круг участников оборота, согласно выводу Федерального верховного суда Германии, представляет собой все население страны[59], в частности, для сферы информационных технологий из такого круга участников исключаются лица, которые с данными товарами или услугами не сталкиваются[60], т. е., например, не пользующиеся Интернетом. Следовательно, администратору в этом отношении получить охрану своего доменного имени в качестве товарного знака без его регистрации несколько проще, чем, например, производителю молока. Тем не менее в судебной практике было определено пороговое значение в 50%[61] от соответствующего круга участников оборота. То есть половина таких участников должна соотнести конкретное доменное имя с соответствующими товарами или услугами предпринимателя.

---

54 Oberlandesgericht München [OLG München] [Высший земельный суд Мюнхена] 11.01.2001, *GRUR* 522, 524 (2001), 6 U 5719/99.

55 Ibid.

56 BGH 18.06.2009, *GRUR* 156, 157 (2010), I ZR 47/07.

57 Markengesetz [Закон о защите товарных знаков] от 25 октября 1994 г., BGBl. I, 2357, с изм., § 4 Nr. 1.

58 Oberlandesgericht Dresden [OLG Dresden] [Высший земельный суд Дрездена] 25.03.2014, *Multimedia und Recht* [MMR] 193 (2015), 14 U 1364/13.

59 BGH 09.07.2009, *GRUR* 138 (2010), I ZB 88/07.

60 Oberlandesgericht Köln [OLG Köln] [Высший земельный суд Кёльна] 09.11.2012, *Gewerblicher Rechtsschutz und Urheberrecht, Rechtsprechungs-Report* [GRUR-RR] 214 (2013), I-6 U 38/12.

61 OLG Dresden 25.03.2014, *MMR* 193 (2015), 14 U 1364/13.

В германской доктрине в качестве предпосылок для квалификации доменного имени как незарегистрированного товарного знака выделяются:

- использование (Weiler, 2025, para. 17). Применительно к доменному имени это означает фактическую адресацию доменного имени на конкретный веб-сайт предпринимателя;
- установление в глазах потребителя связи доменного имени с конкретными товарами или услугами определенного предпринимателя (*Herkunftsfunktion*) (Ingerl, Rohnke, 2010, para. 11).

Важно, что в данном случае доменное имя в обороте должно как индивидуализировать собственно товары и услуги, которые предлагаются к продаже на расположенном на домене веб-сайте, так и выполнять иные функции товарного знака, прежде всего указывать на происхождение товара или услуги, т. е. на связь домена, товаров и услуг с конкретным производителем[62].

В германской доктрине отмечается, что для получения известности в качестве товарного знака использование домена должно во многих случаях выходить за рамки Интернета (Elkemann & Lieckfeld, 2022, para. 193), т. е. предполагается, что потребители в конечном итоге получают физические товары или некие материальные результаты услуг (работ). В то же время можно представить много ситуаций, когда использование доменного имени в качестве товарного знака виртуальные границы Интернета покидать не будет, например в случае распространения ключей (лицензий) для онлайн-игр и пр.

Охрана права на доменное имя как имущественного

В соответствии с § 1 Условий регистрации доменных имен *DENIC eG* будущий администратор домена направляет в *DENIC eG* заявку на домен[63], в свою очередь, *DENIC eG* акцептует эту заявку (т. е. оферту) посредством ее подтверждения. Согласно абз. 1 § 7 Условий договор между администратором домена и *DENIC eG* заключается на неопределенный срок[64]. Таким образом, между администратором и *DENIC eG* возникает обязательственное правоотношение по поводу доменного имени.

Согласно абз. 1 ст. 14 Основного закона Федеративной Республики Германия от 23 мая 1949 г. (далее — Основной закон) собственность (*Eigentum*) гарантируется[65]. Приобретаемое администратором в результате заключения договора право использования домена (*Nutzungsrecht*) подпадает под конституционную гарантию собственности (*eigentumsfähige Position*) по смыслу Основного закона. Согласно сложившейся судебной практике Федерального конституционного суда Германии конституционно-правовую охрану в соответствии с абз. 1 ст. 14 Основного закона получают и обязательственные требования, основанные на договоре[66]. Возникающее у администратора в результате регистрации доменного имени договорное право пользования доменом представляет собой право требования, которое исключительным образом связано с его обладателем, т. е. администратором домена, так же как и право собственности исключительным

---

62 Ibid.

63 DENIC Services. (n.d.). *DENICdirect Online-Registrierung* [Онлайн-регистрация DENICdirect]. https://www.denic-services.de/denic-direct/online-registrierung

64 DENIC eG. (n.d.). *DENIC-Domainbedingungen* [Условия регистрации доменов DENIC]. https://www.denic.de/domainbedingungen/

65 Grundgesetz [Основной закон ФРГ], ст. 14.

66 Bundesverfassungsgericht [BVerfG] [Федеральный конституционный суд Германии] 24.11.2004, *MMR* 165 (2005), 1 BvR 1306/02.

образом связано с соответствующей вещью, и поэтому, по мнению Федерального конституционного суда Германии, подпадает под гарантию права собственности, закрепленную в абз. 1 ст. 14 Основного закона[67].

При этом важно учитывать следующее. Как указывает П. Аксер, конституционно-правовое понятие «собственность», используемое в Основном законе, шире гражданско-правового и включает в себя «все имущественные правовые позиции» (*alle vermögenswerten Rechtspositionen*), включая права требования (*Forderungen*) (Axer, 2024).

Впрочем, несмотря на то что право требования из договора с *DENIC eG* может получить конституционно-правовую защиту на основе абз. 1 ст. 14 Основного закона, т. е. как собственность, администратор домена *права собственности* на доменное имя *не получает*[68].

Как отмечает Федеральный конституционный суд Германии, такое право использования домена представляет собой по сути охраняемую имущественную ценность (*Vermögenswert*)[69]. С таким выводом соглашаются и К.-Х. Фецер и Р. Хаук, указывая, что администратор домена при заключении договора с *DENIC eG* не получает ни права собственности, ни какого-либо иного вещного права, а лишь договорное право использования доменного имени (Fezer & Hauck, 2023, para. 199).

Квалификация права на доменное имя в качестве имущественного отражена и в правоприменительной практике к германскому законодательству об исполнительном производстве и несостоятельности (банкротстве).

В соответствии с абз. 1 § 857 Гражданского процессуального уложения допускается принудительное исполнение судебного акта в отношении прочих имущественных прав, которые не относятся к недвижимому имуществу[70]. В связи с этим Федеральный верховный суд разъясняет, что в отношении доменных имен взыскание может быть обращено не на само доменное имя, но на «совокупность обязательственных прав требования» (*Gesamtheit der schuldrechtlichen Ansprüche*), которые администратор имеет к *DENIC eG*[71].

Поскольку в рамках принудительного исполнения судебного акта обращение взыскания допускается в отношении прав на доменное имя, это позволяет обойти запрет, установленный в абз. 1 § 36 Закона о банкротстве от 5 октября 1994 г., который не допускает включения в конкурсную массу имущества, в отношении которого взыскание в рамках принудительного исполнения невозможно. При этом согласно § 35 указанного Закона в конкурсную массу включается все имущество, которое принадлежит должнику на момент открытия конкурсного производства и которое он приобретает уже в процессе такого производства[72]. Как отмечает М. Фифхюс, право использования и управления доменным именем, в соответствии с абз. 1 § 80 Закона о банкротстве, переходит к конкурсному управляющему, что позволяет указывать конкурсного управляющего и в качестве административного контакта в отношении конкретного домена в реестре координатора (Viefhues, 2024, para. 417). То есть при обращении к сервису *WHOIS* третье лицо увидит данные именно конкурсного управляющего в качестве администратора домена (если такая информация не скрыта).

---

67 Bundesverfassungsgericht [BVerfG] [Федеральный конституционный суд Германии] 24.11.2004, *MMR* 165 (2005), 1 BvR 1306/02.

68 Ibid. Para. 165.

69 BVerfG 21.11.2023, *Beck-Rechtsprechung* [BeckRS] 38765 (2023), 1 BvL 6/21.

70 Zivilprozessordnung [Гражданское процессуальное уложение ФРГ], § 857.

71 BGH 05.07.2005, *MMR* 685 (2005), VII ZB 5/05.

72 Insolvenzordnung [Положение о несостоятельности], § 36.

Доменное имя как цифровой актив и объект инвестирования

В Германии развит вторичный рынок доменных имен, который, однако, специально на законодательном уровне не урегулирован.

Среди крупнейших сделок в зоне *.de* (от первых двух букв *Deutschland*) в средствах массовой информации отмечают сделки по доменам *kredit.de* (892 500 евро), poker.de (695 тыс. евро), *casino.de* (400 тыс. евро), *chat.de* (320 тыс. евро), *blackjack.de* (300 тыс. евро) и пр.[73]

Анализ конкретных сделок показывает, что стороны, как правило, именуют их «договор купли-продажи интернет-домена» (*Kaufvertrag über die Internet-Domain*), «договор купли-продажи и передачи домена» (*Domainkauf- und Übertragungsvertrag*).

Впрочем, с правовой точки зрения в данной ситуации речь не идет о договоре купли-продажи.

В случае если администратор доменного имени захочет передать принадлежащее ему доменное имя третьему лицу, то речь будет идти о передаче договора (*Vertragsübernahme*), т. е. об одновременной передаче администратором всех прав и обязанностей по договору с *DENIC eG* в отношении конкретного домена (Fezer & Hauck, 2023, para. 311), но не о передаче доменного имени как такового.

В связи с этим Р. Хайне отмечает некорректность формулировок Условий регистрации доменных имен *DENIC eG,* касающихся возможности «передачи домена» иному лицу (Heine, 2025, para. 299). Действительно, параграф 6 Условий регистрации доменных имен *DENIC eG* носит название «Передача домена», а в соответствии с абз. 1 указанного параграфа «[д]омен может быть передан». Условием для такой передачи домена выступает расторжение договора между *DENIC eG* и прежним администратором и заключение — между *DENIC eG* и будущим администратором. При этом обязательным является предоставление будущим администратором в адрес *DENIC eG* «документов, которые подтверждают его [будущего администратора. — *И. Т., Е. А.*] такой статус», т. е. речь идет о не названном в Условиях договоре между прежним и будущим администраторами.

Таким образом, данные положения Условий регистрации доменных имен *DENIC eG* следует воспринимать скорее с технической точки зрения, чем с юридической. Очевидно, что *DENIC eG* пыталась, возможно не в полной мере удачно, создать общее правило передачи права администрирования доменного имени от одного лица другому, без попыток квалификации доменного имени как такового (в связи с чем определения доменного имени в Условиях также не дается).

Как видно из приведенных положений, в германской практике договор между текущим администратором и будущим предоставляется регистратору вместе с заявлением о смене администратора домена. Из договора должно однозначно следовать, что права на домен, т. е. права и обязанности из договора с регистратором, в полном объеме переходят к новому администратору.

В соответствии с абз. 1 § 415 Германского гражданского уложения действительность передачи долга зависит от *одобрения* (т. е. согласия *post factum*) кредитора. Одобрение может быть получено только после того, как должник или третье лицо сообщит кредитору о переводе долга. До этого момента стороны договора могут вносить в него изменения или расторгнуть его. Данная особенность отличает германский подход к сделкам на вторичном рынке доменных имен от российского, поскольку регистратор получает фактический доступ к договору между

[73] Dettweiler, M. (2008, 12 ноября). *Top Ten der teuersten .de-Domains: Die Deutschen wollen nur spielen* [Топ-10 самых дорогих доменов *.de*: Немцы хотят только играть]. *Frankfurter Allgemeine Zeitung*. https://www.faz.net/aktuell/technik-motor/digital/top-ten-der-teuersten-de-domains-die-deutschen-wollen-nur-spielen-1723602.html

администраторами (текущим и будущим) и вправе как одобрить, так и отклонить передачу договора, руководствуясь в том числе анализом сделки между администраторами.

Вывод по германскому подходу

Таким образом, несмотря на отсутствие в Германии законодательного определения доменного имени, администратор в конкретной ситуации может иметь достаточно широкие правовые возможности для защиты своего права администрирования доменного имени даже в тех ситуациях, когда он не является правообладателем иных средств индивидуализации: товарных знаков, фирменных наименований и пр., которые бы распространяли сферу своей правовой охраны и защиты на спорное доменное имя. Данное обстоятельство коренным образом отличает германский правоприменительный подход от российского и позволяет в большей степени учитывать интересы добросовестного администратора доменного имени и тем самым обеспечивать баланс интересов администратора доменного имени и правообладателя средства индивидуализации товаров или услуг.

Германскому правоприменителю удалось встроить доменное имя в существующие законодательно урегулированные правовые категории коммерческих обозначений, названий произведений, товарных знаков, имущественных прав, предоставив уникальный инструментарий, который позволяет эффективно разрешать многие правовые конфликты по поводу доменных имен.

Не отказываясь от изначальной функции доменного имени как средства адресации, законодатель намеренно не стал включать такое узкое понимание соответствующего термина в систему правового регулирования, предоставив широкую свободу судебному толкованию, которое в большой степени основано на мнениях ведущих германский ученых, а следовательно, носит гибкий характер, не зависящий от жестких рамок закона.

Правовая природа доменного имени: американский подход

Законом о защите потребителей от кибersквоттинга (*Anticybersquatting Consumer Protection Act*) в Закон о товарных знаках 1946 г. (*Trademark Act of 1946*, также известный как Закон Лэнхэма — *Lanham Act*) было добавлено следующее действующее определение понятия «доменное имя»: «любое буквенно-цифровое обозначение, которое зарегистрировано или назначено регистратором доменных имен, реестром доменных имен или иным органом регистрации доменных имен в качестве электронного адреса в Интернете»[74].

Таким образом, федеральный законодатель сегодня исходит из технической функции доменного имени — адресации в сети Интернет.

В американской доктрине квалификация доменного имени как средства адресации выступает в качестве отправной точки многих научных исследований. Например, М. Лиффер схожим образом определяет доменное имя как «буквенную противоположность цифрового интернет-адреса, связанную с ним для целей удобства» пользователей (Leaffer, 1998, p. 143).

Ш. Р. Рид также указывает на первичную функцию доменного имени как средства адресации (Reed, 2011, p. 225).

Впрочем, очевидно, что в стране, где Интернет был изобретен, практика использования доменных имен потребовала переосмысления правовой природы доменного имени, в связи с чем возникли следующие подходы.

[74] 15 U.S.C. § 1127.

Правовая природа доменного имени как идентификатора

В своих исследованиях Дж. Райхман относил объекты, которые не вписываются в дихотомическую, по его мнению, устаревшую парадигму интеллектуальной собственности, сформированную в XIX в. Конвенцией по охране промышленной собственности от 20 марта 1883 г. и Бернской конвенцией по охране литературных и художественных произведений от 9 сентября 1886 г., к так называемым правовым гибридам (*legal hybrids*) (Reichman, 1995, p. 504).

Развивая данную идею, М. Лиффер предлагал квалифицировать доменные имена как правовые гибриды, указывая, что «[с] одной стороны они служат практической цели обозначения того, куда необходимо направить информацию. С другой стороны, они часто указывают на место происхождения, и потребители воспринимают их как товарные знаки» (Leaffer, 1998, p. 145).

Апелляционный суд США по девятому федеральному апелляционному округу в деле *Panavision International v. Toeppen*[75] отмечал, что доменное имя служит нескольким целям: «Оно определяет положение сайта в киберпространстве, как почтовый адрес в реальном мире, но оно также может указывать пользователям на информацию относительно содержания сайта и, в случаях с общеизвестными товарными знаками или товарными знаками, может давать информацию о происхождении содержания сайта»[76]. При этом суд прямо подчеркнул, что «отклоняет... утверждение, что доменное имя представляет собой не более чем адрес. Важная цель доменного имени — идентификация компании, которая владеет веб-сайтом»[77]. Существенным является также указание суда на некорректность сравнения доменных имен с телефонной книгой, где пользователь, например по наименованию общества, может найти его телефон или адрес. В сети Интернет *de facto* отсутствует подобный справочник доменных имен, и «потребитель... зачастую будет предполагать, что доменное имя соответствует фирменному наименованию»[78].

Цитируя решение Федерального окружного суда Южного округа Нью-Йорка по делу *MTV Networks, Inc. v. Curry*[79], Апелляционный суд США по девятому федеральному апелляционному округу приходит к выводу, что «доменное имя, отражающее наименование компании, может представлять собой ценный корпоративный актив, поскольку оно обеспечивает коммуникацию с клиентами»[80].

Таким образом, в практике федеральных судов США отражено более широкое понимание доменного имени, выходящее за пределы действующего федерального законодательства и предполагающее квалификацию доменного имени не только как средства адресации, но и как идентификатора администратора домена, а также ценного корпоративного актива.

Охрана права на доменное имя как имущественного

Актуальность определения правовой природы доменного имени в США связана также с положениями Закона Лэнхэма:

«(A) Лицо подлежит ответственности по гражданскому иску правообладателя товарного знака... если, независимо от товаров или услуг сторон, это лицо:

(i) действует с недобросовестным намерением извлечь выгоду из данного знака <...>;

---

75 *Panavision Int'l, L.P. v. Toeppen,* 141 F.3d 1316, 46 U.S.P.Q.2d (BNA) 1511 (9th Cir. 1998).

76 Ibid.

77 Ibid.

78 Ibid.

79 *MTV Networks, Inc. v. Curry*, 867 F. Supp. 202, 203–04 n.2 (S.D.N.Y. 1994).

80 Ibid.

(ii) регистрирует, использует в коммерческих целях или иным образом применяет доменное имя, которое:

(I) в случае товарного знака на момент регистрации доменного имени является идентичным или сходным до степени смешения с таким товарным знаком...»[81]

В практике американских судов возник вопрос о толковании категории «регистрация», в связи с чем суды пришли к различным выводам о правовой природе самого доменного имени и соответственно разнились правовые последствия для администратора доменного имени, которое сходно до степени смешения с зарегистрированным товарным знаком.

