



Научная статья

УДК 343.1

<https://doi.org/10.24412/2073-0454-2025-6-200-204>

EDN: <https://elibrary.ru/yfjuza>

НИОН: 2003-0059-6/25-432

MOSURED: 77/27-004-2025-06-631

Цифровая реальность и социальные гарантии: проблемы уголовно-правового обеспечения

Алексей Александрович Ходусов

Международный юридический институт, Москва, Россия, yustas-73@mail.ru

Аннотация. Приводится авторское понимание цифровой реальности и ее использования для защиты прав граждан; представлены угрозы для обеспечения социальных гарантий граждан; указаны отдельные виды преступлений и основные нормативные акты, регулирующие ответственность за них; сформулирован ряд конкретных предложений по совершенствованию механизмов защиты социальных прав в условиях цифровой трансформации.

Ключевые слова: цифровая реальность, права граждан, социальные гарантии, цифровая трансформация, преступления, законодательство, механизм защиты

Для цитирования: Ходусов А. А. Цифровая реальность и социальные гарантии: проблемы уголовно-правового обеспечения // Вестник Московского университета МВД России. 2025. № 6. С. 200–204. <https://doi.org/10.24412/2073-0454-2025-6-200-204>. EDN: YFJUZA.

Original article

Digital reality and social guarantees: problems of criminal law

Alexey A. Khodusov

International Law Institute, Moscow, Russia, yustas-73@mail.ru

Abstract. The author's understanding of digital reality and its use to protect the rights of citizens is provided; threats are presented to ensure social guarantees of citizens; individual types of crimes and basic regulations governing their responsibility are indicated; a number of specific proposals were formulated to improve the mechanisms for protecting social rights in the context of digital transformation.

Keywords: digital reality, citizens' rights, social guarantees, digital transformation, crimes, legislation, protection mechanism

For citation: Khodusov A. A. Digital reality and social guarantees: problems of criminal law. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2025;(6):200–204. (In Russ.). <https://doi.org/10.24412/2073-0454-2025-6-200-204>. EDN: YFJUZA.

В контексте правовой сферы под цифровой реальностью будем понимать алгоритмы, которые самостоятельно улучшают свою эффективность, как правового регулирования, так и правоприменения на основе цифровых данных и вычислительных систем; технологии, позволяющие машинам имитировать когнитивные функции для защиты социальных прав.

Цифровизация обеспечения социальных гарантий открывает новые возможности для оптимизации государственного управления, образования, медицинского и социального обслуживания. Например, внедрение

проектов типа «Цифровой социальный помощник» [2], может улучшить способ оказания государственных и муниципальных социальных услуг. Расширение точек доступа к информации, возможность получения круглосуточной поддержки, упрощение процесса подачи заявок на получение социальных выплат и услуг — все это повышает уровень социальной защиты граждан.

Процесс предоставления государственных услуг в области социальной защиты населения существенно облегчается благодаря новейшим цифровым тех-



нологиям, так как последние создают условия для осуществления удаленного обмена информацией, как частными лицами, так и государственными компаниями. Выполнение тех же самых задач возложено на специально организованные многофункциональные центры, которые занимаются предоставлением услуг в государственной и муниципальной сферах, а именно, осуществляют назначение и использование так называемого принципа «одного окна» для оказания социальной поддержки. Между тем, наряду с возникновением дополнительных возможностей вследствие внедрения и развития информационно-цифровых технологий, имеет место определенный риск для общества в отдельных его членов, поскольку появляется трудность эффективной реализации и охраны свобод и прав личности, которые должны обеспечиваться предпринимательским сообществом и государством, получающими таким образом обширные возможности для проникновения в частную жизнь граждан. Данные обстоятельства обусловлены наличием объективно существующих сложностей процесса реализации ограничения доступа к личным данным третьих лиц, а в частности, тех, кто имеет отношение к деятельности образовательных, медицинских или социальных организаций. Этим обосновывается позиция ряда ученых [1, с. 36], согласно которой каждая отдельно взятая личность, национальные законодатели и компании должны быть нацелены на защиту персональных данных, уделять достаточно внимания данной проблеме.

Преступный мир также не остался в стороне от цифровых технологий. Все чаще средством для достижения разнообразных преступных замыслов становятся мобильные приложения для телефонов, компьютерные программы и вся телекоммуникационная сеть Интернет [11]. Специалисты в области статистики фиксируют наличие положительной динамики данного показателя из года в год. Все изложенное подтверждает необходимость проявления особого внимания со стороны общественности и компетентных экспертов к проблемам обеспечения надлежащего уровня безопасности личных данных лиц, использующих современные технологии, а также охраны частной жизни.

