

УДК 34.03

## Законность и юридическая ответственность: современные вызовы цифровизации

Морозова Лада Евгеньевна, студент, Донской государственный технический университет, ladilla.m@yandex.ru

Приймак Елена Николаевна, старший преподаватель, Донской государственный технический университет, кандидат психологических наук, erpimak@donstu.ru

В статье исследуются трансформация принципов законности и особенности реализации механизмов юридической ответственности в условиях цифровизации. Анализируются ключевые правовые противоречия, возникающие при регулировании цифровых отношений, и предлагаются направления совершенствования нормативной правовой базы. Особое внимание уделяется вопросам защиты персональных данных, противодействия киберпреступности и обеспечения баланса между развитием цифровых технологий и соблюдением требований законности.

Ключевые слова: цифровизация, юридическая ответственность, законность, цифровое право, искусственный интеллект, персональные данные, киберпреступления.

Стремительная цифровизация всех сфер общественной жизни порождает принципиально новые вызовы для правовой системы. Традиционные механизмы обеспечения законности и привлечения к юридической ответственности сталкиваются с различными проблемами: скоростью технологических изменений, сложностью идентификации субъектов правоотношений, а также отсутствием судебной практики и другими пробелами, возникающими ежедневно.

Цель исследования обусловлена необходимостью создания соответствующего правового регулирования цифровой среды при сохранении фундаментальных принципов законности.

Российской Федерации за январь–июль 2025 г. зарегистрировано 424,9 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Ущерб от данных преступлений за семь месяцев увеличился на 16 % — со 100,5 млрд руб. до 119,6 млрд руб. Это на 2,3 % меньше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 38,9 % в январе–июле 2024 г. до 39,2 % [6]. Данная статистика свидетельствует о том, что киберпреступления продолжают расти, и для их предотвращения требуются модернизация права.

Принцип законности как верховенство закона и недопустимость произвольного правоприменения подвергается испытаниям в условиях цифровизации, т. к. законодательство не успевает за темпами развития данных инноваций. Появление новых цифровых объектов, таких как искусственный интеллект, NFT, криптовалюты и множество других разработок современности, создает правовые пробелы. Конфликты юрисдикций при зарубежных правоотношениях усложняют определение применимого права и компетентного суда. Использование алгоритмов принятия решений создает риски «черного ящика» в правовом регулировании, особенно в случаях, когда алгоритмы нарушают права человека [4].

Российская Федерация уделяет все большее внимание вопросам укрепления информационного правопорядка. В Концепции национальной безопасности РФ подчеркивается, что ключевыми задачами в сфере информационной безопасности страны выступают обеспечение конституционных прав и свобод граждан РФ в области информационной деятельности, развитие и защита национальной информационной инфраструктуры, включение Российской Федерации в глобальное информационное пространство, предотвращение рисков возникновения конфликтов в информационной сфере [5].

В чч. 3 и 4 ст. 29 Конституции РФ закреплено, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом. Гарантируется свобода массовой информации. Цензура запрещается [1]. Это означает, что можно использовать интернет-ресурсы, однако государство имеет возможность ограничивать доступ к ним для защиты прав граждан и безопасности страны. Российская Федерация активно предпринимает меры по обеспечению кибербезопасности и внедрению в законодательство новых проектов для регулирования цифрового права.

Цифровизация радикально трансформирует общепринятые представления о юридической ответственности. Меняются субъекты, объекты, способы совершения правонарушений, методы доказывания и механизмы исполнения санкций.

По мнению С. И. Колотыркиной, цель юридической ответственности трактуется в двух аспектах. В широком смысле она заключается в защите сложившегося общественного уклада и правопорядка, а также в предотвращении будущих правонарушений. В узком смысле — в наказании лица, виновного в совершении деяния. Исходя из этих целевых установок, в виртуальной среде выявляются две ключевые проблемы. Первая — не всегда ясно, какие действия следует считать легитимными в виртуальном пространстве. Вторая — затруднено выявление виновного субъекта, поскольку в киберсреде участвует целая цепочка посредников: от провайдеров услуг до операторов, обрабатывающих персональные данные пользователей [3].

Возникает вопрос: кто есть кто и за что отвечает? При рассмотрении данной проблемы следует проанализировать каждый элемент. В цифровой среде формируются новые субъекты ответственности:

1. Анонимные и псевдонимные участники — лица, использующие VPN, TOR, криптокошельки. Они значительно затрудняют идентификацию, что приводит к росту числа мошеннических действий и киберпреступлений. Выявление правонарушителей становится крайне затруднительным.