Апелляционный суд США по девятому федеральному апелляционному округу в деле *GoPets Ltd. v. Hise*[82] анализировал, является ли перерегистрация доменного имени регистрацией по смыслу приведенных законоположений. В случае положительного ответа на данный вопрос недобросовестность нового администратора позволяла бы привлечь его к гражданско-правовой ответственности.

Впрочем, суд указал, что анализ приведенных положений законодательства с точки зрения континентального имущественного права позволяет прийти к выводу о том, что при первоначальной добросовестной регистрации доменного имени у администратора возникает право на такое доменное имя, которое является имущественным и относится к категории *property*. Продление регистрации доменного имени позволяет администратору сохранять права на него бессрочно, как и в случае с имущественным правом. При этом обладатель имущественного права вправе передать все принадлежащие ему права иному лицу, при этом само право, будучи связанным с его объектом, не прекращается, а следует за ним. Аналогичным образом происходит и с правом на доменное имя, которое следует за доменным именем и в случае его передачи новому администратору. Обратное бы означало невозможность передачи прав на доменные имена в принципе, как посредством дарения, наследования, отчуждения, так и другим способом. Как отметил суд, «[н]ичто в тексте или структуре закона не говорит о том, что Конгресс имел в виду, что права на доменные имена не должны быть отчуждаемы»[83].

Квалификация доменного имени в качестве имущественного права позволила американским судам разрешить и вопрос подсудности, когда администратор доменного имени находится за рубежом или в другом штате США.

Дж. Стори, анализируя высказывания императора Диоклетиана, указывает, что общее правило подсудности заключалось в том, что истец должен был подавать иск по месту нахождения ответчика (*domicile of the defendant*). Однако в некоторых случаях по искам *in rem* допускалось обращение в суд по месту нахождения вещи (*rei sitae*) (Story, 2007, pp. 445–446).

Как отмечает Х. Х. Перритт-младший, «доменное имя в некотором смысле является имуществом физического или юридического лица, за которым оно зарегистрировано. Оно также присутствует по сути в каждой юрисдикции по всему миру» (Perritt, 1998, p. 1138). Далее профессор приводит такой пример: «Если кто-то в Иллинойсе пострадал от действий лица из Македонии, то пострадавший из Иллинойса может, как представляется, обратиться с иском в суд в Иллинойсе на основании действия в Иллинойсе македонского доменного имени. Это будет выступать примером классической юрисдикции *in rem*» (Perritt, 1998, p. 1138).

Федеральный законодатель, с одной стороны, подтвердил юрисдикцию *in rem* по доменным спорам, а с другой — уточнил ее следующим образом: «Владелец знака вправе

[81] 15 U.S.C. § 1125(d)(1)(A).

[82] *GoPets Ltd. v. Hise*, 657 F.3d 1024, 1026–27 (9th Cir. 2011).

[83] Ibid.

подать гражданский иск *in rem* в отношении доменного имени в судебном округе, где находится регистратор доменного имени, реестр доменных имен или иной орган по доменным именам, который зарегистрировал или предоставил доменное имя»[84].

Несмотря на то, что юрисдикция *in rem* не является приоритетной: истцу сначала необходимо доказать суду, что юрисдикция *in personam*, т. е. по месту нахождения ответчика, недоступна для истца (*not able to obtain in personam jurisdiction over a person who would have been a defendant*[85]), сама возможность применения юрисдикции *in rem* показывает допустимость квалификации доменного имени как квазивещи или виртуальной вещи и применения соответственно вещного иска в отношении доменных имен.

Признав свою юрисдикцию *in rem,* некоторые суды прямо признают и доменные имена имуществом администратора домена. При этом важно учитывать, что понятие имущества (*property*) в толковании американских судов выходит далеко за рамки вещного права. Калифорнийский апелляционный суд второго округа в деле *Downing v. Mun*, в частности, указывает, что «категория *property* носит всеобъемлющий характер и включает любое нематериальное благо и прерогативу, которые могут находиться во владении или распоряжении»[86]. В прецедентном деле *Kremen v. Cohen* Апелляционный суд США по девятому федеральному апелляционному округу указал, что он применяет трехчастный тест для определения наличия такого имущественного права: «...во-первых, должен существовать интерес, поддающийся точному определению; во-вторых, он должен допускать исключительное владение или контроль; в-третьих, предполагаемый владелец должен обосновать законное право на исключительное использование... Доменные имена отвечают всем критериям»[87].

Таким образом, квалификация права на доменное имя как имущественного, в том числе на нематериальный объект, которым и является домен, позволяет прежде всего признавать американским судам юрисдикцию *in rem* и проводить судебные заседания по доменным спорам *ex parte*, устраняя необходимость применения персональной юрисдикции (*in personam*) администратора домена (Liu, 2014, p. 481).

Правовая охрана права на доменное имя как права из договора

Выработанная Апелляционным судом США по девятому федеральному апелляционному округу в деле *GoPets Ltd. v. Hise*[88] концепция права на доменное имя как права собственности имеет противников, что следует из практики судов иных федеральных апелляционных округов США. В частности, Апелляционный суд США по третьему федеральному округу анализировал аналогичный, как и в деле *GoPets Ltd. v. Hise*, вопрос, является ли перерегистрация доменного имени регистрацией по смыслу Закона Лэнхэма. В деле *Schmidheiny v. Weber* суд указал на договорный характер правоотношений между администратором и регистратором доменного имени. В частности, суд пришел к выводу, что «[д]ля регистрации доменного имени сторона, заинтересованная в эксклюзивном использовании доменного имени, администратор, должна связаться с регистратором и заключить [с ним] договор. В качестве встречного предоставления за право использования доменного имени в течение определенного промежутка времени

84 15 U.S.C. § 1125 (d)(2)(A).

85 Ibid.

86 *Downing v. Municipal Court*, 88 Cal. App. 2d 345, 350, 198 P.2d 923 (1948).

87 *Kremen v. Cohen*, 337 F.3d 1024 (9th Cir. 2003).

88 *GoPets Ltd. v. Hise*, 657 F.3d 1024, 1026–27 (9th Cir. 2011).

администратор уплачивает определенное вознаграждение и соглашается с иными известными условиями»[89].

В конкретном случае доменное имя было изначально зарегистрировано до вступления в силу Закона о защите потребителей от кибersквоттинга на господина Вебера, а в последующем было передано новому администратору — компании *Famology.com, Inc.*, в которой Вебер занимал должность президента и казначея. Вторичная регистрация на нового администратора (*reregistration*) произошла уже после вступления в силу названного Закона. Квалификация доменного имени в качестве собственности, право на которую следует за вещью, не позволила суду распространить действие Закона на такую вторичную регистрацию.

Именно в связи с данным обстоятельством суд указал, что договорное правоотношение между господином Вебером и регистратором относительно спорного доменного имени прекратилось в связи с передачей права администрирования новому лицу — компании *Famology.com, Inc.* При этом новый администратор «связал себя договорным правоотношением посредством нового регистрационного соглашения с новым регистратором... для закрепления за собой [права администрирования. — *И. Т., Е. А.*] доменного имени на новый период продолжительностью один год»[90].

В противном случае доменные имена, изначально зарегистрированные добросовестно, могли бы в последующем бесконечное количество раз «перепродаваться» без учета прав третьих лиц, например правообладателей товарных знаков, что не соответствует идее, заложенной в Закон о защите потребителей от кибersквоттинга[91].

Концепцию права на доменное имя как права из договора развил Апелляционный суд США по одиннадцатому федеральному апелляционному округу в деле *Jysk Bed'N Linen Inc. v. Dutta-Roy*[92], также отвергший идею квалификации права на доменное имя как права собственности и указавший на договорный характер правоотношений между администратором и регистратором доменного имени.

Анализ положений стандартных договоров регистраторов доменных имен с администраторами также подтверждает преобладающий характер рассматриваемого подхода к доменному имени. Например, в соответствии с пунктом 3, который специально обозначен заголовком «Собственность» (*Ownership*), соглашения о регистрации доменного имени одного из крупнейших американских регистраторов доменных имен — делавэрской корпорации *GoDaddy.com, LLC* (*GoDaddy — Domain Name Registration Agreement*) — администратор доменного имени в результате регистрации доменного имени на себя, т. е. заключения указанного соглашения, не получает права собственности ни на само обозначение, используемое в качестве доменного имени, ни на доменное имя как таковое[93]. В соглашении также установлено, что администратор не имеет права каким-либо образом передавать или пытаться передать право администрирования доменного имени другому лицу под видом права собственности, использовать такое право под видом права собственности в качестве залога или иным образом обременять его[94].

---

89 *Schmidheiny v. Weber*, 02/11/2003, 02-1668 (3rd Cir. 2003). https://caselaw.findlaw.com/court/us-3rd-circuit/1213148.html

90 Ibid.

91 Ibid.

92 *JYSK Bed'N Linen v. Dutta-Roy*, No. 13-15309 (11th Cir. 2015). https://law.justia.com/cases/federal/appellate-courts/ca11/13-15309/13-15309-2015-12-16.html

93 GoDaddy — *Domain Name Registration Agreement*. https://se.godaddy.com/legal/agreements

94 Ibid.

Как заключает Н. Ф. Барбантонис, квалификация доменного имени через призму договорного права, а не права собственности, имеет явные преимущества: необоснованно рассматривать регистрацию доменных имен с точки зрения права собственности лишь для того, чтобы избежать придания доменным именам статуса неотчуждаемых в случаях, когда текущий администратор использует доменное имя с недобросовестными намерениями (Barbantonis, 2016, p. 108).

Правовая охрана доменного имени как товарного знака

Несмотря на схожесть доменных имен, выполняющих функции указания места происхождения, с товарными знаками, по мнению М. Лиффера, первые не отвечают ряду базовых принципов системы регистрации товарных знаков: в частности, для надлежащего функционирования с точки зрения технической адресации на соответствующий ресурс доменные имена должны быть уникальными, в то время как с позиции законодательства о товарных знаках идентичные товарные знаки могут быть зарегистрированы и разными правообладателями, если это не вызывает смешения в глазах потребителей (Leaffer, 1998, p. 145).

Впрочем, данное противоречие находит решение в системе федерального законодательства и системе общего права США.

Федеральное законодательство США

В соответствии с федеральным законодательством основным способом получения доменным именем правовой охраны как товарного знака является его регистрация в качестве такового в Ведомстве по патентам и товарным знакам США (*Patent and Trademark Office*). Однако для нас данный вопрос регистрации интересен не сам по себе: как указывалось ранее, мы исключили из предмета анализа очевидные способы получения правовой охраны доменными именами, не отражающие их правовую природу. Важно для нашего исследования следующее.

В соответствии с положениями Закона Лэнхэма «владелец товарного знака, используемого в коммерческом обороте, может подать заявку на регистрацию своего товарного знака в утвержденном настоящим Законом главном реестре»[95]. То есть федеральный законодатель по общему правилу исходит из того, что перед регистрацией товарного знака в Ведомстве по патентам и товарным знакам США предприниматель должен какое-то время использовать такое обозначение без регистрации в коммерческом обороте. Если же такого использования не было, то заявитель может ссылаться на положение Закона Лэнхэма, допускающее регистрацию товарного знака и без его предварительного использования, если заявитель покажет добросовестные намерения (*bona fide intention*) по использованию товарного знака в коммерческом обороте после его регистрации[96].

Из данных законоположений следует, что в первом случае законодатель исходит из того, что использование незарегистрированного товарного знака в целом возможно.

Кроме того, согласно § 43(a) Закона Лэнхэма «любое лицо, которое... в отношении любых товаров или услуг использует в коммерческом обороте слово, термин, наименование, символ, изображение или их комбинацию или ложное указание происхождения, ...подлежит гражданско-правовой ответственности по иску любого лица, считающего, что оно уже понесло или может понести убытки в результате таких действий»[97].

[95] 15 U.S.C. § 1051(a)(1).

[96] 15 U.S.C. § 1051(b)(1).

[97] 15 U.S.C. § 1125(a)(1).

Следовательно, и незарегистрированные товарные знаки, в том числе и доменные имена, выполняющие их функции, могут получить определенную охрану по Закону Лэнхэма. Однако как таковое правовое существование незарегистрированных товарных знаков основано в США на общем праве (*common law*).

Доменные имена как товарные знаки общего права

Исключительные права на товарные знаки общего права (*common law trademarks*) у соответствующего правообладателя возникают без регистрации, на основании доктрины первого использования, которую можно сформулировать следующим образом: кто на соответствующей территории первым начал применять обозначение в качестве товарного знака (или знака обслуживания), т. е. в коммерческом обороте, тому исключительные права и принадлежат: исключительное право «возникает в связи с... использованием [обозначения в качестве товарного знака. — *И. Т., Е. А.*], а не с его регистрацией»[98].

Такой правообладатель, который первым стал применять на территории свое обозначение, выступает в качестве «старшего пользователя» (*senior user*) по отношению к иным правообладателям, которые начали использование тождественного или схожего обозначения позднее, — «младшим пользователям» (*junior users*).

Впрочем, концепция товарных знаков общего права, которая зародилась до эры Интернета и до появления федерального законодательства о товарных знаках, основана на предоставлении правовой охраны такому товарному знаку только на определенной географической территории, границы которой устанавливаются по зоне распространения репутации предпринимателя (*goodwill zone*) и зоне фактической товарной экспансии предпринимателя (*natural expansion*) (Johnson, 2014, p. 1276).

Само по себе данное ограничение не препятствует признанию доменного имени товарным знаком общего права, если посредством веб-сайта, на который доменное имя адресует, предлагаются товары или услуги на определенной территории. Однако, как отмечается в решении Окружного суда США по округу Юта, «[правообладатель] не может ссылаться на тот факт, что он использует веб-сайт... для возникновения общенациональной правовой охраны у его товарного знака»[99].

Следовательно, добросовестная регистрация доменного имени и использование такого доменного имени для предложения к продаже и продажи товаров или услуг могут при определенных обстоятельствах рассматриваться как основание для квалификации доменного имени в качестве товарного знака общего права и, соответственно, выступать правовым основанием для сохранения доменного имени за таким правообладателем в случае предъявления требований правообладателями тождественных или сходных до степени смешения товарных знаков, желающих получить право администрирования спорного домена. Особенность регистрации доменных имен — невозможность существования двух идентичных доменных имен — приводит к выводу о том, что приоритет в администрировании доменного имени должен быть предоставлен тому лицу, которое первым зарегистрировало соответствующее доменное имя на себя и использовало его в коммерческих целях на соответствующей территории ранее конкурентов.

Как отмечает Окружной суд США по округу Юта, «Интернет тем не менее не является географической территорией, которая может быть разделена на зоны; наоборот, это средство глобальной коммуникации, доступное из любой точки планеты»[100].

---

98 Trademark Cases, 100 U.S. 82 (1879). https://supreme.justia.com/cases/federal/us/100/82/

99 *UFirst Fed. Credit Union v. Univ. First Fed. Credit Union,* No. 2:2022cv00646 (D. Utah Sept. 27, 2023).

100 Ibid.

С учетом изложенного «старший пользователь» в спорной ситуации сможет сохранить за собой право администрирования домена, однако территориальный характер товарного знака общего права хотя и не будет влиять на сам факт регистрации домена, но должен быть учтен при фактическом использовании веб-сайта, к которому такое доменное имя адресует. Кроме того, наличие товарного знака общего права в виде домена, например на домене первого уровня *.com*, не может являться основанием для оспаривания регистрации аналогичного доменного имени на домене первого уровня *.us*, если у второго правообладателя также возникло право на использование товарного знака общего права, однако в рамках других территориальных границ.

Поскольку наличие схожих доменов может ввести потребителя в заблуждение, С. Джонсон предлагает решение данной проблемы посредством использования доктрины конкурентного использования Интернета (*concurrent Internet use doctrine*), подразумевающей одновременное присутствие в Интернете обоих правообладателей при соблюдении двух условий: «(1) оба правообладателя должны разместить заметный дисклеймер на соответствующем товаре или странице, где товар предлагается к продаже, с указанием того, где их продукты доступны (в случае ограниченной территориальной зоны [поставок]) или недоступны (при общенациональном использовании [товарного знака общего права]), и (2) использование в Интернете не должно недобросовестно распространяться на территорию [действия товарного знака общего права. — *И. Т., Е. А.*] другого правообладателя» (Johnson, 2014, p. 1298).

Доменное имя как цифровой актив и объект инвестирования

Национальным доменным именем в Соединенных Штатах выступает доменное имя *.us*. Среди крупнейших доменных сделок в зоне *.us* (от первых двух букв *United States*) публично известны сделки в отношении доменов *drive.us* (99 999 долл. США), *video.us* (75 тыс. долл. США), *lawyer.us* (50 тыс. долл. США), *job.us* (35 532 долл. США) и иные[101].

Впрочем, если говорить о мировом рынке доменных имен, то, конечно, нельзя не упомянуть домен *.com* (от *commercial* — «коммерческий»), который изначально был под управлением Министерства обороны США (*United States Department of Defense*), а сейчас управляется делавэрской корпорацией *Verisign, Inc*. Домены в зоне *.com* являются самыми привлекательными не только для коммерческих организаций, но и для иных лиц. Стоимость некоторых доменных имен стремится к миллиарду долларов.

Среди самых дорогих сделок в отношении доменных имен в зоне *.com* можно выделить договоры по доменам *cars.com* (872 млн долл. США), *business.com* (345 млн долл. США), *lasvegas.com* (90 млн долл. США), *carinsurance.com* (49,7 млн долл. США), *insurance.com* (35,6 млн долл. США), *vacationrentals.com* (35 млн долл. США) и пр.[102]

Кроме того, на рынке популярны и доменные биржи. Например, на сайте одного из самых крупных американских регистраторов доменов *GoDaddy* работает биржа, на которой любой желающий по множеству критериев может подобрать и «приобрести» себе домен. Например, в отношении домена *ope.com* «возрастом» 30 лет последняя ставка на аукционе составляла 43 500 долл. США[103].

