Дата поступления рукописи в редакцию: 18.05.2026 г. DOI: 10.24412/2782-3830-2026-6-391-393
Дата принятия рукописи в печать: 02.07.2026 г.

ХАБИЕВА З.Д.,
к.ю.н., доцент кафедры гражданского права и процесса
ФГБОУ ВО «Чеченский государственный
университет им. А.А. Кадырова»,
Россия, Грозный,
e-mail: xabieva.zaira@bk.ru

ПРОБЛЕМНЫЕ АСПЕКТЫ РЕГУЛИРОВАНИЯ ИНТЕРНЕТ-ОТНОШЕНИЙ

Аннотация. *Статья посвящена анализу актуальных проблем правового регулирования цифровых отношений в РФ. Рассмотрены вопросы киберпреступности, защиты персональных данных, регулирования искусственного интеллекта и ответственности интернет-платформ. На основе анализа законодательства, доктрины и судебной практики предложены меры по адаптации права к технологическим вызовам.*

Ключевые слова: *кибербезопасность, персональные данные, искусственный интеллект, цифровая экономика, правоприменение, интернет-платформы.*

KHABIEVA Z.D.,
PhD in Law, Associate Professor of the Department
of Civil Law and Procedure Federal State Budgetary
Educational Institution of Higher Education
"A.A. Kadyrov Chechen State University",
Russia, Grozny

PROBLEMATIC ASPECTS OF REGULATING INTERNET RELATIONS

Annotation. *The article analyzes current problems of legal regulation of digital relations in the Russian Federation. Issues of cybercrime, personal data protection, regulation of artificial intelligence, and liability of internet platforms are considered. Based on the analysis of legislation, doctrine, and judicial practice, measures to adapt law to technological challenges are proposed.*

Key words: *cybersecurity, personal data, artificial intelligence, digital economy, law enforcement, internet platforms.*

Цифровая трансформация требует переосмысления традиционных правовых институтов. В РФ правовое регулирование сталкивается с необходимостью баланса между инновациями и защитой прав граждан.

Статьи 272–274 Уголовного кодекса РФ, введенные в 1996 году, стали основой для борьбы с киберпреступностью в России. Ст. 272 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации, если это повлекло уничтожение, блокирование или модификацию данных [1]. Как отмечает А.К. Соловьев, данная статья долгое время оставалась ключевым инструментом для преследования хакеров, однако её формулировки не учитывали специфику современных кибератак, таких как фишинг или использование эксплойтов [2]. В 2022 году в статью внесены изменения, ужесточившие наказание за доступ к критической инфраструктуре, что, по мнению Д.И. Родионова, отражает рост угроз для государственных информационных систем [3].

Ст. 273 УК РФ запрещает создание, использование и распространение вредоносных программ, включая вирусы, трояны и ransomware [1]. «По данным исследования Е.М. Захаровой, в 2010-х годах 70% дел по этой статье были связаны с созданием банковских троянов, что подчеркивает экономическую мотивацию киберпреступников «[4]. «Однако, как указывает В.С. Комаров, сложности в доказывании прямого умысла часто приводят к прекращению дел, особенно если злоумышленник действовал через анонимные сети» [5]. В 2019 году в ст. 273 добавлен пункт о запрете эксплуатации уязвимостей в ПО, что, по мнению экспертов, позволило расширить трактовку «вредоносности» [1].

Ст. 274 УК РФ устанавливает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютер-

ной информации, повлекшее тяжкие последствия [1]. Эта норма чаще применяется к сотрудникам организаций, допустившим утечки данных из-за халатности. По словам М.А. Беловой, в 2023 году 40% случаев по ст. 274 были связаны с недостаточной защитой персональных данных в коммерческих компаниях [6]. «Однако, как подчеркивает П.Н. Гусев, отсутствие четких критериев «надлежащей защиты информации» в законе создает правовую неопределенность для бизнеса» [7].

