

УДК 342.7

## Цифровые права в качестве современных конституционных ценностей: обеспечение приватности и безопасности персональных данных

Кирпиченко Каролина Владимировна, студент, Донской государственный технический университет, karolinakirpichenko@yandex.ru

Сизько Игорь Александрович, доцент кафедры уголовного права и публично-правовых дисциплин, Донской государственный технический университет, кандидат юридических наук, isizko@donstu.ru

Значимость исследования цифровых прав как современных конституционных ценностей обусловлена углублением процессов цифровизации общественных отношений и возрастанием роли информационных технологий в жизни личности, общества и государства. В статье рассматривается становление цифровых прав в качестве конституционных ориентиров, оказывающих влияние на формирование современного правопорядка. Основное внимание уделяется праву личности на приватность в цифровой среде и обеспечению безопасности персональных данных, значимость которых возрастает по мере усложнения цифрового пространства. Анализируются российские правовые стандарты защиты цифровых прав, а также подходы государств, поддерживающих устойчивое взаимодействие с Российской Федерацией. Рассматриваются проблемы, возникающие при автоматизированной обработке данных, применении алгоритмических технологий и трансграничном обмене информацией. Выявлены ключевые риски для приватности, включая чрезмерное накопление сведений о пользователях, формирование поведенческих профилей, непрозрачность алгоритмов обработки информации, вероятность утечек данных и усиление контроля со стороны компаний и государственных органов. Обосновано, что эффективная реализация цифровых прав возможна при сочетании правового регулирования, повышения уровня цифровой грамотности граждан и внедрения этико-ориентированных принципов обращения с информацией.

Ключевые слова: цифровые права, приватность, персональные данные, информационная безопасность, алгоритмическая обработка данных, цифровая среда.

Право на частную жизнь в сети и контроль над персональными сведениями сегодня превращаются в одну из ключевых составляющих современной правовой архитектуры, что обусловлено экспоненциальным ростом объема цифровых следов, которые ежедневно создаются частными лицами и компаниями.

В условиях доминирования социальных платформ, цифровых сервисов и облачных хранилищ практически любая активность пользователя в сети превращается в ценную информацию, порождая новые задачи для правового регулирования [1].

Обеспечение цифровых прав осложняется трансграничным характером интернета, при котором информация перемещается между серверами разных стран и подпадает под действие несовпадающих правовых режимов. Это вызывает вопросы о соблюдении правовых норм различных государств, о порядке уведомления и получения согласия пользователей на обработку их данных, а также о механизмах контроля за соблюдением данных прав [2].

Среди наиболее значимых рисков цифровой приватности можно выделить незаметное для пользователя накопление персональных данных, формирование обширных профилей без согласия субъекта, уязвимости в системах хранения и закрытость алгоритмов обработки информации. Все это требует скоординированных мер как со стороны государства, так и со стороны частного сектора [3].

Надлежащая защита прав в цифровой среде возможна лишь при реализации многокомпонентной стратегии, основанной на сочетании нормативного регулирования, технологической модернизации и повышении уровня информированности населения. На законодательном уровне ключевое значение имеют нормы о персональных данных, кибербезопасности и регулировании алгоритмической обработки информации.

В России защита персональных данных обеспечивается Федеральным законом N 152-ФЗ, который определяет правовые рамки обработки сведений о гражданах — от момента их получения до последующего хранения и удаления, а также закрепляет право субъекта данных на доступ к своим сведениям, их уточнение и удаление в случае нарушения установленных правил обработки [4].

Аналогичные правовые механизмы развиваются и в ряде государств-партнеров Российской Федерации. Так, в Республике Казахстан действует Закон «О персональных данных и их защите», предусматривающий обязательные меры безопасности при обработке сведений и ответственность операторов за допущенные утечки [5]. В Республике Беларусь законодательство направлено на усиление государственного контроля над обращением персональных данных и защиту прав граждан при их использовании цифровыми сервисами [6]. Расширение такого нормативно-правового взаимодействия в дружественном международном пространстве способствует формированию единых подходов к охране цифровой приватности и укреплению гарантий информационной безопасности личности [5; 6].

Анализ недавних инцидентов показывает, что утечки персональных сведений в России имеют устойчивый характер и фактически стали нормой для цифровой инфраструктуры. Так, только в 2024 г. было зафиксировано 135 случаев распространения баз с личной информацией, что привело к публикации более 710 млн записей. Однако это лишь часть проблемы: общее число скомпрометированных записей, по оценкам экспертов, превысило 1,58 млрд. Уже в 2023 г. утечки затронули порядка 1,12 миллиарда записей, что на 60 % больше по сравнению с 2022 г. Даже с учетом частичной анонимизации и удаления отдельных данных специалисты указывают, что персональная информация может быть доступна в отношении от половины до 90 % взрослого населения страны. Все это подчеркивает, что цифровая приватность в России представляет собой не абстрактное понятие, а крайне актуальную проблему, требующую оперативного внимания со стороны государства, бизнеса и общества.

Технологический аспект защиты включает применение шифрования, цифровых идентификаторов, распределенных реестров и продвинутых систем контроля доступа. Указанные технологии заметно сокращают вероятность несанкционированного доступа к конфиденциальной информации и повышают уровень доверия общества к цифровым сервисам [7]. Существенную роль играет внед-

рение независимых проверок функционирования алгоритмов, позволяющих выявлять нарушения принципов справедливости и конфиденциальности при автоматизированной обработке данных [10].