---

101 Perez, A. K. (2024, August 29). *The most popular .US top level domains*. LinkedIn. https://www.linkedin.com/pulse/most-popular-us-top-level-domains-ana-karely-perez-msjye/

102 Rosaupan, V. (n.d.). *10 most expensive domain names ever sold*. Network Solutions. https://www.domain.com/blog/most-expensive-domains/

103 GoDaddy. (n.d.). *Auctions*. https://auctions.godaddy.com/beta

Если желаемый домен не выставлен на «продажу», то регистратор может предложить брокерские услуги, в рамках которых он проведет переговоры с текущим администратором домена, и если убедит его совершить сделку, т. е. «продать» домен, то клиент, помимо цены сделки, заплатит регистратору еще 20% от этой суммы плюс 99,99 долл. США[104].

Анализ договоров, которыми опосредуются такое «свободное обращение» доменного имени и его переход от одного администратора к другому, показывает, что стороны, как правило, именуют свои сделки «соглашение о передаче доменного имени» (*Domain name transfer agreement*), если предметом договора является только передача прав администрирования доменного имени, либо, когда доменное имя лишь один из передаваемых объектов, «соглашение о купле-продаже активов» (*Asset purchase agreement*), где собственно одним из активов и выступает доменное имя.

Помимо указанных договоров, стороны, как правило, заключают соглашение о передаче домена с регистратором. Например, у упомянутого ранее регистратора *GoDaddy* такая сделка именуется «Соглашение о смене администратора» (*Change of registrant agreement*)[105] и заключается как прежним, так и будущим администраторами с регистратором. В соответствии со ст. 2 названного соглашения стороны признают, что единственной обязанностью регистратора *GoDaddy* являются изменение информации об администраторе в реестре и обработка соответствующего запроса на передачу доменного имени на другой аккаунт. Со времени регистрации аккаунта приобретатель права на доменное имя сначала становится — в момент регистрации аккаунта — стороной соглашения об общих условиях обслуживания (*Universal terms of service agreement*)[106], в процессе передачи права администрирования — стороной вышеуказанного соглашения о смене администратора, а после приобретения права администрирования доменного имени — стороной соглашения о регистрации доменных имен (*Domain name registration agreement*)[107]. Согласно ст. 4 последнего оно сохраняет силу до тех пор, пока у администратора остается в администрировании хоть один домен. В дальнейшем соглашение не прекращается полностью, некоторые его положения, не связанные непосредственно с администрированием доменного имени, продолжают действие. Следовательно, у прежнего и будущего администратора доменного имени не происходит передачи договора.

Таким образом, в американской системе роль регистратора в сделках по передаче права администрирования доменного имени техническая и организационная.

Вывод по американскому подходу

Таким образом, с одной стороны, американский поход характеризуется наличием законодательного определения понятия доменного имени как средства адресации, что не добавляет правовой определенности в разрешении конкретных споров. Тем не менее анализ правоприменительной практики показывает, что сама дефиниция носит вторичный характер, а ключевое значение имеет инкорпорация соответствующего термина и связанных с ним положений в федеральное законодательство, что позволяет использовать средства правовой защиты, которые предоставляются на федеральном уровне.

[104] GoDaddy. (n.d.). *Domain Broker Service*. https://www.godaddy.com/domains/domain-broker

[105] GoDaddy. (n.d.). *Change of registrant agreement*. https://www.godaddy.com/legal/agreements/change-of-registrant-agreement

[106] GoDaddy. (n.d.). *Universal terms of service agreement*. https://www.godaddy.com/legal/agreements/universal-terms-of-service-agreement

[107] GoDaddy. (n.d.). *Domain name registration agreement*. https://www.godaddy.com/legal/agreements/domain-name-registration-agreement

С другой стороны, очевидная узость понимания доменного имени в качестве средства адресации нашла отражение в судебной практике и позволила выработать, на первый взгляд, противоположные подходы к определению правовой сути доменного имени: в качестве имущественного права или права из договора. Несмотря на тенденцию квалификации права на доменное имя как права из договора, трактовка доменного имени как имущественного права позволила решить ряд процессуальных проблем, с которыми сталкивались американские суды, в частности применить юрисдикцию *in rem* к доменным спорам, т. е. предоставить истцу возможность обращаться в суд не по месту нахождения ответчика, а по месту регистрации доменного имени.

Одной из ключевых характеристик правового регулирования доменных имен в США является уникальная для стран общего права концепция доменного имени как товарного знака общего права. Применение института товарного знака общего права, т. е. незарегистрированного обозначения, правовая охрана которого обеспечивается благодаря репутации и товарной экспансии правообладателя на определенной территории, к доменным именам показывает гибкость правового инструментария стран общего права, в рассматриваемом случае — США, при решении правовых проблем современности.

Сравнительный анализ подходов к правовой квалификации доменных имен

Проведенное исследование позволяет сделать выводы по основным критериям, в рамках которых проводился анализ доктрины, законодательства и судебной практики рассматриваемых правопорядков, и изложить их в виде таблицы 1.

Как видно из таблицы 1, несмотря на разницу правового регулирования и правоприменительных подходов в исследуемых правопорядках, можно сделать вывод о схожести правовых возможностей охраны доменных имен, хотя во всех государствах активность и реальная возможность использования того или иного варианта правовой охраны и в конечном итоге защиты различаются.

Заключение

По результатам исследования трех правопорядков: России, Германии и США, — мы можем прийти к выводу о широком диапазоне возможностей для квалификации доменных имен в зависимости от конкретных обстоятельств их регистрации и дальнейшего использования.

Законодательное регулирование доменных имен в рассматриваемых правопорядках не отражает реалии современного экономического оборота: в России и США доменное имя всё еще трактуется как средство адресации, а в Германии законодательное определение отсутствует в принципе.

Экономическое развитие на современном этапе, в свою очередь, позволяет квалифицировать доменное имя как ценный цифровой, т. е. неовеществленный и существующий исключительно в информационно-цифровой среде, актив и объект инвестирования. Поскольку в силу технических характеристик доменное имя является уникальным объектом (второго тождественного доменного имени зарегистрировано быть не может), многие перспективные с точки зрения бизнеса доменные имена уже «принадлежат» соответствующим лицам, т. е. администрируются ими, особое значение приобретает вторичный рынок доменных имен, на котором стоимость отдельных сделок приближается к миллиарду долларов США.

Таблица 1 / Table 1

Сравнительная таблица подходов к квалификации доменных имен / Comparative table of approaches to domain name qualification

Критерий	Россия	Германия	США
Законодательное определение	Техническое, в качестве средства адресации	Отсутствует	Техническое, в качестве средства адресации
Квалификация в качестве средства адресации	Используется в качестве исходной, закреплена законодательно	Используется в качестве исходной, отражена в доктрине и судебной практике	Используется в качестве исходной, закреплена законодательно
Квалификация в качестве идентификатора	Признается на доктринальном уровне, в судебной практике не раскрывается, но упоминается	Признается на доктринальном уровне	Признается на доктринальном уровне и в судебной практике
Квалификация в качестве средства индивидуализации	Теоретическая возможность охраны: – как общеизвестного товарного знака; – в качестве коммерческого обозначения (отвергается судами)	Возможность охраны в качестве коммерческого обозначения, в качестве товарного знака в силу использования	Возможность охраны в качестве товарного знака в силу использования
Квалификация в качестве объекта имущественных прав	Возможность охраны в качестве объекта имущественных прав (преобладающая судебная практика). Может быть частью имущественного комплекса (предприятия)	Возможность охраны в качестве объекта имущественных прав	Возможность охраны в качестве объекта имущественных прав
Квалификация в качестве цифрового актива и объекта инвестирования	Возможность выступать объектом инвестирования	Возможность выступать объектом инвестирования	Возможность выступать объектом инвестирования

Примечание. Составлено авторами.

С точки зрения функциональной теории доменные имена могут быть отнесены к категории идентификаторов по аналогии с товарными знаками, коммерческими обозначениями и использоваться для ведения коммерческой деятельности, в качестве элемента брендинга, средства коммуникации, рекламы и выполнять иные задачи.

Отсутствие на законодательном уровне самостоятельного правового статуса доменного имени вынуждает правоприменителя квалифицировать доменное имя при помощи имеющихся правовых категорий и инструментария, например как коммерческое обозначение, название произведения, а в некоторых случаях и обозначение, используемое в качестве товарного знака без регистрации, для того чтобы обеспечить правовую охрану и защиту доменного имени.

Базовой служит квалификация права на доменное имя как обязательственного, вытекающего из договора между администратором и регистратором доменного имени, что влечет возможность уступки такого права или — в более широком плане — передачи договора администрирования доменного имени иному лицу. Однако данный подход не объясняет высокой стоимости такого права и характерен в основном для России и Германии, где большинство договоров о передаче доменных имен конструируются именно по схеме уступки или передачи договора.

В свою очередь, в США, где имеется один из самых развитых вторичных рынков доменных имен, последние передаются в основном в качества актива (*asset*), зачастую наряду с иными объектами, например товарными знаками. Данный подход подчеркивает самостоятельную ценность доменного имени не просто как права из договора, но ценного цифрового актива.

Квалификация права на доменное имя как права собственности в широком западном понимании, т. е. как имущества (имущественного права), *de facto* применяется не только в США, но и в России для определения юрисдикции *in rem*, т. е. для подачи искового заявления не по месту нахождения ответчика – администратора домена.

Исходя из проведенного исследования, особого внимания сегодня заслуживает подход о квалификации доменного имени в качестве цифрового актива и объекта инвестирования, причем подобный вид инвестиционной деятельности носит высокорисковый характер и требует проведения обширного *Due Dillidgence* в отношении соответствующего доменного имени с учетом влияния сферы правовой охраны иных объектов, в том числе средств индивидуализации, которые могут быть ему противопоставлены в каком-либо из правопорядков, где планируется ведение предпринимательской деятельности.

Выявленные правовые возможности квалификации доменных имен открывают широкие перспективы для будущих углубленных научных цивилистических исследований и учета вышеупомянутых подходов судов при разрешении доменных споров, а также совершенствования и модернизации действующего законодательства в сфере регулирования доменных имен.

Список литературы / References

1. Axer, P. (2024). GG Art. 14. Eigentum, Erbrecht und Enteignung [Basic Law (GG) Article 14. Property, Inheritance, and Expropriation]. In V. Epping & C. Hillgruber (Eds.), *BeckOK Grundgesetz* (60th ed.). C. H. Beck.
2. Barbantonis, N. F. (2016). Is domain name classification a property right or a contractual right? The circuit split and a clear path forward. *Wake Forest Law Review Common Law*, *52*(100), 101–108.
3. Danilenkov, A. (2018). K voprosu o kvaziveshchno-pravovoi prirode domennogo imeni [On the quasi-proprietary nature of domain names]. *Khozyaistvo i Pravo*, (4), 97–112.
4. Elkemann, K., & Lieckfeld, M. (2022). Schutz der Domain als Marke [Trademark Protection for Domain Names]. In G. N. Hasselblatt (Ed.), *Münchener Anwalts Handbuch. Gewerblicher Rechtschutz* (6th ed.). C. H. Beck.

5. Eremenko, V. I. (2013). Opredelennye sdvigi v oblasti pravovogo regulirovaniya otnoshenii, svyazannykh s domennymi imenami [Certain shifts in the legal regulation of domain name relations]. *Birzha Intellektual'noi Sobstvennosti*, *12*(3), 1–6.
6. Fezer, K.-H., & Hauck, R. (2023). Rechtsnatur des Domainnamens [Legal nature of domain names]. In K.-H. Fezer (Ed.), *Marckenrecht. Kommentar zum Markengesetz (MarkenG) und zum Internationalen Markenrecht der Pariser Verbandsübereinkunft (PVÜ) und des Madrider Markenabkommens (MMA). Beck'she Kurz-Kommentare. Band 13b* (5th ed., paras. 198–316). C. H. Beck.
7. Geets, K. V. (2023). *Domennye imena i domennye spory v Rossii i za rubezhom* [Domain names and domain disputes in Russia and abroad]. Prospekt.
8. Gladkaya, E. I. (2014). *Pravovoi rezhim domennogo imeni v Rossii i SShA* [Legal regime of the domain name in Russia and the United States] [PhD in Law Dissertation, Russian State Academy of Intellectual Property].
9. Heine, R. (2025). Namens- und Kennzeichenschutz von Domainnamen [Name and trademark protection for domain names]. In F. J. Säcker, R. Rixecker, H. Oetker, B. Limperg, & C. Schubert (Eds.), *Münchener Kommentar zum Bürgerlichen Gesetzbuch* (10th ed., paras. 245–301). C. H. Beck.
10. Ingerl, R., & Rohnke, C. (2010). *Markengesetz. Gesetz über den Schutz von Marken und sonstigen Kennzeichen* [Trademark Act. Act on the Protection of Trademarks and Other Signs] (3rd ed.). C. H. Beck.
11. Johnson, S. (2014). Trademark territoriality in cyberspace: An Internet framework for common-law trademarks. *Berkeley Technology Law Journal*, *29*(2), 1253–1300. https://doi.org/10.15779/Z381Q40
12. Koos, S. (2004). Die Domain als Vermögensgegenstand zwischen Sache und Immaterialgut – Begründung und Konsequenzen einer Absolutheit des Rechts an der Domain [The domain as an asset between tangible and intangible property — justification and consequences of an absolute right to the domain]. *MMR Zeitschrift für IT-Recht und Recht der Digitalisierung,* (6), 359–365.
13. Kopylov, S. A., & M. A. Rozhkova (2022). Domennye imena: Napravleniya sovershenstvovaniya pravovogo regulirovaniya [Domain names: Directions for improving legal regulation]. *Zhurnal Suda po Intellektual'nym Pravam*, (2), 99–113.
14. Kozhemyakin, D. V. (2019). Domennoe imya: Imushchestvo ili usluga? [Domain name: Property or service?]. In E. P. Gavrilova & S. V. Butenko (Eds.), *Intellektual'nye prava: Vyzovy 21-go veka: Materialy mezhdunarodnoi konferentsii* (pp. 71–77). Tomsk State University Publishing House.
15. Kozhemyakin, D. V. (2023). *Domennoe imya v sisteme ob"ektov grazhdanskikh prav* [Domain names as objects of civil rights]. Prospekt.
16. Leaffer, M. (1998). Domain names, globalization, and Internet governance. *Indiana Journal of Global Legal Studies*, *6*(1), 139–165.
17. Liu, M. X. (2014). Jurisdictional limits of *in rem* proceedings against domain names. *Michigan Telecommunications and Technology Law Review*, *20*(2), 467–496.
18. Novikova, N. A. (2018). K voprosu o ponyatii domennogo imeni [On the concept of a domain name]. *Permskii Yuridicheskii Al'manakh*, (1), 239–247.
19. Perritt, H. H. (1998). Will the judgment-proof own cyberspace? *The International Lawyer*, *32*(4), 1121–1165.
20. Reed, S. R. (2011). Sensible agnosticism: An updated approach to domain-name trademark infringement. *Duke Law Journal*, *61*(1), 211–250.
21. Reichman, J. (1995). Charting the collapse of the patent-copyright dichotomy: Premises for a restructured international intellectual property system. *Cardozo Arts & Entertainment Law Journal*, (13), 475–520.
22. Rozhkova, M. A. (2015a). Domennye imena kak identifikatory i sredstva kommunikatsii [Domain names as identifiers and means of communication]. *Khozyaystvo i Pravo*, (3), 55–70.
23. Rozhkova, M. A. (Ed.). (2015b). *Zashchita delovoi reputatsii v sluchayakh ee diffamatsii ili nepravomernogo ispol'zovaniya (v sfere kommercheskikh otnoshenii): Nauchno-prakticheskoe posobie* [Protection of business reputation in cases of defamation or unlawful use (in commercial relations): A scientific-practical guide]. Statut.

24. Rozhkova, M. A. (2018). Prava na domennoe imya [Rights to domain name]. In M. A. Rozhkova (Ed.), *Pravo v sfere Interneta: Sbornik statei* (pp. 195–223). Statut.
25. 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.
26. Rozhkova, M. A. (2025). Problemy ustanovleniya samostoyatel'nogo pravovogo rezhima dlya tsifrovykh ob"yektov [Problems of establishing an independent legal regime for digital objects]. *Zhurnal Suda po Intellektualnym Pravam*, (2), 146–157. https://doi.org/10.58741/23134852_2025_2_14
27. Sannikova, L. V., & Kharitonova, Yu. S. (2020). *Tsifrovye aktivy: Pravovoy analiz* [Digital assets: Legal analysis]. 4Print.
28. Savelyev, A. I. (2020). *Elektronnaya kommertsiya v Rossii i za rubezhom: Pravovoe regulirovanie* [E-commerce in Russia and abroad: Legal regulation] (3rd ed.). Statut.
29. Story, J. (2007). *Commentaries on the conflict of laws, foreign and domestic, in regard to contracts, rights, and remedies, and especially in regard to marriages, divorces, wills, successions, and judgments*. The Lawbook Exchange.
30. Viefhues, M. (2024). Domainrecht [Domain law]. In T. Hoeren, U. Sieber, & B. Holznagel (Eds.), *Handbuch Multimedia-Recht* (paras. 1–417). C. H. Beck.
31. Weiler, F. (2025). Entstehung der Benutzungsmarke [Establishment of a trademark by use]. In A. Kur, V. von Bomhard, & F. Albrecht (Eds.), *BeckOK Markenrecht* (40th ed., paras. 17). C. H. Beck.
32. Yukhnova, Yu. I., Yatsenko, D. V., & Morgunova, A. A. (2020). Problema pravovoi prirody domennogo imeni po grazhdanskomu zakonodatel'stvu [The problem of the legal nature of domain names under civil legislation]. *Nauka i Obrazovanie*, (3), 110–118.