2. Автоматизированные системы — боты, алгоритмы, ИИ-агенты, действующие без прямого контроля человека. В случае нарушения, совершенного такими системами, возникает вопрос, кто должен нести ответственность за их действия: разработчик, пользователь или куратор системы. Поскольку законодательство еще не сформировало нормативно-правовые акты, способные регулировать данные отношения, вопрос остается открытым.

3. Децентрализованные автономные организации — структуры без четкой иерархии и центра принятия решений. Поскольку решения принимаются путем голосования через блокчейн и смарт-контракты, отсутствует единый ответственный субъект, что усложняет определение юридической ответственности.

4. Транснациональные платформы — компании, чьи серверы и пользователи находятся в разных юрисдикциях. Регулирование подобных отношений также является сложной задачей.

Общепризнанное право предполагает наличие конкретного физического или юридического лица, подлежащего ответственности. В цифровых реалиях это условие нередко оказывается трудноисполнимым.

Появились и новые объекты, не имеющие традиционных аналогов:

- цифровые активы — криптовалюты, токены, NFT;
- большие данные (Big Data) и алгоритмы их обработки;
- виртуальные пространства — метавселенные, игровые миры;
- цифровые идентичности — аккаунты, профили, цифровые двойники.

Следовательно, подобные новшества требуют пересмотра категорий имущества и посягательства в контексте нематериальных объектов.

В результате развития общества возникла специфика противоправных деяний. Правонарушения приобрели уникальные черты. Можно выделить следующее.

Скорость и масштаб цифровых правонарушений значительно отличаются от традиционных: одно действие может затронуть миллионы пользователей, например при утечке данных. Фиксация и выявление места и времени совершения правонарушения осложняются, т. к. цифровые следы могут быть легко уничтожены или замаскированы. В таких случаях требуется проведение современной экспертизы. Кроме того, одно правонарушение может одновременно нарушать нормы гражданского, административного и уголовного права.

Возникает вопрос о механизмах привлечения к ответственности. Рассмотрим некоторые из них.

Общепринятые санкции возможно адаптировать к цифровой среде, например применять оборотные штрафы за утечки данных, а также конфискацию цифровых активов (криптовалют). Такие меры практически не отличаются от стандартных, но при этом адаптированы к условиям развивающегося общества. С технической стороны допустимо применять блокировку сайтов и приложений, а также ограничивать доступ к сервисам (например, путем отключения от платежных систем). В отношении репутационных инструментов следует использовать публичное раскрытие информации о нарушителях. Включение платформ в «черный список» также представляется эффективной мерой.

Отдельные сферы требуют специализированных подходов. Платформы должны осуществлять контроль за публикуемым контентом, однако они не обязаны отвечать за действия пользователей: к ответственности надлежит привлекать тех лиц, чьи деяния нарушили общественный порядок. Разработчики ИИ обязаны обеспечивать безопасность алгоритмов и функционирование механизмов компенсации вреда, причиненного автономными решениями. В случаях вредоносных воздействий (например, DDoS-атак) следует возлагать коллективную ответственность на хакерские группировки.

Следует отметить, что в Уголовном кодексе РФ предусмотрена специальная глава, посвященная преступлениям в сфере компьютерной информации, — гл. 28 УК РФ [1]. Это свидетельствует о том,

что законодательство, хотя и не успевает изменяться в соответствии с темпами развития цифровой среды, тем не менее постепенно предусматривает необходимые меры по обеспечению цифрового права.

Вследствие проанализированных вопросов необходимо изучить проблемы доказывания цифровых нарушений. Особые сложности возникают при оценке достоверности электронных доказательств, таких как подлинность цифровых подписей, скриншотов, переписки и иных материалов, т. к. эти данные подвержены высокому риску фальсификации. Возникают противоречия между отраслями и системами права, т. к. затруднительно определить, какой суд компетентен рассматривать дело и какие нормы следует применять, если невозможно или крайне сложно установить происхождение, место, время и участников совершения преступления. Для выявления существенных обстоятельств требуется проведение технической экспертизы, следовательно, необходимы специалисты по кибербезопасности, технологиям блокчейна и анализу данных. Стоимость таких услуг достаточно высока, т. к. специалистов, обладающих компетенциями в области цифровых технологий, недостаточно для количества проблем, возникающих в стране.