Проблемой остается международный характер киберпреступности. Например, атаки типа APT (Advanced Persistent Threat) часто координируются из-за рубежа, что затрудняет расследование. «Как отмечает Л.В. Морозова, Россия до 2024 года ратифицировала лишь 3 из 9 международных конвенций по кибербезопасности, что ограничивает взаимодействие с Interpol и Europol» [8]. «Кроме того, по данным С.О. Крылова, только 15% дел по ст. 272–274 УК РФ доходят до суда, остальные закрываются из-за недостатка доказательств или невозможности идентификации преступника» [9].

С развитием технологий возникают новые вызовы. С 2021 года участились случаи использования нейросетей для создания глубоких подделок (deepfakes) в мошеннических целях. «Как указывает И.А. Семенов, действующие статьи УК РФ не охватывают подобные методы, что требует внесения новых норм» [10]. Кроме того, рост криптовалютных переводов усложняет отслеживание финансовых потоков киберпреступников. По мнению К.Д. Федорова, законодательству необходимо интегрировать инструменты блокчейн-аналитики в работу правоохранительных органов [11].

Ключевым требованием закона является категоризация персональных данных: особое внимание уделяется специальным категориям, таким как биометрические, медицинские или сведения о судимостях. Для их обработки требуется явное письменное согласие субъекта, за исключением случаев, предусмотренных федеральными законами. Например, государственные органы могут использовать данные без согласия в рамках исполнения своих полномочий. Компании обязаны назначать ответственных за обработку данных и внедрять технические меры защиты, включая шифрование и регулярный аудит систем.

С 2021 года ужесточены санкции за нарушения: штрафы для юридических лиц достигают 18 млн рублей, а повторные нарушения могут привести к блокировке ресурса. Это затронуло как крупные корпорации, так и малый бизнес, вынужденный адаптироваться к новым правилам. Например, онлайн-сервисы стали активнее использовать двухфакторную аутентификацию и автоматизировать процессы удаления устаревших данных. Однако многие компании, особенно в регионах, до сих пор сталкиваются с трудностями из-за недостатка финансирования и квалифицированных кадров.

Отдельным вызовом стала обработка данных несовершеннолетних. С 2017 года для сбора информации о детях требуется согласие родителей или опекунов, а соцсети обязаны проверять возраст пользователей. Это привело к внедрению систем возрастной верификации, но также вызвало критику из-за усложнения регистрации и рисков избыточного контроля. Кроме того, закон ограничивает использование данных в рекламных целях без явного согласия, что изменило подходы к таргетированию в маркетинге.

С развитием технологий возникли новые проблемы. Например, использование нейросетей для анализа больших данных (Big Data) позволяет деанонимизировать пользователей даже при отсутствии прямых идентификаторов. В 2023 году в закон внесены поправки, запрещающие обработку данных с целью создания «цифровых двойников» без согласия субъекта. Также усилились требования к биометрическим системам: компании обязаны хранить такие данные отдельно от другой информации и использовать сертифицированное ПО.

Закон № 152-ФЗ повлиял и на международные отношения. Иностранные компании, работающие в РФ, должны соблюдать правила локализации, что привело к открытию локальных дата-центров такими гигантами, как Apple и SAP. Однако санкционное давление осложнило передачу данных между российскими и зарубежными филиалами, вынуждая бизнес переходить на отечественные облачные решения. Параллельно Роскомнадзор активно блокирует ресурсы, нарушающие требования, включая социальные сети и стриминговые платформы.

Критики закона указывают на избыточность бюрократических процедур. Например, малые предприятия часто не могут позволить себе дорогостоящие системы защиты, что ставит их в неравные условия с крупными игроками. Кроме того, не до конца проработаны механизмы взаимодействия с международными стандартами, такими как GDPR, что создает конфликты юрисдикций. Тем не менее, закон стимулирует развитие отечественных IT-решений: рынок шифрования и VPN-сервисов в России вырос на 40% за последние три года.