Сведения об авторах:

Титов И. Е. — магистр права (Свободный университет Берлина), аспирант, кафедра гражданского права и процесса и международного частного права, Юридический институт, Российский университет дружбы народов имени Патриса Лумумбы, юрист, практика защиты прав интеллектуальной собственности (IP/IT/Media), международная юридическая фирма ADVANT Beiten, Москва, Россия.
1142230458@rudn.ru
ORCID: https://orcid.org/0009-0006-4961-470X

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

Information about the authors:

Ilya E. Titov — LL.M. (Free University of Berlin), Ph.D. Student, Department of Civil Law and Procedure and International Private Law, Peoples Friendship University of Russia Named After Patrice Lumumba (RUDN University), Lawyer, IP/IT/Media Practice Group, International Law Firm ADVANT Beiten, Moscow, Russia.
1142230458@rudn.ru
ORCID: https://orcid.org/0009-0006-4961-470X

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

https://doi.org/10.38044/2686-9136-2025-6-17

ARTICLES

ARTIFICIAL INTELLIGENCE AND LIABILITY: EXPLORING LEGAL CHALLENGES AND RESPONSIBILITY IN AI DECISION-MAKING AND AUTONOMOUS SYSTEMS

Kolawole O. Afuwape

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

Abstract

The rapid integration of artificial intelligence (AI) across a wide range of economic sectors, including transportation, healthcare, and finance, has significantly transformed decision-making processes and operational efficiency. At the same time, increasing reliance on AI has generated new legal challenges, particularly with respect to accountability and sanctions. Central issues include decisional responsibility, algorithmic transparency, and data regulation, especially in relation to bias. Traditional legal frameworks, which were developed to govern human conduct, are poorly equipped to address the self-learning capabilities, unpredictability, and opacity of AI systems. This paper examines the emerging concept of shared responsibility within multi-stakeholder AI ecosystems, in which liability may extend across developers, manufacturers, operators, and users. It analyzes product liability principles and the allocation of accountability in cases where AI systems cause harm. Particular emphasis is placed on the need to adapt legal frameworks to keep pace with the rapid evolution of AI technologies, ensuring flexibility, resilience, and alignment with international legal standards. The European Union's AI Act is examined as a case study illustrating efforts to address accountability gaps while promoting ethical guidelines to strengthen public trust. Through the use of case studies and hypothetical scenarios, this paper highlights the importance of transparency and fairness in managing the legal implications of AI. Finally, it advocates for closer collaboration between computer science and law to bridge gaps in AI literacy, product development, and regulation. By addressing contemporary challenges and proposing legal responses, this paper offers a coherent framework for managing liability in the age of artificial intelligence.

Keywords

artificial intelligence, autonomous systems, accountability, transparency, explainable AI, XAI, algorithmic bias, ethical AI, product liability, shared responsibility

Conflict of interest The author declares no conflict of interest.

Financial disclosure The study has no sponsorship.

For citation Afuwape, K. O. (2025). Artificial intelligence and liability: Exploring legal challenges and responsibility in AI decision-making and autonomous systems. *Digital Law Journal, 6*(4), 82–100. https://doi.org/10.38044/2686-9136-2025-6-17

Submitted: 28 Jun. 2025, accepted: 16 Nov. 2025, published: 30 Dec. 2025

СТАТЬИ

ОТВЕТСТВЕННОСТЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПРАВОВЫЕ ВЫЗОВЫ В ПРОЦЕССЕ ПРИНЯТИЯ РЕШЕНИЙ С ПОМОЩЬЮ ИИ И АВТОНОМНЫХ СИСТЕМ

К. О. Афувапе

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

Аннотация

Быстрая интеграция искусственного интеллекта (ИИ) в широкий спектр секторов экономики, включая транспорт, здравоохранение и финансы, значительно изменила процессы принятия решений и операционную эффективность. В то же время растущая зависимость от ИИ породила новые правовые проблемы, особенно в отношении ответственности. К центральным вопросам относятся ответственность за принятие решений, прозрачность алгоритмов и регулирование данных, особенно в связи с предвзятостью. Традиционные правовые рамки, разработанные для регулирования поведения людей, плохо приспособлены для решения проблем, связанных с самообучающимися способностями, непредсказуемостью и непрозрачностью систем ИИ. В данной статье рассматривается новая концепция совместной ответственности в многосторонних экосистемах ИИ, в которых ответственность может распространяться на разработчиков, производителей, операторов и пользователей. Анализируются принципы ответственности за качество продукции и распределение ответственности в случаях, когда системы ИИ причиняют вред. Особое внимание уделяется необходимости адаптации правовых рамок к быстрому развитию технологий ИИ, обеспечению гибкости, устойчивости и соответствия международным правовым стандартам. Закон Европейского союза об ИИ рассматривается в качестве примера, иллюстрирующего усилия по устранению пробелов в ответственности при одновременном продвижении этических принципов для укрепления доверия общественности. С помощью конкретных примеров и гипотетических сценариев в данной статье подчеркивается важность прозрачности и справедливости в правовом регулировании ИИ. В заключение статья выступает за более тесное сотрудничество между компьютерными науками и правом с целью устранения пробелов в знаниях об ИИ, разработке продуктов и регулировании. Рассматривая современные вызовы и предлагая правовые решения, данная статья предлагает последовательную структуру для регулирования ответственности в эпоху искусственного интеллекта.

Ключевые слова

искусственный интеллект, автономные системы, подотчетность, прозрачность, объяснимый ИИ, алгоритмическая предвзятость, этический ИИ, ответственность за качество продукции, совместная ответственность

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.
Для цитирования	Афувапе, К. О. (2025). Ответственность искусственного интеллекта: правовые вызовы в процессе принятия решений с помощью ИИ и автономных систем. *Цифровое право, 6*(4), 82–100. https://doi.org/10.38044/2686-9136-2025-6-17

Поступила: 28.06.2025, принята в печать: 16.11.2025, опубликована: 30.12.2025

Introduction—Overview of AI

Artificial intelligence (AI) possesses characteristics that emulate human intelligence through numerical and computational systems (Zhang & Lu, 2021). These systems are capable of forming representations, learning from data, making predictions, conducting analyses, drawing conclusions, and, in some cases, applying self-corrections. AI is designed to address a wide range of tasks, including medical prediction, planning, image visualization, voice recognition, and the acquisition of specific skills. AI systems rely on training datasets to improve predictive accuracy and to assist in solving complex problems with a high degree of precision (Kumar et al., 2023, pp. 8459–8486).

To a certain extent, AI may be understood as a scientific field concerned with the learning capabilities of intelligent machines, primarily intelligent computer programs, which generate outcomes in a manner comparable to human cognitive and attentional processes (Khaleel et al., 2024, pp. 1–21). As a rule, AI involves sequential processes of data accumulation, the creation of effective structures for utilizing acquired data, the production of definite or approximate outcomes, self-evaluation, and subsequent adjustment. Overall, AI is used to assess and advance machine-learning techniques that aim to replicate aspects of human cognition (Dong et al., 2020, pp. 1–10). AI technologies are increasingly employed to perform more accurate analyses and to generate practical and economic value. From this perspective, a range of statistical models, along with computational intelligence methods, are integrated into AI systems.

AI has seen remarkable and rapid development over the past two decades. Its subdomains—such as machine learning (ML), natural language processing (NLP), and computer vision—are progressively converging and expanding across numerous sectors of society. Artificial intelligence is increasingly embedded in human activities and, in certain contexts, is replacing human decision-making processes (Chukwuani et al., 2020, pp. 444–449). Although AI originates within computer science, it is closely connected to many other disciplines, including mathematics, cognitive science and philosophy, biology, business and logistics, engineering and manufacturing, transportation, healthcare, education, and government (Adnan et al., 2024).

The deployment of AI has enhanced productivity while reducing costs, and its effects contribute to economic development, social transformation, and individual welfare (Adigwe et al., 2024,

pp. 126–146). AI aims to create digital computers or computer-operated robots capable of performing intellectual and cognitive tasks typically associated with humans, without external assistance (Markauskaite et al., 2022). These cognitive functions include acquiring knowledge, reasoning, problem-solving, perception and comprehension, and speech. A foundational aspect of AI is knowledge engineering, whereby machines are constructed using data and information about the human world so that they can act in human-like ways (McCarthy, 2022, pp. 66–90). Another major branch of AI is machine learning, in which predefined algorithms and statistical models are used to minimize or converge errors without explicit, task-specific programming (Telikani, 2021, pp. 1–35). This approach is based on the premise that machines can learn from data, identify problems, and determine solutions with minimal human intervention.

This paper offers specific recommendations to support the argument that data protection and privacy laws are essential for improving the transparency and accountability of AI systems. Nevertheless, significant issues, debates, and ongoing controversies surround the practical implementation of these rights, particularly regarding the extent to which they can be enforced and the manner of their enforcement. Moreover, current data protection laws exhibit notable limitations in their coverage of, and applicability to, AI systems. In particular, this paper demonstrates how de-identification techniques intended to circumvent legal obligations by removing personal identifiers are undermined by AI technologies, which are capable of directly re-identifying data or indirectly inferring sensitive attributes from datasets that have been anonymized.

Results

The findings indicate that the autonomous actions of AI systems cannot be adequately regulated through traditional legal frameworks that are grounded in human agency. Such autonomous action requires distinct and domain-specific regulatory consideration, particularly in sectors such as healthcare, transportation, and finance. This paper highlights the potential problem of overlapping and shared interests among AI developers, users, and manufacturers. To address these challenges, it proposes a hybrid model of liability that combines elements of strict liability with algorithmic transparency requirements. The paper concludes that global accountability is central to necessary legal reforms and suggests that, without such reforms, society will be reluctant to rely on AI technologies or to adopt them at a rapid pace.

Role of AI in Autonomous Systems and Decision-Making

Autonomous Decision-Making Systems (ADMS) are advanced computing systems capable of receiving and responding to information in both digital and physical forms, and of generating outputs that may either support or substitute human decision-making processes (Dwivedi et al., 2023). ADMS can be defined as processes that, with or without the use of AI techniques, take inputs and data received or collected from the environment and, based on predefined objectives, produce a wide range of outputs.[1]

Autonomous AI represents a subcategory of artificial intelligence in which systems and tools have developed to the point where they can operate largely independently of human input (Atakishiyev et al., 2024, pp. 51182–51221). The actions performed by autonomous AI systems range from relatively simple operations to complex data analysis tasks (Bathla et al., 2022). In this respect, autonomous AI

[1] Anderson, A., Vadari, S., Wall, L., Sharma, P., & Reiman, A. (2023). *Distributed rules-based deconfliction of ADMS applications: Part 2: Conceptual implementation.* Pacific Northwest National Laboratory. https://doi.org/10.2172/1996255

brings real-world AI systems closer to the portrayals commonly found in fictional representations of artificial intelligence (Lucci et al., 2022, p. 850).

When effectively implemented, AI systems composed of multiple interacting components can significantly enhance the operational capacity of businesses and other organizations (Dalsaniya & Patel, 2022, pp. 322–337). Some components are software-based and provide specific functionalities, such as algorithms that analyze collected data, while other components are embedded within systems to capture data from the environment and supply it to analytical processes. The term "AI" may apply to systems that still require continuous human intervention,[2] as well as to more advanced architectures—such as reinforcement learning, machine learning, and deep learning platforms—that are capable of processing and correlating large datasets with limited human involvement (ZainEldin et al., 2024).

Self-governing or autonomous AI represents one of the most advanced forms of contemporary AI. However, since many AI applications widely used today are not fully self-sufficient, they are commonly described as narrow AI (Perwej et al., 2024, pp. 1–32). Narrow AI refers to systems designed to perform specific tasks that generally require human oversight or guidance (Hopgood, 2021, p. 514). In contrast, artificial general intelligence (AGI) refers to a hypothetical or fictional concept in which AI systems are fully autonomous, capable of operating independently of any human operator, and able to outperform human intelligence across all domains (Mikki, 2024).

Current AI systems, including those described as autonomous, do not yet meet the criteria of AGI. Rather, autonomous AI constitutes an intermediate stage in the progression toward that theoretical goal. While such systems may rely on equipment and infrastructures that still require human intervention for data collection and system support (Paesano, 2023, pp. 1694–1723), they also incorporate advanced learning structures—such as reinforcement learning, machine learning, and deep learning—that enable the classification and analysis of large datasets with minimal direct human interaction. As such, autonomous AI is among the most complex AI concepts developed to date, marking a significant step toward greater machine independence while remaining distinct from fully autonomous artificial general intelligence.

Specialists define narrow AI as the many AI systems and tools currently in use that cannot perform certain tasks independently without human guidance (Hopgood, 2021, p. 514). By contrast, artificial general intelligence refers to an AI that can operate fully autonomously, independent of any human operator, and surpass human intelligence in all respects. Autonomous AI fits neither category, but it represents a significant step toward the development of artificial general intelligence.

An autonomous AI system requires the following two components:

- **Data collection instruments**, commonly referred to as sensors, which are physical devices used to gather data from the environment.[3]
- **Algorithms**. For a system to autonomously achieve a goal defined by a human, the collected data must be processed by computer algorithms (Lehmann et al., 2023). In the ideal case, where all components are smoothly integrated, an autonomous AI agent can operate independently of human input, make its own decisions, and perform tasks autonomously. An autonomous AI

[2] Moruzzi, C., & Margarido, S. (2024). Customizing the balance between user and system agency in human-AI co-creative processes. In *Proceedings of the 15th International Conference on Computational Creativity, ICCC'24, Jonköping, Sweden* (pp. 108–117). Association for Computational Creativity. https://www.research.ed.ac.uk/en/publications/customizing-the-balance-between-user-and-system-agency-in-human-a/

[3] Saari, M. (2024). *Software hardware combination for IoT sensor data gathering and prototyping: Architecture model, framework, and process model*. Tampere University. https://trepo.tuni.fi/handle/10024/154585

agent may be understood as a tool that receives a goal from a human and develops a strategy for achieving that goal through a set of tasks and actions (Sado et al., 2023, pp. 1–41).

It is evident that several potential benefits can be derived from ADMS-based systems (Salvini et al., 2023), although attitudes toward the acceptability of ADMS vary depending on the application and the end user (Aysolmaz et al., 2023). Human decision-making capacity is inherently limited and varies across individuals, as a single person can respond effectively to only a restricted number of stimuli at any given time (Sosnowski & Brosnan, 2023, pp. 1103–1117). By contrast, once an ADMS has been trained, it can be replicated indefinitely.[4] Beyond computational efficiency, the use of ADMS may offer additional benefits, including improvements in safety, cost reduction, efficiency, and accuracy (Attaran, 2020, pp. 158–172).

The potential risks associated with Automated Decision-Making Systems (ADMS), and the serious consequences they may impose on individuals in critical sectors such as healthcare, military operations, finance, and justice, highlight the need to integrate human oversight into automated decision-making frameworks (Leslie & Perini, 2024). Such integration is often presented as an essential means of ensuring accountability and effective supervision. However, the concept of meaningful human control gives rise to a paradox. On the one hand, systems are designed to make decisions independently in order to reduce or eliminate human involvement, thereby enhancing safety, lowering costs, and improving the prediction of behavior. On the other hand, there is a growing demand to monitor autonomous systems to ensure ethical outcomes, for example, by addressing concerns related to fairness.

Particularly troubling is the phenomenon of quasi-automation, in which humans are formally involved but function largely as a superficial source of validation, while the system performs the substantive decision-making tasks. In many organizations, insufficient staff training or a lack of adequate time allocated for decision-making have been identified as common issues. This problem was notably demonstrated in 2018, when Amazon faced criticism over an AI-based recruitment tool that ranked job candidates, which was found to be biased against women and black applicants.[5] The algorithm ranked applicants on a scale from one to five based on their résumés but systematically rated female candidates poorly because it had been trained on historical data reflecting male dominance in the technology sector. As will be discussed later in this paper, recruiters retained partial responsibility for shortlisting, interviewing, and hiring new employees, but they rarely reviewed the full pool of applicants due to the sheer volume of applications, which caused candidate lists to be processed very quickly. This example illustrates the need for clearly defined parameters to establish meaningful human control over ADMS (Saeik et al., 2021).

Legal Framework for AI in the EU

The European Commission has developed a number of legislative instruments in response to the rapid emergence and widespread deployment of diverse AI technologies across multiple sectors, as well as the ethical concerns and risks associated with their use. In 2021, the European Commission

[4] Smith, S., Patwary, M., Norick, B., LeGresley, P., Rajbhandari, S., Casper, J., Liu, Z., Prabhumoye, S., Zerveas, G., Korthikanti, V., Zhang, E., Child, R., Aminabadi, R. Y., Bernauer, J., Song, X., Shoeybi, M., He, Y., Houston, M., Tiwary, S., & Catanzaro, B. (2022). *Using DeepSpeed and Megatron to Train Megatron-Turing NLG 530B, A Large-Scale Generative Language Model* (arXiv:2201.11990). arXiv. https://doi.org/10.48550/arXiv.2201.11990

[5] Njoto, S. M. (2020). Gendered Bots? Bias in the use of Artificial Intelligence in Recruitment (pp. 11–15). *The Policy Lab, The University of Melbourne.* https://www.academia.edu/43650660/Gendered_Bots_Bias_in_the_use_of_Artificial_Intelligence_in_Recruitment

proposed the AI Act,[6] which establishes a comprehensive legal framework for the development, deployment, and use of AI systems across various sectors within the EU and its internal market (Schmidt et al., 2024). On July 12, 2024, the AI Act was published in the Official Journal of the European Union, marking it as the first horizontal legal framework specifically aimed at regulating artificial intelligence across the EU.[7] The AI Act became applicable on August 1, 2024, and will enter into full effect on August 2, 2026, unless specific provisions listed in Article 113 apply.[8]

As of February 2025, the EU AI Liability Directive—initially proposed by the European Commission to address legal challenges related to the attribution of responsibility in cases involving AI systems—has been formally withdrawn from the Commission's legislative agenda[9] (Grozdanovski, 2025, pp. 1–24). Despite early momentum, including the adoption of a position by the European Parliament's Committee on Legal Affairs (JURI Committee), proposals to extend the Directive's scope, and broader parliamentary interest, the Directive encountered strong opposition from EU member countries. Critics argued that it duplicated provisions already addressed by the newly adopted Product Liability Directive.[10] This withdrawal reflects institutional reluctance to create overlapping legal regimes and underscores the EU's preference to regulate AI liability and responsibility through existing legislation, particularly through the AI Act, and to rely on its overall regulatory effectiveness (Greenstein & Zamboni, 2025, pp. 1–41). The absence of a harmonized, specifically tailored AI liability regime creates a regulatory gap, especially in cases involving non-material harm and complex decision-making chains, which may undermine legal certainty and consumer protection in AI-related contexts.