Целью мошенничества, реализуемого с использованием электронных источников социальной инженерии, в большинстве случаев становится незаконное получение права на распоряжение денежными средствами физических и юридических лиц, а также доступа к каким-либо личным данным. Более того, социальные сети стали распространителями терроризма, экстремизма, ненависти на почве национальности, религии и т. д. [10].

К сожалению, традиционные методы правоохранительной деятельности не успевают за технологическим развитием криминальных схем, поэтому уровень раскрываемости цифровых преступлений невысок — в 2024 г. он составил лишь 23 % и продолжает снижаться

[3]. Осознавая остроту проблемы, государство только за последний год приняло ряд масштабных мер, призванных переломить ситуацию. В конце прошлого года распоряжением правительства РФ № 4154-р от 30 декабря 2024 г. утверждена Концепция государственной системы противодействия киберпреступлениям [5].

Она закладывает основу для создания специализированной цифровой платформы по оперативному обмену информацией между правоохранительными органами, Банком России, кредитными организациями и операторами связи. С начала текущего года принят пакет федеральных законов, направленных на защиту прав граждан и противодействие незаконным действиям в цифровой среде. Так, Закон № 9-ФЗ от 13 февраля 2025 г. [6] вводит «период охлаждения» (от четырех до 48 час.) для потребительских кредитов. Он призван удерживать граждан от скоропалительных решений, принятых под психологическим влиянием злоумышленников. Банки же закон обязывает сверяться с базой данных о мошеннических операциях, а также освобождает жертв от обязательств по кредиту, если финансовое учреждение не приняло всех необходимых мер для проверки добровольности получения займа.

Закон № 41-ФЗ от 1 апреля 2025 г. [7] направлен на создание государственной информационной системы (ГИС) для межведомственного взаимодействия. Он содержит важные практические нормы: запрет госорганам и банкам использовать иностранные мессенджеры, верификацию продавцов на маркетплейсах, маркировку звонков от юридических лиц, ограничение на передачу SIM-карт, а также распространяет антифрод-мероприятия на операции через банкоматы.

Закон № 176-ФЗ, принятый 24 июня 2025 г. [8] усиливает ответственность по ст. 187 УК РФ («Незаконные действия с платежными картами»). При этом введены новые составы преступлений, связанные с передачей и использованием электронных средств платежа (ЭСП) в корыстных целях, для борьбы с дропами — лицами, предоставляющими свои карты для обналичивания денег.

Закон № 278-ФЗ от 31 июля 2025 г. [9] дает следователям и дознавателям право внесудебного приостановления операций по счетам на срок до 10 суток, если есть подозрение, что переводимые средства связаны с преступлением. Это важная мера для быстрой блокировки и сохранения похищенных денег до вынесения судебного решения.

Тем не менее, по-прежнему существуют следующие риски системного характера, оказывающие свое воздействие на практику предупреждения преступности и имеющие отношение к сфере цифровизации.

1. Легкость совершения преступлений. Нет необходимости обладания специальными познаниями для осуществления таких действий, как шантаж или хищение информации. В большинстве случаев для



реализации данных целей преступнику достаточно кликнуть компьютерной мышкой несколько раз.

2. Легкость сокрытия следов преступлений. Цифровые преступления практически невидимы, у большинства населения и даже у правоохранителей нет эффективного способа для обнаружения преступников.

3. Отсутствие корпоративного (профессионального) осуждения. Резко негативные отклики со стороны профессиональных кругов и интернет сообществ поступают исключительно в отношении вопиющих случаев пренебрежения нормами морали и закона (к примеру, порнографические ролики с участием несовершеннолетних).

Принятые в 2024–2025 гг. законы и другие нормативные акты — значительный шаг вперед в построении системы противодействия кибермошенничеству. Они носят комплексный характер: затрагивают профилактические и технические аспекты, ужесточают ответственность. Однако, для полноценной защиты прав граждан необходимо принятие дополнительных мер: а) опережающее правовое регулирование; б) усиление международного сотрудничества в области экстрадиции и правовой помощи по киберпреступлениям, невзирая на политическую обстановку; в) создание учебных программ для подготовки киберследователей, оснащение правоохранительных органов современными инструментами цифровой криминалистики и аналитики; г) внедрение упрощенных процедур взыскания ущерба с банков и виновных лиц в пользу потерпевших, формирование единообразной судебной практики по вопросам признания недействительными кредитных договоров, заключенных обманным путем; д) масштабная образовательная и просветительская кампания, проводимая на постоянной основе и с охватом всех групп населения.

Только такой многоуровневый подход, сочетающий жесткое законодательство с техническими возможностями, международную кооперацию и просвещение граждан, сможет обеспечить должную защиту прав человека в цифровой среде.