Особое значение имеет обучение граждан цифровой безопасности и правовой культуре, что позволяет им более осознанно управлять собственными данными и снижать риск их неправомерного использования. Программы повышения правовой и информационной культуры пользователей способствуют пониманию значимости защиты персональных данных, снижению числа нарушений и повышению уровня осведомленности о возможных рисках. Внедрение образовательных модулей, посвященных этике применения цифровых технологий и защите данных, способствует формированию правового мышления, адаптированного к реалиям цифровой экономики [11].

Международная координация усилий становится ключевым фактором формирования универсальных стандартов защиты цифровых прав и ответственности компаний за обработку пользовательской информации. Совместные инициативы, такие как рекомендации ОЭСР, деятельность Всемирной организации интеллектуальной собственности (ВОИС), а также разработка глобальных стандартов кибербезопасности, позволяют гармонизировать под-

ходы к защите персональных данных и обеспечивать ответственность цифровых платформ за их обработку [12].

Значительные трудности вызывает применение систем искусственного интеллекта, поскольку их закрытая архитектура может порождать ошибки, дискриминационные решения и нарушения прав личности. В связи с этим все чаще поднимается вопрос о нормативном закреплении «права на объяснение» автоматизированных выводов и возможности их пересмотра.

Закрытость логики функционирования алгоритмов приводит к тому, что гражданин нередко не понимает причин принятия системой того или иного решения, что усиливает риск ошибок и дискриминации и обуславливает необходимость внедрения принципа «права на объяснение», а также механизмов обжалования решений автоматизированных систем.

Таким образом, формирование устойчивого режима цифровых прав требует комплексного подхода, включающего совершенствование законодательства, внедрение соответствующих технологических инструментов и системное просвещение пользователей. Сочетание указанных элементов формирует среду, в которой обеспечивается защита частной жизни, а сбор и использование данных становятся прозрачными и подотчетными.

#### Примечания

1. Алферова М. В. Цифровые права: понятие и особенности их защиты // Молодой ученый. 2023. N 49.
2. Айкинская А. А. Защита персональных данных в эпоху цифровизации // Молодой ученый. 2024. N 2.
3. Богатырев К. М. Угрозы медиабезопасности в цифровой среде: систематизация и анализ // Актуальные проблемы российского права. 2022. N 7.
4. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» // Собрание законодательства РФ. 2006. N 31 (ч. 1). Ст. 3451.
5. Закон Республики Казахстан от 21.05.2013 N 94-V «О персональных данных и их защите» // Ведомости Парламента Республики Казахстан. 2013.
6. Закон Республики Беларусь от 07.05.2021 N 99-3 «О защите персональных данных» // Национальный правовой Интернет-портал Республики Беларусь. URL: <https://pravo.by/?ysclid=mjhh7adxbz966186769> (дата обращения: 20.12.2025).
7. Солдатова Г. У., Рассказова Е. И., Нестик Т. А. Цифровое поколение России: компетентность и безопасность: монография. М., 2017.
8. Кутейников Д. Л., Ижаев О. А., Зенин С. С., Лебедев В. А. Алгоритмическая прозрачность и подотчетность: правовые подходы к разрешению проблемы «черного ящика» // Lex Russica. 2020. N 6.
9. Морозова С. С., Смирнова Ю. Г. Защита прав граждан современной России в цифровую эпоху: политико-правовой анализ // Креативная экономика. 2024. N 6.
10. Прокопец Г. К. Цифровые права личности в конституционном праве // Научный лидер. 2022. N 31.
11. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris, 2023.
12. Деев С. А. Перспективы и проблемы применения искусственного интеллекта в правотворческой деятельности и в правоприменении // Молодой ученый. 2022. N 38.

#### English version

Digital rights as contemporary constitutional values: ensuring privacy and personal data security

Kirpichenko Karolina Vladimirovna, student, Don State Technical University

Siz'ko Igor' Aleksandrovich, associate professor of the department of criminal law and public law disciplines, Don State Technical University, candidate of sciences (law)

The relevance of studying digital rights as contemporary constitutional values is determined by the deepening digitalization of social relations and the increasing role of information technologies in the life of the individual, society, and the state. This article examines the development of digital rights as constitutional guidelines that influence the formation of the modern legal order. Particular attention is paid to the individual right to privacy in the digital environment and to ensuring the security of personal data, the significance of which grows as the digital space becomes more complex. The study analyzes Russian legal standards for the protection of digital rights, as well as the approaches of states maintaining stable interaction with the Russian Federation. It also considers challenges arising from automated data processing, the use of algorithmic technologies, and cross-border information exchange. Key risks to privacy are identified, including excessive accumulation of user data, the creation of behavioral profiles, the lack of transparency of data-processing algorithms, the likelihood of data breaches, and increased control by corporations and public authorities. The article substantiates that the effective realization of digital rights is possible through a combination of legal regulation, the enhancement of citizens' digital literacy, and the implementation of ethics-oriented principles of information governance.

Keywords: digital rights, privacy, personal data, information security, algorithmic data processing, digital environment.