Several EU legal acts and regulations are relevant to the governance of AI, including the EU Artificial Intelligence Act (AI Act),[11] the Digital Markets Act (DMA),[12] the Cyber Resilience Act (CRA),[13] the Data Act,[14] the Digital Services Act,[15] and the General Data Protection Regulation (GDPR),[16] all of which influence the regulation and deployment of AI systems within the EU.

6 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, 2024 O.J. (L 1689) 1 [hereafter AI Act].

7 Ibid., art. 3(1).

8 Zwitter, A., Gstrein, O. J., & Haleem, N. (2024). *General-purpose AI regulation and the European Union AI Act.* Social Science Research Network. https://doi.org/10.2139/ssrn.4916400

9 AI Liability Directive. (n.d.). *The Artificial Intelligence Liability Directive.* https://www.ai-liability-directive.com/

10 Council Directive 85/374/EEC of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products, 1985 O.J. (L 210) 29.

11 AI Act, art. 3(1), 2024 O.J. (L 1689) 46.

12 Regulation 2022/1925, of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022 OJ (L 265).

13 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 (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), 2024 O.J. (L 2024/2847) 1.

14 Regulation 2023/2854, of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation 2017/2394 and Directive 2020/1828 (Data Act), 2023 O.J. (L 2023/2854) 1.

15 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.

16 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.

The AI Act defines an "AI system" as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments." A "general-purpose AI model" is defined as an AI model, including those trained on large datasets using self-supervision at scale, that demonstrates significant generality and is capable of competently performing a wide range of distinct tasks, regardless of how it is placed on the market, and that can be integrated into a variety of downstream systems or applications, excluding models used solely for research, development, or prototyping prior to market placement. The term "general-purpose AI system" refers to an AI system derived from a general-purpose AI model that can be used either as a standalone product or as part of other systems.

Pursuant to Article 3(66),[17] the AI Act has extraterritorial applicability to the following actors:

- any provider that places an AI system or a general-purpose AI model on the EU market, uses it for its own purposes, or otherwise makes it available, irrespective of whether the provider is established within the EU or in a third country;
- any deployer of AI systems that is established or located within the EU;
- any provider or deployer of an AI system established or located in a third country, where the output generated by the AI system is used within the EU.

The AI Liability Directive primarily addressed non-contractual, fault-based civil liability claims within the EU and was expected to adopt the same definition of AI as that used in the AI Act (Nikolinakos, 2024, pp. 477–621).

Under the AI Act, any developer of an AI system or general-purpose AI model, as well as any natural or legal entity, public authority, agency, or other body that develops and places such systems or models on the EU market, is classified as a "provider".[18]

A "distributor" is defined as any natural or legal entity in the supply chain other than a provider or importer who makes an AI system available on the EU market, but a provider or importer does not become a distributor solely by placing an AI system on the market.[19]

An "importer" is any natural or legal entity within the EU that places an AI system on the EU market which is marketed under the name or trademark of an entity established in a third country.[20]

The proposed AI Liability Directive sought to revise civil liability rules to make it easier for victims of AI-related harm to prove fault and obtain compensation. It aimed to enhance legal certainty by introducing mechanisms such as disclosure obligations and rebuttable presumptions to address the technical complexity and opacity of AI systems. However, the European Commission withdrew the Directive in early 2025 due to concerns about over-regulation and a lack of legislative progress. Although the Directive is no longer proceeding through the formal legislative process, its underlying objective of complementing the AI Act by addressing AI-related liability concerns remains relevant.

The AI Liability Directive was intended to ensure that individuals harmed by AI systems would have access to compensation equivalent to that available to victims of other forms of technological harm within the EU (Nikolinakos, 2024). Existing fault-based liability regimes are often ill-suited to address damage caused by AI-driven products and services. Victims may encounter significant

[17] AI Act, art. 3(66), 2024 O.J. (L 1689) 50.

[18] Ibid., art. 3(3).

[19] Ibid., art. 3(7).

[20] Ibid., art. 3(6).

practical and financial barriers when attempting to demonstrate fault and establish causation, largely due to the opaque, complex, and self-learning nature of AI systems.

Risk Categorization

The categorization of AI systems by risk level and the corresponding regulatory requirements under the EU Artificial Intelligence Act are set out in the following provisions:

- Article 5—Prohibited AI Practices, which lists AI systems and practices that are outright banned, such as manipulative subliminal techniques, social scoring by public authorities, and certain uses of biometric technologies.
- Article 6—High-Risk AI Systems, which defines what constitutes a high-risk AI system, including AI applications used in areas such as critical infrastructure, education, employment, law enforcement, migration, and the administration of justice.
- Article 7—Amendments to the List of High-Risk AI Systems, which establishes the mechanism through which the European Commission may update or expand the list of high-risk AI applications.

Under the AI Act, any undertaking that provides an AI system as a service, produces a product incorporating an AI system, deploys an AI system, imports an AI system, distributes an AI system, or acts as an authorized representative of an operator is classified as an "operator," regardless of legal form. Both individual providers and contractors specializing in general-purpose AI models are subject to obligations relating to technical documentation and transparency. They are also required to consult with the European Commission and national competent authorities and to comply with national legislation concerning copyright and related rights. Compliance may be demonstrated, *inter alia*, through adherence to approved codes of practice.

Additional obligations apply to providers of general-purpose AI models that pose systemic risk. These include requirements to conduct standardized model evaluations, identify and manage systemic risks, monitor incidents, and implement appropriate cybersecurity measures.

The AI Act further provides for the development of codes of conduct for AI systems, with the European Commission expressing the expectation that providers will adopt such codes on a voluntary basis (Cantero Gamito & Marsden, 2024). By contrast, the AI Liability Directive does not impose any comparable compliance obligations (Hacker, 2023).

Legal Personification of AI

The products and actions of artificial intelligence cannot easily be accommodated within existing legal categories, whether as property or as persons. Many scholars compare the current role of artificial intelligence in law to the historical concept of a "quasi-person", a legal status previously used to address entities that did not fit neatly into established legal classifications (Amelin et al., 2022, pp. 294–302). A number of authors have drawn analogies between the present legal treatment of artificial intelligence and earlier encounters with quasi-personhood in legal doctrine (Mecaj, 2022, pp. 180–196).

A related issue arises from the position of other legal scholars who argue that if discussions concerning the behavior of AI and its moral and ethical dimensions are to be treated as meaningful and coherent, then it may also be appropriate to consider the legal recognition of the personality of artificial intelligence. In this context, legal personality is viewed as a significant stage in the realization of constitutional rights. Once an AI system is granted legal personality under the law, it would, in principle, become a bearer of constitutional rights (Bublitz, 2024, pp. 1095–1106).

Complexities of Multi-Stakeholder Liability

Explainable AI (XAI) and Interpretability

Cognitive approaches to transparency and accountability in AI systems focus on the application of technological processes, tools, and practices that make artificial intelligence systems comprehensible, explainable, and traceable to organizational stakeholders (Göksal & Solarte Vasquez, 2024). These approaches seek to facilitate an understanding of how an AI system arrives at a particular conclusion and to provide mechanisms for challenging outcomes or identifying points at which the system may have failed. As a result, Explainable AI (XAI) has emerged as an important subfield concerned with making AI systems interpretable to human users (Holzinger et al., 2023, pp. 16–24).

When AI is deployed in serious and high-impact application contexts, there are strong societal imperatives to understand how AI systems function, to critically assess and challenge their outcomes, and to demand justification for AI-driven decisions and actions. In this regard, the EU's General Data Protection Regulation (GDPR) incorporates a so-called "right to explanation" and establishes principles governing solely automated decision-making that has significant effects on individuals (Bayamlıoğlu, 2022, pp. 1058–1078).

Legal and Regulatory Frameworks

Legal and regulatory frameworks play a crucial role in promoting transparency and establishing effective accountability within information systems that rely on artificial intelligence (Díaz-Rodríguez et al., 2023). Privacy laws contribute to fair data processing by requiring organizations to disclose how data is used and by enabling individuals to participate in and influence decisions concerning the use of their personal information (Mijwil et al., 2023, pp. 8–13). These laws also support accountability, as the GDPR grants data subjects the right to bring legal action against organizations for unlawful automated decision-making. Similarly, anti-discrimination laws facilitate accountability by prohibiting the development and deployment of AI systems that produce discriminatory outcomes, while also providing individuals with legal remedies for unfair treatment.

A recent case involving Clearview AI illustrates these concerns. The American facial recognition company was accused by the American Civil Liberties Union (ACLU) of violating Illinois' Biometric Information Privacy Act (BIPA) (Ahmed, 2023, pp. 66–95). The company reportedly collected billions of images from Facebook and other websites to build a facial recognition database without users' consent. This case raises significant questions regarding the use of AI systems that rely heavily on personal data.

Such challenges and regulatory gaps are often viewed as best addressed through incremental reforms to data protection law combined with the development of new AI governance frameworks. These measures may include expanding the definition of "personal data" to encompass inferred data, introducing privacy impact assessments and algorithmic audits for high-risk AI systems, and requiring comprehensive model documentation and reporting.

As artificial intelligence has become increasingly embedded in consumer products and services, growing scrutiny has emerged regarding accountability when AI systems cause harm to individuals (Patel, 2024, pp. 1–17). Traditional product liability regimes hold manufacturers responsible for harm caused by manufacturing defects, design flaws, or inadequate warnings. However, the autonomous and self-learning characteristics of AI systems make them difficult to assess under conventional product liability frameworks (Sayre & Glover, 2024, pp. 357–394). Defining what constitutes a "defect" in an AI system presents particular challenges (Hacker, 2023). This raises complex questions,

such as whether biased outputs generated by an AI system should be considered defects (Lesenciuc, 2024, pp. 9–22). If an AI system functions as intended and harm results from the optimization goals embedded in its design, such harm may be interpreted as a design defect (Li et al., 2023, pp. 1–46). Distinguishing between a flaw and an unavoidable or inherent risk associated with the intended use of AI remains inherently difficult.

Furthermore, under established product liability doctrines, the "component parts" rule generally excludes component suppliers from liability for harm caused by the final integrated product (Beck & Jacobson, 2017, pp. 143–210). The incorporation of AI systems further complicates liability attribution, as emergent properties may arise from interactions among multiple AI components (Díaz-Rodríguez et al., 2023). This makes it challenging to assign responsibility among the various actors involved in data provision, model development, and system integration.

The EU AI Liability Directive adopted a progressive yet cautious approach to addressing evidentiary challenges posed by multi-purpose AI systems by proposing two key mechanisms: the right to disclosure of evidence and a shift in the burden of proof. These measures were intended to rebalance procedural inequalities between claimants and powerful AI developers by empowering courts to order the disclosure of relevant technical information, such as system logs and training data, from high-risk AI providers. At the same time, national courts would have been permitted to presume causality where claimants could demonstrate that an AI system's failure plausibly caused the harm suffered, thereby easing evidentiary burdens in civil liability claims. While these mechanisms would have enhanced access to justice for victims, they also raised concerns about excessive disclosure of proprietary algorithms and the potential chilling effect on innovation. The Directive's emphasis on procedural fairness reflected the EU's preference for soft harmonization rather than strict liability. However, its withdrawal has created a regulatory gap in addressing evidentiary asymmetries in AI-related litigation (Ziosi et al., 2023).

As a result, plaintiffs may continue to face significant difficulties in obtaining sufficient evidence to prove that an AI system caused alleged harm, particularly because relevant algorithms and operational processes are often protected as proprietary information and not easily discoverable. This also complicates the apportionment of damages, as harms caused by AI systems may consist not of isolated losses but of cumulative minor inconveniences or diffuse negative externalities. Legislative reform may therefore be necessary to clarify procedural mechanisms in AI-related litigation. Such reforms could include requiring AI companies to establish integrated AI incident response teams to address liability claims or to maintain detailed data logs, testing records, and validation documentation for AI systems implicated in harm.

Guidelines on Business Ethics

There are multiple approaches to ethical AI, which are reflected in a range of core principles and bodies of work. One prominent example is the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, which has developed a set of principles for ethical AI known as the IEEE standards for AI (Jedličková, 2024, pp. 1–14). These principles can serve as a foundation for developing AI systems that are safe and socially relevant, in line with widely accepted societal values. Issues of bias and non-bias are critical considerations in the advancement of AI systems, along with principles of fairness and equality.

Improving collaboration among academia, industry, and government can contribute to greater transparency in AI systems and help ensure accountability for the outcomes they produce (Sharma, 2024). The integration of perspectives from disciplines such as computer science, law, ethics, and the

social sciences can provide the expertise needed to address the complex and multi-layered challenges of AI governance.[21]

This paper advocates for the development of collaborative governance models, emphasizing that this should be understood as a long-term process that demands sustained and coordinated effort. AI governance requires the participation of a broad range of societal actors, including policymakers, industry and business representatives, non-governmental organizations, and the general public (Zaidan & Ibrahim, 2024, pp. 1–18). Such inclusive involvement will help ensure that current and future AI systems are developed and deployed in accordance with diverse perspectives and expectations. In this way, collaborative governance supports responses to the complexity and multidimensional nature of AI governance challenges. The establishment of independent regulatory agencies for AI implementation is also proposed as a means of ensuring oversight and improving efficiency that encompasses multiple stakeholders.

Balancing Competing Interests

One of the central challenges of AI governance is the need to balance competing interests, including privacy, intellectual property rights, and transparency (Walter, 2024). Particular tension exists between the demand for transparency in AI processing and the protection of user privacy, indicating that while transparency is important, it should not be pursued in a manner that infringes upon individual privacy rights (Ramya et al., 2025, pp. 85–110). Various approaches have been proposed to address this discord, such as the use of differential privacy techniques, which aim to preserve individual privacy while maintaining a degree of transparency. These approaches highlight the difficulty of protecting proprietary innovations while simultaneously promoting transparency.

Because machine learning algorithms are often protected as intellectual property, companies are generally reluctant to disclose them, which can result in reduced transparency. To address these competing concerns, legal and policy recommendations have been proposed that would permit access to AI systems by third-party auditors under conditions that preserve confidentiality and anonymity.

Facebook* faced a class action lawsuit in which it was accused of violating the Illinois Biometric Information Privacy Act (BIPA)[22] by using facial recognition technology to collect and store its users' biometric data without their consent. In 2020, the company settled the case for $650 million (Nieves, 2021, pp. 1–20). This outcome was subsequently affirmed by the United States Court of Appeals for the Ninth Circuit in the well-known *Patel v. Facebook, Inc.* case.[23] In addition, in 2023, the Illinois Supreme Court issued another significant decision concerning BIPA enforcement. In *Cothron v. White Castle System, Inc.*,[24] the Court reaffirmed its prior jurisprudence by holding that each instance of biometric data collection without required consent constitutes a separate BIPA violation. This ruling has substantial implications for the calculation of damages and poses significant legal risks to organizations that fail to comply with the statute.

[21] Teixeira, N., & Pacione, M. (2024). *Implications of Artificial Intelligence on Leadership in Complex Organizations: An Exploration of the Near Future* [MRP]. OCAD University. https://openresearch.ocadu.ca/id/eprint/4190/

* 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.

[22] Biometric Information Privacy Act of 2009, 740 ILCS 14/1–14/99 (Ill.).

[23] 932 F.3d 1264 (9th Cir. 2019).

[24] 2023 IL 128004.

Legal Challenges in AI Decision Making

A fault-based liability system, which requires proof of negligence or intent, is ill-suited to AI systems that operate autonomously or rely on opaque machine-learning processes and are, in many cases, beyond the direct control or even full understanding of users and developers alike (Botero Arcila, 2024). The evidentiary burden imposed by such a system would create unnecessary obstacles for victims, particularly in high-stakes sectors such as autonomous transportation or healthcare, where AI malfunctions may result in catastrophic harm. By contrast, a strict liability regime, which does not require proof of fault, is more compatible with the unpredictability and risk profile of advanced AI systems, especially those classified as high-risk under the AI Act.[25] However, the blanket application of strict liability may stifle innovation and impose disproportionate burdens on small-scale developers.

An alternative approach offering a more balanced solution is a hybrid liability model that combines strict liability for operators or deployers of high-risk AI systems with fault-based liability for designers and developers (Popa Tache & Vâlcu, 2025, pp. 281–305). Under this model, primary responsibility rests with the "AI owner" or deploying entity—such as a hospital, logistics provider, or digital platform—that determines how and where the system is used. Secondary liability may be attributed to developers or manufacturers where defects in design, training, or system updates can be demonstrated. Regulators may further support this framework by imposing obligations related to transparency, risk assessment, and insurance coverage. Ultimately, the construction of AI liability regimes must protect victims without imposing undue constraints on responsible innovation by ensuring accountability across the entire AI value chain and adapting legal frameworks to the distinctive risks and opacity associated with intelligent systems (Zekos, 2023, pp. 293–359).

Policy Recommendation on the Need for a Visionary Legal Framework for AI

There is an urgent need to establish a progressive legal framework that addresses liability for high-intelligence AI systems involved in decision-making in critical sectors such as healthcare, transportation, security, and commerce. Existing liability regimes, which are largely premised on human agency, are inadequate to address the challenges posed by autonomous and opaque AI-driven decision-making. The central legal questions that require resolution include identifying who should bear liability when harm is caused through the use of AI and determining how causation and fault should be established in a manner that balances innovation with justice. Addressing these issues is essential to ensure that the legal system evolves alongside technological development rather than lagging behind it.

The law should clearly distinguish between actors across the AI value chain in order to allocate liability appropriately. A recommended approach is a tiered liability model, under which strict liability is imposed on deployers and operators of high-risk AI systems—namely, those entities that choose to integrate such systems into real-world contexts, oversee their operation, and derive benefits from their use. These actors are generally best positioned to assess contextual risks and to implement appropriate protective measures. Conversely, liability for AI developers and model providers should be based on fault, with particular emphasis placed on whether reasonable care was exercised with respect to transparency, safety, and diligence in the design, training, and updating of AI systems. This approach encourages prudent behavior while avoiding undue constraints on innovation.