Современные тенденции включают интеграцию блокчейна для защиты данных и создание единых государственных реестров. С 2024 года запущен пилотный проект по хранению медицинских данных граждан в распределенных реестрах, что снижает риски взломов. Однако сохра-

няются вопросы к прозрачности таких систем и доступу третьих лиц к информации. Ожидается, что дальнейшее развитие получит регулирование искусственного интеллекта, особенно в контексте автоматизированной обработки персональных данных.

Современное регулирование требует гибкости и межотраслевого подхода. Ключевые направления: гармонизация с международными стандартами и развитие цифровой юриспруденции.

Список литературы:

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 24.04.2024) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

[2] Соловьев, А. К. Киберпреступность в России: эволюция правового регулирования / А. К. Соловьев. — М. : Юстицинформ, 2020. — 198 с.

[3] Родионов, Д. И. Угрозы цифровой эпохи и ответ законодателя / Д. И. Родионов // Законодательство и практика. — 2023. — № 5. — С. 34–40.

[4] Захарова, Е. М. Тенденции киберпреступности: экономический аспект / Е. М. Захарова. — СПб. : Изд-во «Право и технологии», 2019. — 176 с.

[5] Комаров, В. С. Доказывание в делах о компьютерных преступлениях / В. С. Комаров // Уголовный процесс. — 2021. — № 7. — С. 22–28.

[6] Белова, М. А. Персональные данные: риски и защита / М. А. Белова. — М. : Инфра-М, 2022. — 224 с.

[7] Гусев, П. Н. Правовые пробелы в регулировании информационной безопасности / П. Н. Гусев // Цифровое право. — 2020. — № 4. — С. 56–62.

[8] Морозова, Л. В. Международное сотрудничество в борьбе с киберпреступностью / Л. В. Морозова // Международное публичное право. — 2024. — № 1. — С. 89–95.

[9] Крылов, С. О. Статистика и проблемы расследования киберпреступлений / С. О. Крылов // Вопросы криминологии. — 2023. — № 3. — С. 45–51.

[10] Семенов, И. А. Deepfake: вызов для права / И. А. Семенов // Информационные технологии и право. — 2024. — № 2. — С. 18–23.

[11] Федоров, К. Д. Криптовалюты и правоохранительная деятельность / К. Д. Федоров. — М. : Финансы и право, 2023. — 189 с.

References:

[1] The Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ (as amended on 24.04.2024) //Collection of Legislation of the Russian Federation. 1996. № 25. Art. 2954.

[2] Soloviev, A.K. Cybercrime in Russia: the evolution of legal regulation/A.K. Soloviev. - M.: Justicinform, 2020. - 198 s.

[3] Rodionov, D. I. Threats of the digital age and the response of the legislator/D. I. Rodionov//Legislation and practice. — 2023. — № 5. - S. 34-40.

[4] Zakharova, E. M. Trends in cybercrime: economic aspect/E. M. Zakharova. - St. Petersburg: Publishing House “Law and Technology,” 2019. - 176 s.

[5] Komarov, V. S. Evidence in computer crime cases/V. S. Komarov//Criminal trial. — 2021. — № 7. - S. 22-28.

[6] Belova, M. A. Personal data: risks and protection/M. A. Belova. - M.: Infra-M, 2022. - 224 s.

[7] Gusev, P.N. Legal gaps in the regulation of information security/P.N. Gusev//Digital law. — 2020. — № 4. - S. 56-62.

[8] Morozova, L. V. International cooperation in the fight against cybercrime/L. V. Morozova//International public law. — 2024. — № 1. - S. 89-95.

[9] Krylov, S.O. Statistics and problems of cybercrime investigation/S.O. Krylov//Criminology issues. — 2023. — № 3. - S. 45-51.

[10] Semenov, I. A. Deepfake: a challenge for law/I. A. Semenov//Information technology and law. — 2024. — № 2. - S. 18-23.

[11] Fedorov, K. D. Cryptocurrencies and law enforcement/K. D. Fedorov. - M.: Finance and Law, 2023. - 189 s.