При регулировании развивающихся цифровых процессов в государстве следует уделить особое внимание вопросам защиты персональных данных и противодействия киберпреступности. Наша страна активно противодействует новым видам преступлений и постепенно внедряет новые способы их регулирования.

Так, ст. 272.1 УК РФ претерпела изменения. С 30 мая 2025 г. вступили в силу изменения в законодательстве, которые усиливают ответственность за нарушения в сфере персональных данных. Теперь предусмотрены оборотные штрафы за утечки, а также уголовная ответственность за незаконный сбор и хранение информации [1].

Практически половина преступлений относится к категории тяжких и особо тяжких. Ущерб составил почти 120 млрд руб. уже к середине текущего года и к настоящему времени значительно возрос. Новые составы преступлений, связанные с передачей и использованием электронных средств платежа в корыстных целях, направлены на борьбу с лицами, которые предоставляют свои банковские карты для обналичивания денежных средств (ч. 3 ст. 187 УК РФ).

Министерство цифрового развития, связи и массовых коммуникаций РФ анонсирует принятие Цифрового кодекса в рамках разработанной стратегии развития отрасли связи до 2035 г. [2]. Данный проект призван существенно улучшить регулирование законности, ответственности и правонарушений в цифровой сфере.

Проанализировав главные аспекты данной темы, представляется необходимым определить направления совершенствования правового регулирования.

Для обеспечения законности в цифровой среде необходимо принять нормативные меры, такие как:

- 1) разработка специализированных законов о цифровой деятельности;
- 2) преобразование составов киберпреступлений и нарушений в УК РФ и Кодексе об административных правонарушениях РФ;
- 2) унификация международных стандартов.

В части технологических решений следует внедрить системы блокчейн-доказательств и иных электронных средств фиксации доказательств, создать цифровые платформы для фиксации правонарушений, а также уделить особое внимание развитию инструментов цифровой криминалистики.

Немаловажно повышение квалификации и обучение гражд-

дан РФ и сотрудников государственных структур. Необходимо формирование специализированных киберподразделений правоохранительных органов, подготовка судей по цифровым делам.

Процедурные инновации также требуются:

- 1) упрощенные механизмы блокировки вредоносного контента;
- 2) электронные формы судопроизводства;
- 3) автоматизированный мониторинг нарушений.

Современные проблемы требуют современных решений, поскольку общепринятые меры поддержания законности и определения юридической ответственности оказываются малоэффективными. Трансформация принципа законности в цифровую эпоху не означает отказа от традиционных ценностей, а предполагает их адаптацию к новым реалиям. Ключевой задачей становится формирование гибкой системы юридической ответственности в различных направлениях.

#### Примечания

1. СПС «КонсультантПлюс». URL: <https://www.consultant.ru> (дата обращения: 30.11.2025).
2. Правовые ресурсы по законодательству, судебной системе, новости и аналитика. Все о юридическом рынке. URL: <https://pravo.ru/news/250016> (дата обращения: 30.11.2025).
3. Рымкевич Я. А. Юридическая ответственность в цифровом пространстве // Образование и право. 2023. N 7.
4. Савченко О. В. Правовое регулирование в цифровой среде: новые вызовы и направления трансформации // Вестник науки. 2025. N 11.
5. Смоленский М. Б., Алексеева М. В. Информационное право: учебник. Ростов-на-Дону, 2015.
6. Статистика деятельности МВД РФ. URL: <https://alf.ru/news/v-rossii-za-yanvar-iyul-2025-goda-ushcherb-ot-it-prestupleniy-vyros-na-16-i-sostavil-pochti-120-mlrd> (дата обращения: 29.11.2025).

#### English version

Legality and legal liability: contemporary challenges of digitalization

Morozova Lada Evgen'evna, student, Don State Technical University

Priymak Elena Nikolaevna, senior lecturer, Don State Technical University, candidate of sciences (psychology)

This article examines the transformation of the principles of legality and the specific features of implementing mechanisms of legal liability in the context of digitalization. It analyzes key legal contradictions that arise in the regulation of digital relations and proposes directions for improving the regulatory framework. Particular attention is paid to issues of personal data protection, counteracting cybercrime, and ensuring a balance between the development of digital technologies and compliance with the requirements of legality.

Keywords: digitalization, legal liability, legality, digital law, artificial intelligence, personal data, cybercrime.