[25] Buiten, M., De Streel, A., & Peitz, M. (2021). *EU Liability Rules for the Age of Artificial Intelligence*. Social Science Research Network. https://doi.org/10.2139/ssrn.3817520

To address the difficulties associated with establishing causation and fault, traditional evidentiary rules must be adapted. AI systems are often described as "black boxes," making it difficult to trace specific outcomes to particular design or operational decisions. Accordingly, the legal framework should adopt a presumption of causality whereby, if an AI system causes harm, courts presume a causal link between the system and the injury. The burden would then shift to the operator or developer to demonstrate that appropriate care was taken to prevent this harm. Such a shift acknowledges the practical impossibility faced by victims in unpacking complex AI operations while incentivizing risk prevention by AI stakeholders.

In addition, the legal framework should mandate transparency, auditability, and traceability throughout the development and deployment of AI systems. Regulators should require that high-risk AI systems implement robust logging mechanisms, including comprehensive decision logs and metadata audit trails, to enable the reconstruction of system behavior in the context of liability proceedings. These technical requirements should be formalized through binding regulations similar to safety standards found in sectors such as pharmaceuticals or aviation. Establishing such shared evidentiary infrastructure would facilitate reasoned adjudication of responsibility and encourage openness in system design.

Given the distributed and collaborative nature of AI development, the framework should also incorporate mechanisms for shared liability in situations where responsibility cannot be clearly attributed to a single actor. For example, assigning joint and several liability may be appropriate in cases where commercial AI systems incorporate open-source models or third-party application programming interfaces. In cases where attribution remains particularly difficult, the establishment of AI compensation funds or mandatory insurance schemes for high-risk AI activities could provide effective remedies for victims while maintaining trust in the AI ecosystem and avoiding deterrence of investment.

From a governance perspective, there should be a central AI regulatory or supervisory authority with a mandate to enforce liability rules, issue binding safety certifications, and resolve disputes. This body should coordinate with sector-specific regulators and data protection authorities to ensure consistency in standards and enforcement. It should also maintain a public registry of certified high-risk AI systems and compliance audit reports, thereby enhancing transparency, accountability, and public oversight. Such an institution would serve both preventive and adjudicatory functions.

A forward-looking, dynamic, and socio-technically sensitive AI liability framework must take into account the technological complexity inherent in artificial intelligence. It should define liability across the entire AI lifecycle, reconceptualize evidentiary rules to address informational opacity, establish enforceable transparency and monitoring obligations, and provide effective compensation mechanisms. Crucially, it should also be aligned at the international level to avoid regulatory fragmentation and to support the safe, fair, and innovative development of AI on a global scale. Public policy should reinforce these objectives by embedding them within AI ecosystems and ensuring that legislative efforts continue to safeguard fundamental rights alongside technological progress.

Conclusion

This paper confirms that the emergence of AI-based decision-making and autonomous systems fundamentally disrupts existing liability frameworks, which were developed on the assumption of human actors and deterministic causation. Its central finding is that traditional tort, contract, and product liability regimes are inadequate in situations where autonomous systems operate with a high degree of independence, giving rise to significant challenges in assigning accountability when harm occurs.

A further key observation is that responsibility for AI-related harm cannot be easily attributed to a single actor. Instead, liability is often distributed among developers, manufacturers, deployers, and users. This diffusion of responsibility underscores the need for more refined mechanisms to allocate liability, particularly in high-risk sectors such as healthcare, transportation, and finance, where autonomous decision-making may generate systemic risks.

The study also highlights the limited effectiveness of fault-based liability mechanisms when applied in isolation and suggests that strict liability and risk-distribution models may be more effective in ensuring compensation and deterrence. Comparative analysis indicates that jurisdictions such as the European Union are moving toward more harmonized regulatory approaches, including the AI Liability Directive and reforms to product liability frameworks, while the United States has largely retained a sector-specific regulatory model.

Finally, the paper argues for a reconciliation of innovation and accountability through the implementation of transparency, explainability, and auditability requirements in AI systems. Liability regimes will need to evolve toward hybrid models that integrate fault-based, strict, and enterprise liability in order to ensure legal certainty and maintain public trust in autonomous technologies.

References

1. Dalsaniya, A., & Patel, K. (2022). Enhancing process automation with AI: The role of intelligent automation in business efficiency. *International Journal of Science and Research Archive*, *5*(2), 322–337. https://doi.org/10.30574/ijsra.2022.5.2.0083
2. Adigwe, C. S., Olaniyi, O. O., Olabanji, S. O., Okunleye, O. J., Mayeke, N. R., & Ajayi, S. A. (2024). Forecasting the future: The interplay of artificial intelligence, innovation, and competitiveness and its effect on the global economy. *Asian Journal of Economics, Business and Accounting*, *24*(4), 126–146. https://doi.org/10.9734/ajeba/2024/v24i41269
3. Adnan, M., Xiao, B., Ali, M. U., Bibi, S., Yu, H., Xiao, P., Zhao, P., Wang, H., & An, X. (2024). Human inventions and its environmental challenges, especially artificial intelligence: New challenges require new thinking. *Environmental Challenges*, (16), Article 100976. https://doi.org/10.1016/j.envc.2024.100976
4. Ahmed, I. (2023). ACLU v. Clearview Ai, Inc., 2021 Ill. Cir. LEXIS 292. *DePaul Journal of Art, Technology & Intellectual Property Law*, *33*(1), 66–95.
5. Amelin, R., Channov, S., Dobrobaba, M., Kalinina, L., & Kholodnaya, E. (2022). Transformation of legal personality in the context of the development of modern digital technologies. *International Journal of Computer Science & Network Security, 22*(11), 294–302.
6. Atakishiyev, S., Salameh, M., Yao, H., & Goebel, R. (2024). Explainable artificial intelligence for autonomous driving: A comprehensive overview and field guide for future research directions. *IEEE Access*, (12), 101603–101625. https://doi.org/10.1109/ACCESS.2024.3431437

7. Attaran, M. (2020). Digital technology enablers and their implications for supply chain management. *Supply Chain Forum: An International Journal*, *21*(3), 158–172. https://doi.org/10.1080/16258312.2020.1751568
8. Aysolmaz, B., Müller, R., & Meacham, D. (2023). The public perceptions of algorithmic decision-making systems: Results from a large-scale survey. *Telematics and Informatics*, *79*, Article 101954. https://doi.org/10.1016/j.tele.2023.101954
9. Bathla, G., Bhadane, K., Singh, R. K., Kumar, R., Aluvalu, R., Krishnamurthi, R., Kumar, A., Thakur, R. N., & Basheer, S. (2022). Autonomous vehicles and intelligent automation: Applications, challenges, and opportunities. *Mobile Information Systems*, *2022*, Article 7632892. https://doi.org/10.1155/2022/7632892
10. Beck, J., & Jacobson, M. (2017). 3D printing: What could happen to products liability when users (and everyone else in between) become manufacturers. *Minnesota Journal of Law, Science and Technology*, *18*(1), 143–210.
11. Botero Arcila, B. (2024). AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight? *Computer Law & Security Review*, *54*, Article 106012. https://doi.org/10.1016/j.clsr.2024.106012
12. Bublitz, J. C. (2024). Might artificial intelligence become part of the person, and what are the key ethical and legal implications? *AI & SOCIETY*, *39*(3), 1095–1106. https://doi.org/10.1007/s00146-022-01584-y
13. Cantero Gamito, M., & Marsden, C. T. (2024). Artificial intelligence co-regulation? The role of standards in the EU AI Act. *International Journal of Law and Information Technology*, *32*, Article eaae011. https://doi.org/10.1093/ijlit/eaae011
14. Chukwuani, V. N., & Egiyi, M. A. (2020). Automation of accounting processes: Impact of artificial intelligence. *International Journal of Research and Innovation in Social Science*, *4*(8), 444–449.
15. Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López De Prado, M., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, Article 101896. https://doi.org/10.1016/j.inffus.2023.101896
16. Dong, Y., Hou, J., Zhang, N., & Zhang, M. (2020). Research on how human intelligence, consciousness, and cognitive computing affect the development of artificial intelligence. *Complexity*, *2020*, 1–10. https://doi.org/10.1155/2020/1680845
17. Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., … Wright, R. (2023). Opinion Paper: "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, *71*, Article 102642. https://doi.org/10.1016/j.ijinfomgt.2023.102642
18. Göksal, Ş.-İ., & Solarte-Vasquez, M. C. (2024). The blockchain-based trustworthy artificial intelligence supported by stakeholders-in-the-loop model. *Scientific Papers of the University of Pardubice, Series D: Faculty of Economics and Administration*, *32*(2). https://doi.org/10.46585/sp32022083
19. Greenstein, S., & Zamboni, M. (2025). Navigating the legislative dilemma: Evaluating the EU AI Act's approach to regulating emerging technologies. *The Theory and Practice of Legislation*, *13*(3), 312–352. https://doi.org/10.1080/20508840.2025.2513177
20. Grozdanovski, L. (2025). Non-discrimination law, the GDPR, the AI act and the—Now withdrawn—AI liability directive proposal offering gateways to pre-trial knowledge of algorithmic discrimination. *AI and Ethics*, *5*(5), 5039–5062. https://doi.org/10.1007/s43681-025-00754-0
21. Hacker, P. (2023). The European AI liability directives – Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, *51*, Article 105871. https://doi.org/10.1016/j.clsr.2023.105871

22. Holzinger, A., Keiblinger, K., Holub, P., Zatloukal, K., & Müller, H. (2023). AI for life: Trends in artificial intelligence for biotechnology. *New Biotechnology*, *74*, 16–24. https://doi.org/10.1016/j.nbt.2023.02.001
23. Hopgood, A. A. (2021). *Intelligent systems for engineers & scientists: A practical guide to artificial intelligence*. CRC Press Inc. https://doi.org/10.1201/9781003226277
24. Jedličková, A. (2025). Ethical approaches in designing autonomous and intelligent systems: A comprehensive survey towards responsible development. *AI & Society*, *40*(4), 2703–2716. https://doi.org/10.1007/s00146-024-02040-9
25. Khaleel, M., Jebrel, A., & Shwehdy, D. M. (2024). Artificial intelligence in computer science. *International Journal of Electrical Engineering and Sustainability*, *2*(2), 1–21. https://doi.org/10.5281/zenodo.13836932
26. Kumar, Y., Koul, A., Singla, R., & Ijaz, M. F. (2023). Artificial intelligence in disease diagnosis: A systematic literature review, synthesizing framework and future research agenda. *Journal of Ambient Intelligence and Humanized Computing*, *14*(7), 8459–8486. https://doi.org/10.1007/s12652-021-03612-z
27. Lehmann, J., Schorz, S., Rache, A., Häußermann, T., Rädle, M., & Reichwald, J. (2023). Establishing reliable research data management by integrating measurement devices utilizing intelligent digital twins. *Sensors*, *23*(1), Article 468. https://doi.org/10.3390/s23010468
28. Lesenciuc, A. (2024). Defective truth. AI or HI ideological imprints and political biases? *Romanian Journal of Information Technology and Automatic Control*, *34*(3), 9–22. https://doi.org/10.33436/v34i3y202401
29. Leslie, D., & Perini, A. M. (2024). Future shock: Generative AI and the international AI policy and governance crisis. *Harvard Data Science Review*, (Special Issue 5). https://doi.org/10.1162/99608f92.88b4cc98
30. Li, B., Qi, P., Liu, B., Di, S., Liu, J., Pei, J., Yi, J., & Zhou, B. (2023). Trustworthy AI: From principles to practices. *ACM Computing Surveys*, *55*(9), Article 177. https://doi.org/10.1145/3555803
31. Lucci, S., Musa, S., & Kopec, D. (2022). *Artificial intelligence in the 21st century* (3rd ed.). Mercury Learning and Information. https://doi.org/10.1515/9781683922520
32. Markauskaite, L., Marrone, R., Poquet, O., Knight, S., Martinez-Maldonado, R., Howard, S., Tondeur, J., De Laat, M., Buckingham Shum, S., Gašević, D., & Siemens, G. (2022). Rethinking the entwinement between artificial intelligence and human learning: What capabilities do learners need for a world with AI? *Computers and Education: Artificial Intelligence*, *3*, Article 100056. https://doi.org/10.1016/j.caeai.2022.100056
33. McCarthy, J. (2022). Artificial intelligence, logic, and formalising common sense. In *Machine learning and the city* (pp. 69–90). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119815075.ch6
34. Mecaj, S. E. (2022). Artificial intelligence and legal challenges. *Revista Opinião Jurídica (Fortaleza)*, *20*(34), 181–196. https://doi.org/10.12662/2447-6641oj.v20i34.p180-196.2022
35. Mijwil, M., Aljanabi, M., & ChatGPT. (2023). Towards artificial intelligence-based cybersecurity: The practices and ChatGPT generated ways to combat cybercrime. *Iraqi Journal for Computer Science and Mathematics*, *4*(1). https://doi.org/10.52866/ijcsm.2023.01.01.0019
36. Mikki, S. (2024). Generalized neuromorphism and artificial intelligence: Dynamics in memory space. *Symmetry*, *16*(4), Article 492. https://doi.org/10.3390/sym16040492
37. Nieves, A. M. (2021). Facial recognition technology: Can we tame the wild west? *Journal of Law and Technology at Texas, 5*, 1–20.
38. Nikolinakos, N. Th. (2024). Reforming the EU civil liability framework applicable to artificial intelligence and other emerging digital technologies: Defective products—The revised Product Liability Directive. In N. Th. Nikolinakos (Ed.), *Adapting the EU civil liability regime to the digital age: Artificial intelligence, robotics, and other emerging technologies* (pp. 477–621). Springer International Publishing. https://doi.org/10.1007/978-3-031-67969-8_9
39. Paesano, A. (2021). Artificial intelligence and creative activities inside organizational behavior. *International Journal of Organizational Analysis*, *31*(5), 1694–1723. https://doi.org/10.1108/IJOA-09-2020-2421

40. Patel, K. (2024). Ethical reflections on data-centric AI: Balancing benefits and risks. *International Journal of Artificial Intelligence Research and Development (Ijaird)*, *2*(1), 1–17.
41. Perwej, Y., Akhtar, N., & Agarwal, D. (2024). The emerging technologies of Artificial Intelligence of Things (AIoT): Current scenario, challenges, and opportunities. In *Convergence of artificial intelligence and internet of things for industrial automation* (pp. 1–32). CRC Press.
42. Popa Tache, C. E., & Vâlcu, E. N. (2025). Artificial intelligence and corporate liability towards a new legal-ethical contract in the dynamics of emerging global human rights convergences. *Juridical Tribune-Review of Comparative and International Law*, *15*(2), 281-305.
43. Ramya, R., Priya, S., Thamizhikkavi, P., & Anand, M. (2025). The pillars of AI ethics: Transparency, accountability, and privacy. In *Responsible implementations of generative AI for multidisciplinary use* (pp. 85–110). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-9173-0.ch004
44. Sado, F., Loo, C. K., Liew, W. S., Kerzel, M., & Wermter, S. (2023). Explainable goal-driven agents and robots: A comprehensive review. *ACM Computing Surveys*, *55*(10), Article 211. https://doi.org/10.1145/3564240
45. Saeik, F., Avgeris, M., Spatharakis, D., Santi, N., Dechouniotis, D., Violos, J., Leivadeas, A., Athanasopoulos, N., Mitton, N., & Papavassiliou, S. (2021). Task offloading in edge and cloud computing: A survey on mathematical, artificial intelligence and control theory solutions. *Computer Networks*, *195*, Article 108177. https://doi.org/10.1016/j.comnet.2021.108177
46. Salvini, P., Reinmund, T., Hardin, B., Grieman, K., Ten Holter, C., Johnson, A., Kunze, L., Winfield, A., & Jirotka, M. (2023). Human involvement in autonomous decision-making systems. Lessons learned from three case studies in aviation, social care and road vehicles. *Frontiers in Political Science*, *5*, Article 1238461. https://doi.org/10.3389/fpos.2023.1238461
47. Sayre, M., & Glover, K. (2024). Machines make mistakes too: Planning for AI liability in contracting. *Journal of Law, Technology, & the Internet*, *15*(2), 357–394.
48. Schmidt, J., Schutte, N. M., Buttigieg, S., Novillo-Ortiz, D., Sutherland, E., Anderson, M., de Witte, B., Peolsson, M., Unim, B., Pavlova, M., Stern, A. D., Mossialos, E., & van Kessel, R. (2024). Mapping the regulatory landscape for artificial intelligence in health within the European Union. *NPJ Digital Medicine*, *7*(1), Article 229. https://doi.org/10.1038/s41746-024-01221-6
49. Sharma, S. (2024). Benefits or concerns of AI: A multistakeholder responsibility. *Futures*, *157*, Article 103328. https://doi.org/10.1016/j.futures.2024.103328
50. Sosnowski, M. J., & Brosnan, S. F. (2023). Under pressure: The interaction between high-stakes contexts and individual differences in decision-making in humans and non-human species. *Animal Cognition*, *26*(4), 1103–1117. https://doi.org/10.1007/s10071-023-01768-z
51. Taeihagh, A., Ramesh, M., & Howlett, M. (2021). Assessing the regulatory challenges of emerging disruptive technologies. *Regulation & Governance*, *15*(4), 1009–1019. https://doi.org/10.1111/rego.12392
52. Telikani, A., Tahmassebi, A., & Gandomi, A. (2021). Evolutionary machine learning: A survey. *ACM Computing Surveys*, *54*, 1–35. https://doi.org/10.1145/3467477
53. Walter, Y. (2024). Managing the race to the moon: Global policy and governance in Artificial Intelligence regulation—A contemporary overview and an analysis of socioeconomic consequences. *Discover Artificial Intelligence*, *4*(1), Article 14. https://doi.org/10.1007/s44163-024-00109-4
54. Zaidan, E., & Ibrahim, I. A. (2024). AI governance in a complex and rapidly changing regulatory landscape: A global perspective. *Humanities and Social Sciences Communications*, *11*(1), Article 1121. https://doi.org/10.1057/s41599-024-03560-x
55. ZainEldin, H., Gamel, S. A., Talaat, F. M., Aljohani, M., Baghdadi, N. A., Malki, A., Badawy, M., & Elhosseini, M. A. (2024). Silent no more: A comprehensive review of artificial intelligence, deep learning, and machine learn-

ing in facilitating deaf and mute communication. *Artificial Intelligence Review*, *57*(7), Article 188. https://doi.org/10.1007/s10462-024-10816-0

56. Zekos, G. I. (2023). *Artificial intelligence and competition: Economic and legal perspectives in the digital age*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-48083-6
57. Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. *Journal of Industrial Information Integration*, *23*, Article 100224. https://doi.org/10.1016/j.jii.2021.100224
58. Ziosi, M., Mökander, J., Novelli, C., Casolari, F., Taddeo, M., & Floridi, L. (2023). The EU AI liability directive (AILD): Bridging information gaps. *European Journal of Law and Technology*, *14*(3).

Information about the author:

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

Сведения об авторе:

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

https://doi.org/10.38044/2686-9136-2025-6-16

ЗАМЕТКИ

ПРАВОВОЕ ОФОРМЛЕНИЕ ПЛАТФОРМЕННОЙ ЗАНЯТОСТИ В РОССИИ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РЕФОРМЫ

И. С. Семенова

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Поволжский институт управления имени П. А. Столыпина)
410012, Россия, Саратов, ул. Московская, 164

Аннотация

Последний день июля 2025 года ознаменовался принятием Федерального закона «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации» № 289-ФЗ. Это было ожидаемо и давно назрело. Еще в 2024 г. в послании Федеральному Собранию РФ Президент РФ объявил, что к 2030 г. во всех ключевых отраслях жизнедеятельности страны должны быть созданы цифровые платформы. Платформизация оказалась актуальной, эффективной и, соответственно, востребованной во всех сферах. Не стала исключением и занятость населения. Для устранения уязвимостей, по мнению экспертного сообщества, необходима была новая редакция Федерального закона «О занятости населения в Российской Федерации» от 12 декабря 2023 г. № 565-ФЗ. Но законодатели пошли другим путем, приняв рассматриваемый закон. Основной целью исследования видится краткий обзор правового режима платформенной занятости в контексте законодательной новеллы исходя из сложившихся в настоящий момент научных представлений о концепции платформенной занятости. Исследование базируется на доступных доктринальных источниках о платформенной занятости, релевантных законодательных актах и публикациях в профессиональных СМИ. В исследовании использован формально-юридический метод — для толкования норм, а также системный метод для обобщения научной доктрины и оценки введенных в закон понятий с точки зрения сложившихся представлений об области и техники законотворчества. Сделан вывод, что к положительным аспектам данного регулирования следует отнести введение понятийного аппарата, например «партнер посреднической цифровой платформы», установление классификации партнеров, возможность рейтингования сторон, а также уточнение их прав и обязанностей. Вместе с тем в тексте закона недостаточно четко прослеживается классификация платформ, и это представляется недостатком реформы. В заключение автор отмечает положительный вектор развития законодательства о платформенной занятости и указывает на необходимость принятия подзаконных нормативных правовых актов в развитие данного института.

Ключевые слова

платформа, платформенная занятость, платформизация, платформенная экономика, платформенный занятый, платформенные работники

Конфликт интересов Автор сообщает об отсутствии конфликта интересов.

Финансирование Исследование не имеет спонсорской поддержки.

Для цитирования Семенова, И. С. (2025). Правовое оформление платформенной занятости в России: современное состояние и перспективы реформы. *Цифровое право, 6*(4), 101–112. https://doi.org/10.38044/2686-9136-2025-6-16

Поступила: 06.10.2025, принята в печать: 01.12.2025, опубликована: 30.12.2025

NOTES

LEGAL FRAMEWORK OF PLATFORM EMPLOYMENT IN RUSSIA: OUTCOMES AND PROSPECTS OF REFORM

Iraida S. Semyonova

Russian Presidential Academy of National Economy and Public Administration (Stolypin Volga Region Institute of Administration)
164, Moskovskaya St., Saratov, Russia, 410012

Abstract

The last day of July 2025 was marked by the adoption of Federal Law No. 289-FZ "On Certain Issues of Regulating the Platform Economy in the Russian Federation," fulfilling a long-standing need. Back in 2024, in a message to the Federal Assembly of the Russian Federation, the President of the Russian Federation highlighted the strategic priority of developing digital platforms in all key sectors of the country by 2030. Platformization proved to be relevant, effective and, consequently, highly demanded in all areas, including employment. According to experts, the Federal Law "On Employment in the Russian Federation" dated December 12, 2023, No. 565-FZ required revision to eliminate certain vulnerabilities. However, the legislators took a different course and adopted the law in question. In this article, the author carries out a brief review of the legal framework governing platform employment under the adopted law, taking into account current scientific concepts of platform employment. The research was conducted using available sources of information about platform employment, legislative acts, and publications in professional media. Legal norms were examined using the formal-legal method of analysis. The systems method was applied to generalize the academic doctrine and to assess the concepts introduced into the law in view of established perspectives within the field and legislative drafting practices. Among the positive aspects of the legislation under analysis are the introduction of a conceptual framework, including the notion of a "partner of an intermediary digital platform," the classification of partners, the possibility of rating parties, and clarification of their rights and duties. At the same time, the text of the law does not provide a sufficiently clear classification of platforms, which represents a shortcoming of the reform. In conclusion, the author notes a positive trajectory in the development of legislation on platform employment and emphasized the need to adopt subordinate regulatory acts to further develop this institution.

Keywords

platform, platform employment, platformization, platform economy, platform employees

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Semyonova, I. S. (2025). Legal framework of platform employment in Russia: Outcomes and prospects of reform. *Digital Law Journal, 6*(4), 101–112. https://doi.org/10.38044/2686-9136-2025-6-16

Submitted: 6 Oct. 2025, accepted: 1 Dec. 2025, published: 30 Dec. 2025

Введение

В современных реалиях бурного развития информационных технологий и в связи с тем, что четвертая промышленная революция совершается на наших глазах, неизбежна трансформация всех общественных отношений. Новый тренд современного мира — платформизация.

Это, в свою очередь, образовало поныне неизвестный вид взаимоотношений цифровых платформ и неограниченного круга лиц, получающих доход посредством доступа к различным видам работ (курьерские услуги, такси, клининг, репетиторство и др.). Возможности гибкого графика, взаимодействия с несколькими платформами одновременно, получения дополнительного дохода способствуют росту благосостояния граждан. Однако регулирование отношений между платформами и исполнителями в большинстве стран отсутствует, в том числе до недавнего времени и в Российской Федерации.

Вместе с тем остаются вопросы в части социальной и пенсионной обеспеченности платформенных занятых, недопущения дискриминации платформенных занятых, а также отграничения реальных платформ от де-факто работодателей, заключающих притворные гражданско-правовые договоры с сотрудниками.

Поводом к подготовке данной статьи послужило принятие 31 июля 2025 г. Федерального закона «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации»[1] (далее — Закон о платформенной экономике). Основной целью исследования видится краткий обзор правового режима платформенной занятости в контексте законодательной новеллы исходя из сложившихся в настоящий момент научных представлений о концепции платформенной занятости.

Исследование базируется на доступных доктринальных источниках о платформенной занятости, релевантных законодательных актах и публикациях в профессиональных СМИ. В исследовании использован формально-юридический метод — для толкования норм, а также системный метод для обобщения научной доктрины и оценки введенных в закон понятий с точки зрения сложившихся представлений об области и техники законотворчества.

Правовое оформление платформенной занятости

Концепция цифровой трансформации государственного управления «Государство-как-платформа» была заложена еще Указом Президента РФ от 07 мая 2018 г. № 204 «О национальных

[1] Федеральный закон «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации» от 31 июля 2025 г. № 289-ФЗ. Российская газета, 06.08.2025, № 172–173.

целях и стратегических задачах развития Российской Федерации на период до 2024 года»[2]. А уже в 2024 г. в послании Федеральному Собранию РФ Президент РФ объявил о запуске нового национального проекта «Экономика данных», одной из целей которого является создание к 2030 г. во всех ключевых отраслях жизнедеятельности страны цифровых платформ[3].

Так, по мнению М. С. Орешкина «цифровые платформы формируют новую экономическую реальность», платформизация играет ключевую роль в экономической революции, которую мы сейчас видим воочию[4].

Не стала исключением и сфера занятости населения. Еще недавно профессия на всю жизнь и пожизненная занятость на одном предприятии были нормой, сегодня же подобная стабильность скорее редкость. Прирост занятости последних лет сильно связан со стремительным проникновением платформ в разные сферы нашей экономики, а все потому, что платформизация приблизила экономику к людям[5].

Платформенная занятость — активно растущий как в мире, так и в России сегмент нестандартной занятости с использованием онлайн-платформ и цифровых технологий. В 2022–2023 гг., согласно оценкам Всемирного банка, комбинирующим информацию из нескольких источников, в платформенную занятость были включены 154–435 млн человек, или от 4,4 до 12% мировой рабочей силы, в зависимости от метода учета[6].

Низкие барьеры для входа в платформенную экономику и предоставляемые ею автономность и гибкость делают платформенную занятость привлекательным форматом дополнительной занятости для работников традиционной экономики, а также основной занятости для групп, уязвимых на обычных рынках труда и испытывающих сложности с поиском работы.

По данным исследования ВЦИОМ на тему труда и занятости, в топ-10 ожиданий от работы на пятом месте находится удобный график. Соответственно, деньги и достойная оплата труда являются важными факторами, но иногда преобладает «карибское» мировоззрение, что все же лучше быть хорошо отдохнувшим, чем хорошо заработавшим[7].

К основным преимуществам платформенной занятости относятся расширение базы заказчиков за рамки своей среды обитания, возможность работать практически из любого места, самостоятельно планировать собственный график; к основным недостаткам — отсутствие соцпакета, а также нестабильность заработка.

Столь массовое и масштабное явление, как платформенная занятость, однозначно должно регулироваться федеральным законом, так как именно закон по своей юридической природе должен регламентировать принципиально важные и устойчивые отношения в обществе

[2] Указ Президента Российской Федерации от 7 мая 2018 г. N 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года». Российская газета, 09.05.2018, № 97с.

[3] Послание Президента Российской Федерации Федеральному Собранию Российской Федерации от 29 февраля 2024 г. http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=606589470

[4] Гринкевич, Д., Харнас, А., & Кудрявцева, Е. (2025, 16 июня). *Максим Орешкин: «Цифровые платформы — это новая плановая экономика»*. Эксперт. https://expert.ru/mnenie/maksim-oreshkin-tsifrovye-platformy-eto-novaya-planovaya-ekonomika/. См. также: Балашова, М. (2024, 7 июня). *Как платформы стали фундаментом новой экономики*. РБК Отрасли. https://www.rbc.ru/industries/news/666184909a794797dcc32d74

[5] См. колоритные иллюстрации в интервью М.С. Орешкина: Гринкевич, Д., Харнас, А., & Кудрявцева, Е. (2025, 16 июня). *Максим Орешкин: «Цифровые платформы — это новая плановая экономика»*. Эксперт. https://expert.ru/mnenie/maksim-oreshkin-tsifrovye-platformy-eto-novaya-planovaya-ekonomika/

[6] Оценки Всемирного Банка приведены по Sinyavskaya et al. (2024, p. 4).

[7] Верижников, А. (2024, 4 апреля). *Не только деньги, или Как выбирают работу в России.* ВЦИОМ. https://wciom.ru/expertise/ne-tolko-dengi-ili-kak-vybirajut-rabotu-v-rossii

и государстве. И вот первое, но при этом основополагающее узкое место: экспертное сообщество спорит о степени необходимого законодательного регулирования деятельности платформ. Одни полагают, что избыточная регламентация платформенной занятости затормозит развитие платформ[8]; другие убеждены, что настоящего регулирования недостаточно ввиду неравного положения субъектов: у платформ высокий уровень влияния, а платформенные работники лишены ряда социальных гарантий, которые предоставлены работникам государством и регулируются Трудовым кодексом РФ[9]. И сразу видится следующая проблема: одни признают платформенную занятость видом трудовых отношений[10], другие — гражданско-правовых[11], а третьи приводят доводы, что это новый тип отношений[12].

Справедливости ради надо обозначить, что в 2023 г. в нижнюю палату парламента был внесен проект федерального закона «О занятости населения в Российской Федерации», отразивший изменившиеся форматы занятости[13]. Однако ко второму чтению из него исключили нормы о платформенной занятости[14]. Заявлялось, что в связи с тем, что платформенная занятость — это совершенно новая, гибридная форма занятости, представляющая собой не двусторонние, а трехсторонние отношения, принято решение разработать и внести в 2024 г. в Государственную Думу ФС РФ законопроект «О платформенной занятости»[15].

В послании Президента Федеральному Собранию РФ от 29 февраля 2024 г. отмечено, что повышение эффективности всех сфер производительности труда неразрывно связано с цифровизацией, которая дает возможность создавать цифровые платформы, позволяющие оптимально выстроить взаимодействие граждан, бизнеса и государства[16].

25 апреля 2023 г. компании «Яндекс», *OZON*, *Wildberries*, *HeadHunter*, «СберМаркет», *Avito*, «Газпром нефть», *YouDo* объявили о создании Совета цифровых платформ при Российском союзе промышленников и предпринимателей и подписали Хартию о принципах развития платформенной занятости в России. Цель компаний — обмениваться эффективными практиками и создавать благоприятные условия сотрудничества для всех, кто ежедневно предоставляет и использует цифровые сервисы[17].

В литературе выделяют следующие аспекты платформенной занятости, требующие четкого законодательного регулирования:

1) социальное страхование и контроль за налогообложением (Zueva, 2024, p. 277; Shibarshina, 2025, p. 100);

---

[8] Центр стратегических разработок. (2022). *Платформенная занятость: вызовы и возможные решения*. https://www.csr.ru/upload/iblock/6ca/krk89ha0yxx3ystja243obvc7ly8bntv.pdf

[9] См., например, Loktyukhina & Chernykh (2020).

[10] См.: Zaytseva & Mitryasova (2018).

[11] К примеру, Rozhkova (2022).

[12] Например, Bazzhina et al. (2014).

[13] Законопроект «О занятости населения в Российской Федерации» № 275599-8. https://sozd.duma.gov.ru/bill/275599-8

[14] Там же.

[15] Совет Федерации Федерального Собрания Российской Федерации. (2024, 5 апреля). *И. Святенко: Платформенная занятость должна быть интегрирована в систему трудовых и экономических отношений*. http://council.gov.ru/events/news/155295/

[16] Послание Президента Российской Федерации В.В. Путина Федеральному Собранию Российской Федерации от 29 февраля 2024 г. http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=606589470

[17] Российский союз промышленников и предпринимателей. (2023, 25 апреля). *Цифровые компании подписали Хартию о принципах развития платформенной занятости в России*. https://rspp.ru/events/news/tsifrovye-kompanii-podpisali-khartiyu-o-printsipakh-razvitiya-platformennoy-zanyatosti-v-rossii-6447d9185ac30/?sphrase_id=4722789

2) политика защиты интересов клиентов платформ, которые в текущих российских реалиях часто не защищены от обмана, ущерба и ненадлежащего качества услуг, и прозрачные методы разрешения споров между клиентами и работниками (Chernykh, 2020, p. 95)[18];
3) информационное обеспечение платформенной занятости, создание систем мониторинга, ведения статистики и реализации на местах мероприятий по информированию (Ibragimkhalilova & Ovchinikova, 2024, p. 132);
4) определение основных понятий сферы платформенной занятости, конкретизация правового статуса платформенных занятых и правового режима цифровых трудовых платформ (Zabelina & Sergeyeva, 2024, p. 10)[19] и др.

31 июля 2025 г. принят Закон о платформенной экономике, который положил начало формированию базовой регуляторной рамки рассматриваемого института. Закон вступает в силу 1 октября 2026 г., поэтому, как сообщили представители Минэкономразвития России, основной акцент в ближайшие месяцы на работе над подзаконными актами, запуске механизма реестра цифровых платформ и подготовке разъяснений[20].

«Указанные цели регулирования, — согласно пояснительной записке к проекту федерального закона "Об отдельных вопросах регулирования платформенной экономики в Российской Федерации", — соответствуют национальным целям развития Российской Федерации, установленным подпунктами "в", "д" и "е" п. 1 Указа Президента РФ от 7 мая 2024 г. № 309 "О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года"[21], а именно: комфортная и безопасная среда для жизни, устойчивая и динамичная экономика и технологическое лидерство»[22].

Закон разработан во исполнение поручения Правительства РФ и направлен на урегулирование дисбаланса в правоотношениях, возникающих между операторами посреднических цифровых платформ, их партнерами и пользователями таких платформ при продаже товаров, выполнении работ и оказании услуг. Востребованность платформенной экономики предопределяет ее значительное влияние на гражданский оборот, на экономическое и правовое положение представителей малого и среднего предпринимательства, использующих цифровые платформы, а также на интересы потребителей.

Закон о платформенной экономике видится базовым документом, определяющим цели, основные понятия и принципы правового регулирования данной сферы, а также организацию взаимодействия всех субъектов на платформе.

---

18 По мнению Т. Б. Ивановой и С. М. Мироновой, необходимо расширить функции государственных трудовых инспекций по институциональным формам защиты, возложив на инспекции не только контроль за соблюдением норм трудового права, но и разрешение конфликтов самозанятых с платформой в части оплаты труда, введения штрафов, установления избыточных требованиях к условиям труда (Ivanova & Mironova, 2024, p. 154).

19 Как считает А. В. Серова, требуется разработка уровней правового статуса платформенных трудящихся: общий (общий для всех платформенных трудящихся), видовой (для самозанятых и для работников), специальный (уникальные положения для платформенных самозанятых и работников) (Serova, 2022, p. 265). По мнению А. Я. Нурика, к платформенным занятым должны применяться международные стандарты в контексте действующих конвенций и рекомендаций Международной организации труда и пактов Организации Объединенных Наций (Nurik, 2024, p. 45).

20 Центр стратегических разработок. (2025, 31 июля). *В ЦСР обсудили, как будет развиваться регулирование платформенной занятости.* https://www.csr.ru/ru/news/v-tssr-obsudili-kak-budet-razvivatsya-regulirovanie-platformennoy-zanyatosti/

21 Указ Президента РФ «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» от 7 мая 2024 г. № 309. Российская газета, 11.05.2024, № 100.

22 Пояснительная записка к проекту федерального закона «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации». https://sozd.duma.gov.ru/download/1f058ab6-411d-6f82-9de6-bd83686ba7fd

Занятость как таковая в Законе о платформенной экономике не указана. По моему мнению, это связано с тем, что в платформенной экономике исчезает привычный формат отношений работника и работодателя, но одновременно характер отношений между индивидуальными подрядчиками (платформенными занятыми) и их клиентами (заказчиками), опосредуемых платформами и регулируемых алгоритмами, не в полной мере может быть отнесен и к привычным форматам самозанятости или индивидуального предпринимательства.

Буквально в первых статьях данного Закона мы видим ответ на ключевой вопрос в теории платформенной занятости — классификацию отношений между цифровыми платформами и трудящимися. Те, кого ранее называли «платформенные занятые», «экономически зависимые самозанятые работники», «платформенные работники», «экономически зависимые работники», «гиг-работники» и т. д., в соответствующих пунктах ст. 2 рассматриваемого Закона, где даны определения основных понятий, именуются «партнеры».

Под партнером посреднической цифровой платформы понимается «юридическое лицо, иностранное юридическое лицо, иностранная организация, не являющаяся юридическим лицом, индивидуальный предприниматель либо физическое лицо, в том числе иностранный гражданин или лицо без гражданства (за исключением физических лиц, совершающих между собой на посреднической цифровой платформе сделки, не связанные с осуществлением предпринимательской деятельности), применяющие специальный налоговый режим “Налог на профессиональный доход”» (п. 4 ст. 2 Закона о платформенной экономике). Уже здесь становится ясно, что вряд ли это будут «партнеры по труду» или «трудовые партнеры», так как слово «партнер» все-таки из сферы гражданско-правового оборота. И в следующих пунктах мы убеждаемся в правильности своего предположения: установлено, что партнер заключает гражданско-правовой договор с оператором платформы (см. п. 5–6 ст. 2). Таким образом, из трех распространенных в экспертной среде вариантов сферы регулирования законодатель предпочел остановиться на гражданско-правовой.

Получается, что партнерами платформы могут быть юридическое лицо, индивидуальный предприниматель и самозанятый (специальный налоговый режим), т. е. для работы на платформе физическое лицо регистрируется либо в качестве индивидуального предпринимателя, либо в качестве самозанятого, без соответствующих статусов физическое лицо не может стать партнером платформы. Соответственно, «платформенные занятые» и «самозанятые» не тождественные понятия. Самозанятые могут быть партнерами платформе, а также работать офлайн. В соответствии с п. 4 ст. 3 Федерального закона «О занятости населения в Российской Федерации»[23] граждане, выполняющие работы по договорам гражданско-правового характера, предметами которых являются выполнение работ и (или) оказание услуг, в том числе договорам авторского заказа, являются занятыми. Соответственно, практически снимается вопрос о контроле за налогообложением.

Учитывая разнородность деятельности, которую возможно осуществлять на платформах, законодатель выделяет два вида партнеров: партнер-продавец[24] и партнер-исполнитель[25]. При этом партнер-продавец – это «партнер, заключивший гражданско-правовой договор с оператором посреднической цифровой платформы и осуществляющий деятельность на посреднической цифровой платформе, направленную на продажу товаров

[23] Федеральный закон «О занятости населения в Российской Федерации» от 12 декабря 2023 г. № 565-ФЗ (ред. от 8 августа 2024 г.) (с изм. и доп., вступ. в силу с 1 марта 2025 г.). Российская газета, 18.12.2023, № 286.

[24] П. 5 ст. 2 Закона о платформенной экономике.

[25] П. 6 ст. 2 Закона о платформенной экономике.

пользователям-покупателям», а партнер-исполнитель — «партнер, заключивший гражданско-правовой договор с оператором посреднической цифровой платформы и осуществляющий деятельность на посреднической цифровой платформе, направленную на выполнение работ, оказание услуг для пользователей-заказчиков в рамках гражданско-правовых отношений при условии соблюдения требований, предусмотренных законом». Видится, что классификация как метод познания и регулирования деятельности партнеров на платформе является позитивным моментом, так как позволяет детально выявить особенности партнеров и учесть их при регулировании взаимодействия.

Впрочем, классификации платформ на виды или типы не прослеживается в тексте Закона, и это, на мой взгляд, недостаток регулирования: единые нормы для платформ с принципиально разными моделями — от маркетплейсов до агрегаторов услуг — могут обернуться рисками для гибкости и занятости.

Законодатель воспринял предложения ученых в вопросе осуществления рейтинга как товара, работы и услуги, так и деятельности партнера, рассчитываемого оператором платформы с учетом выставленных пользователями оценок, а также иных критериев, предусмотренных правилами пользования платформой[26]. Несмотря на то что это является правом оператора, а не обязанностью, следует оценить это положительно ввиду установления возможности оценивания потенциальных рисков при сотрудничестве.

Обратимся к обширному вопросу регулирования взаимодействия операторов, пользователей и партнеров-исполнителей, являющихся физическими лицами.

Прежде всего обращает на себя внимание то, что при заключении договора с партнером оператор осуществляет проверку сведений о лице, имеющем намерение стать партнером, способами, установленными Правительством РФ[27]. Однозначно это хорошо, но насколько эти сведения будут исчерпывающими и помогут принять правильное решение, зависит от соответствующего подзаконного нормативного акта, который установит перечень сведений и методы их получения.

Но уже сейчас законодатель, пытаясь полностью отграничить платформенную экономику от сферы трудовых отношений, определил, что партнер — физическое лицо не должен иметь режима (графика) работы, правил внутреннего трудового распорядка и содержащих нормы трудового права локальных нормативных актов оператора и (или) пользователя-заказчика[28]; вправе не принимать заказ без применения к нему мер ответственности[29]; за выполненную работу или оказанную услугу оператором начисляется вознаграждение в рамках каждого заказа отдельно[30]; оператор или пользователь-заказчик не предоставляет ему еженедельных выходных дней и отпуск, предусмотренных трудовым законодательством РФ[31]. Разграничение со смежными институтами — это всегда благо для результативного регулирования общественных отношений.

Оператор платформы обязан размещать договор с партнером с указанием периода действия этого договора, а также предоставлять партнеру беспрепятственный доступ к данному договору и договорам, утратившим силу, в том числе для ознакомления и копирования, в Интернете

[26] П. 2 ст. 17 Закона о платформенной экономике.

[27] П. 2 ст. 5 Закона о платформенной экономике.

[28] П. 1 ст. 15 Закона о платформенной экономике.

[29] П. 2 ст. 15 Закона о платформенной экономике.

[30] П. 4 ст. 15 Закона о платформенной экономике.

[31] Пп. «в» п. 5 ст. 15 Закона о платформенной экономике.

или в соответствующем разделе личного кабинета партнера в течение сроков хранения таких документов, но не менее трех лет[32]. Эта норма закрепляет институт информационного обеспечения партнеров платформ как на протяжении всего периода взаимодействия, так и по окончании его. Следует добавить, что это не единственная обязанность оператора платформы в плане информационного обеспечения.

Так, оператор обязан:

- «устанавливать и публиковать на посреднической цифровой платформе стандарты качества и безопасности выполнения работ, оказания услуг, в отношении которых размещаются заказы, в том числе требования к подтверждению квалификации партнера-исполнителя, необходимой для выполнения работ, оказания услуг, связанных с опасностью для жизни и здоровья»;
- «обеспечивать ознакомление партнера с основными условиями заказа»;
- «предоставлять партнеру техническую возможность ознакомиться с предложениями страховых организаций и негосударственных пенсионных фондов и подавать заявку на заключение договора добровольного страхования и негосударственного пенсионного обеспечения, если указанные организации и фонды воспользовались возможностью разместить такие предложения на платформе»;
- «по запросу страховых организаций, негосударственных пенсионных фондов обеспечивать равные возможности размещения на посреднической цифровой платформе информации о предлагаемых ими страховых продуктах добровольного медицинского страхования, негосударственного пенсионного обеспечения и добровольного страхования от несчастных случаев и болезней, а также техническую возможность заключения соответствующих договоров при наличии такой возможности у этих организаций и фондов»[33].

Следует признать, что институт гражданско-правовой ответственности в части применения оператором в отношении партнера негативных мер, например ограничения доступа партнера к личному кабинету, достаточно регламентирован.

При этом является обязательным, согласно п. 4 ч. 4 ст. 5 Закона о платформенной экономике, «досудебное рассмотрение жалоб или разрешение споров между оператором платформы и партнером, за исключением случаев, когда ограничение размещения карточки товара или прекращение размещения карточки товара и ограничение доступа к личному кабинету осуществлены оператором в целях исполнения вступившего в законную силу решения суда, решения органа государственной власти».

Статья 16 Закона о платформенной экономике определяет права и обязанности партнера-исполнителя, являющегося физическим лицом, при взаимодействии с оператором. Приветствуется, что наблюдается явный перекос в сторону большего количества прав. При этом в обязанности партнера входит самостоятельное исполнение заказов в рамках гражданско-правовых отношений с учетом законодательства Российской Федерации, стандартов качества и безопасности выполнения работ, оказания услуг, установленных оператором, требований к выполнению работ, оказанию услуг, устанавливаемых оператором и пользователем-заказчиком, соблюдение предусмотренных законодательством Российской Федерации требований к выполнению отдельных работ.

Обращает на себя внимание тот факт, что во избежание «ухода в тень» трудящихся посредством платформ разработан механизм, открывающий таким занятым

[32] П. 5 ст. 5 Закона о платформенной экономике.

[33] Ст. 17 Закона о платформенной экономике.

доступ к основным социальным гарантиям, состоящий из прав и обязанностей оператора платформ[34].

К таковым обязанностям можно отнести установление ограничения на систематическое и продолжительное выполнение работ, оказание услуг партнером в интересах одного пользователя-заказчика с использованием платформы оператора; осуществление контроля за соблюдением максимального времени систематического и продолжительного выполнения работ, оказания услуг, связанных с использованием партнером источника повышенной опасности или риском причинения вреда жизни, здоровью и имуществу третьих лиц; предоставление преференций партнерам добровольно вступившим в правоотношения по обязательному пенсионному страхованию, обязательному социальному страхованию на случай временной нетрудоспособности и в связи с материнством, а также заключившим договоры добровольного медицинского страхования, негосударственного пенсионного обеспечения, добровольного страхования от несчастных случаев и болезней. Набор преференций и их количество, а также возможность применения сразу нескольких в Законе не установлены, соответственно, ждем нормы подзаконного акта или внесения изменений и дополнений в действующее законодательство[35].

Среди прав оператора следует выделить право полностью или частично возмещать расходы партнеров добровольно вступивших в правоотношения по обязательному пенсионному страхованию, обязательному социальному страхованию на случай временной нетрудоспособности и в связи с материнством, в части осуществления страховых взносов, а также расходы этих партнеров-исполнителей по договорам добровольного медицинского страхования, негосударственного пенсионного обеспечения, добровольного страхования от несчастных случаев и болезней; право предоставлять возможность получения партнерами дополнительного профессионального образования, а также организовывать обучение этих партнеров, в том числе с использованием программ для электронных вычислительных машин, интернет-сайтов и мобильных приложений, в целях соблюдения стандартов качества и безопасности выполнения работ, оказания услуг и повышения качества исполнения заказов; право предоставлять партнеру инструменты и материалы для исполнения заказа, в том числе одежду, в соответствии со стандартами качества и безопасности выполнения работ, оказания услуг в порядке и на условиях, которые установлены оператором[36].

Получается, что законодатель со своей стороны сделал всё возможное, чтобы обеспечить баланс интересов платформенных занятых, операторов платформ и государства: Закон о платформенной экономике не только вводит в правовое поле большое количество соответствующих дефиниций, но и позволяет решить проблемы социальной защиты платформенных работников.

Заключение

Подводя итог, следует подчеркнуть, что современное состояние законодательной базы платформенной занятости в виде Закона о платформенной экономике характеризуется незавершенностью формирования и систематизации. Необходимость принятия подзаконных нормативных правовых актов в развитие данного института бесспорна. Вместе с тем анализ имеющегося, но не вступившего в силу законодательства подтверждает недостаточное нормативно-правовое

[34] Ст. 17 Закона о платформенной экономике.

[35] П. 1 ст. 17 Закона о платформенной экономике.

[36] П. 2 ст. 17 Закона о платформенной экономике.

обеспечение ряда положений на основе системного мониторинга и прогнозирования. В целом положительный вектор развития законодательства о платформенной занятости способствует совершенствованию отношений, связанных со взаимодействием на платформе, что пойдет на пользу всем сторонам.

Список литературы / References

1. Bazzhina, V. A., Tsygankova, I. V., & Nikishina, O. Yu. (2014). Razvitiye nestandartnykh form zanyatosti v sovremennoy Rossii [Developing types of non-standard employment in contemporary Russia]. *Rossiyskoye Predprinimatel'stvo*, (24), 71–86.
2. Chernykh, E. A. (2020). Kachestvo platformennoy zanyatosti: Neustoychivyye (prekarizovannyye) formy, praktiki regulirovaniya, vyzovy dlya Rossii [The quality of platform employment: Unstable (precarious) forms, regulatory practices, challenges for Russia]. *Uroven' Zhizni Naseleniya Regionov Rossii*, *16*(3), 82–97. https://doi.org/10.19181/lsprr.2020.16.3.7
3. Ibragimkhalilova, T. V., & Ovchinikova, K. O. (2024). Kompleksnyy organizatsionnyy mekhanizm funktsionirovaniya platformennoy zanyatosti [A comprehensive organizational mechanism for the functioning of the employment platform]. *Gosudarstvennoye Upravleniye i Pravo*, (2), 123–134.
4. Ivanova, T. B., & Mironova, S. M. (2024). Sravnitel'nyy analiz razvitiya traditsionnykh i platformennykh otnosheniy zanyatosti [Comparative analysis of developing traditional and platform employment relations]. *Vestnik Moskovskogo Universiteta. Seriya 6 "Ekonomika", 59*(4), 135–159. https://doi.org/10.55959/MSU0130-0105-6-59-4-7
5. Loktyukhina, N. V., & Chernykh, E. A. (2020). Dinamika i kachestvo platformennoy zanyatosti v epokhu koronavirusa: Vyzovy dlya Rossii [Dynamics and quality of platform employment in the era of coronavirus: Challenges for Russia]. *Uroven' Zhizni Naseleniya Regionov Rossii*, *16*(4), 80-95. https://doi.org/10.19181/lsprr.2020.16.4.7
6. Nurik, A. Ya. (2024). Nekotoryye tezisy k diskussii o regulirovanii platformennoy zanyatosti [Some theses to the discussion on the regulation of platform employment]. *Mariyskiy Yuridicheskiy Vestnik*, (3–4), 35–47.
7. Rozhkova, A. Yu. (2022) Osobennosti distantsionnogo truda: setevaya i platformennaya zanyatost' [Particularities of remote labour: Network and platform employment]. *Yuridicheskiy Vestnik Dagestanskogo Gosudarstvennogo Universiteta, 42*(2), 112–120. https://doi.org/10.21779/2224-0241-2022-42-2-112-120
8. Serova, A. V. (2022). V poiskakh kontseptsii pravovogo regulirovaniya platformennoy zanyatosti [Legal regulation of platform employment: In search of a concept]. *Vestnik Tomskogo Gosudarstvennogo Universiteta*, (477), 260–268. https://doi.org/10.17223/15617793/477/30
9. Shibarshina, O. Yu. (2025). Platformennaya zanyatost' v RF: Organizatsionno-pravovyye osobennosti i vektory razvitiya [Platform employment in the Russian Federation: Organizational and legal features and development vectors]. *Vestnik Moskovskogo Universiteta Imeni S. Yu. Vitte. Seriya 1 "Ekonomika i upravleniye"*, (1), 95–103. https://doi.org/10.21777/2587-554X-2025-1-95-103
10. Sinyavskaya, O. V., Biryukova, S. S., Kareva, D. E., & Stuzhuk, D. A. (2024). *Platformennaya zanyatost' v Rossii: Dinamika rasprostranennosti i klyuchevyye kharakteristiki zanyatykh* [Platform-based employment in Russia: Prevalence dynamics and key characteristics of workers]. HSE Publishing House. https://doi.org/10.17323/978-5-7598-4067-1
11. Zabelina, O. V., & Sergeyeva, M. V. (2024). Platformennaya zanyatost' v Rossiyskoy Federatsii: Masshtaby, pravovyye osobennosti i tendentsii razvitiya [Digital platform employment in Russia: Scale, legal features and development trends]. *Sotsial'no-trudovyye Issledovaniya*, (4), 8–20. https://doi.org/10.34022/2658-3712-2024-57-4-8-20

12. Zaytseva L. V., & Mitryasova A. S. (2018). Trud voditeley taksi na osnove internet-platform: Otdel'nyye voprosy pravovogo regulirovaniya [Labor of taxi drivers on the basis of Internet platforms: Some issues of legal regulation]. *Vestnik Tomskogo Gosudarstvennogo Universiteta*, (435), 239–245. https://doi.org/10.17223/15617793/435/30
13. Zueva, K. A. (2024). Platformennaya zanyatost' kak perspektivnaya forma zanyatosti v Rossiyskoy Federatsii: voprosy pravovogo regulirovaniya [Platform employment as a promising form of employment in the Russian Federation: Issues of legal regulation]. *Nauchno-Tekhnicheskoye i Ekonomicheskoye Sotrudnichestvo Stran ATR v XXI veke*, *2*, 275–281.

Сведения об авторе:

Семенова И. С. — кандидат юридических наук, доцент кафедры служебного и трудового права, Поволжский институт управления имени П. А. Столыпина, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Саратов, Россия.
slava210767@yandex.ru

Information about the author:

Iraida S. Semyonova — Ph.D. in Law, Associate Professor of the Department of Service and Labor Law, Russian Presidential Academy of National Economy and Public Administration, Povolzhsky Institute of Management named after P. A. Stolypin, Saratov, Russia.
slava210767@yandex.ru