Что касается уголовно-правового обеспечения защиты социальных прав, то система предупреждения преступности в самых разнообразных областях, будь то семья и несовершеннолетние, здравоохранение, социальное обеспечение или трудовые взаимоотношения, совершенствуется благодаря цифровизации. Возможности, предоставляемые современными технологиями, позволяют существенно увеличивать эффективность профилактических мер, выявлять потенциальные риски и своевременно откликаться на возникающие угрозы.

Одной из принимаемых в данной связи мер, может стать создание единой системы социальной поддержки, где отдельные услуги будут предоставляться автоматически. Таким образом, возникнет возмож-

ность получения от других платформ сведений относительно изменений в жизненных условиях человека, а также обеспечения согласованности деятельности по предоставлению мер поддержки на региональном и федеральном уровнях. Также для полноценной защиты прав граждан необходимо принятие дополнительных мер, среди которых: опережающее правовое регулирование, усиление международного сотрудничества в области экстрадиции и правовой помощи по киберпреступлениям, создание учебных программ для подготовки киберследователей, оснащение правоохранительных органов современными инструментами цифровой криминалистики и аналитики.

В рамках системы опережающего правового регулирования необходимо на постоянной основе осуществлять контроль над технологическими трендами оперативно вносить изменения в нормы законодательства таким образом, чтобы сохранялось определенное соответствие актуальным угрозам. Необходимо разрабатывать законы, которые не только криминализируют новые виды киберпреступлений, но и определяют ответственность поставщиков услуг, платформ и разработчиков программного обеспечения за соблюдение безопасности своих продуктов. Параллельно с этим, также необходимо соблюдать правила защиты личных данных.

В целях выявления преступников в сети интернет, крайне важно создать эффективные инструменты, посредством которых, сотрудники правоохранительных органов, смогут вести активное противостояние подобной преступной деятельности. Также важно внедрять самое современное ПО, которое позволит посредством разнообразного функционала, реализовывать профилактику киберпреступности, оперативно реагировать на любые риски безопасности пользователей.

Итак, представленные рассуждения позволяют сформулировать ряд конкретных предложений по совершенствованию механизмов защиты социальных прав в условиях цифровой трансформации.

1. На основании совершенствования системы уголовно-правовой защиты социальных прав, можно предложить ее дополнение новым структурным элементом в Уголовном кодексе — «Кибернетической (цифровой) составляющей». Данный блок должен аккумулировать нормы, направленные против злоупотреблений в сфере использования цифровых технологий, что позволит системно противостоять таким угрозам, как алгоритмическая дискриминация, манипулятивное воздействие на граждан с использованием цифровых технологий, мошенничество в новой (цифровой) форме.

2. Для применения цифровых технологий по защите социальных прав, можно предложить следующее:

- внедрение на государственном уровне проактивных систем мониторинга, основанных на анализе больших данных, для ключевых социальных сфер;



- закрепление на законодательном уровне обязанности контролирующих органов использовать технологии Big Data и Predictive Analytics для проведения риск-ориентированного надзора за соблюдением трудового, экологического и социального законодательства;
 - создание государственной платформы для анализа спутниковых данных и данных IoT-датчиков в целях обеспечения права на благоприятную окружающую среду, с предоставлением доступа к ней правоохранительных и надзорных органов.
3. Принимая во внимание новые угрозы социальным правам, связанным с ИИ и Big Data, можно предложить следующее:
- разработать и принять отраслевые этические кодексы и стандарты по использованию алгоритмов ИИ в социальной сфере;
 - установить законодательную обязанность для государственных и частных организаций, использующих алгоритмы ИИ для принятия решений, затрагивающих социальные права граждан.
4. В качестве вариантов совершенствования УК РФ можно предложить:
- 4.1. Введение новых статей:
- 159.1 «Мошенничество с использованием искусственного интеллекта и иных передовых цифровых технологий» (для специфических способов обмана, не полностью охватываемых текущей редакцией ст. 159 УК РФ);
 - 136.1 «Нарушение равенства прав и свобод человека и гражданина, совершенное с использованием алгоритмических систем» (для целевого противодействия алгоритмической дискриминации).
- 4.2. Дополнение примечаний к статьям:
- 159 УК РФ «Мошенничество» добавить примечание, разъясняющее, что «Под обманом в настоящей статье понимается также умышленное введение в заблуждение с использованием информационно-телекоммуникационных сетей, включая применение технологий искусственного интеллекта для имитации голоса, изображения или создания иных ложных цифровых представлений, направленных на выдачу себя за представителя власти, банка или иной организации»;
 - 140 УК РФ «Отказ в предоставлении гражданину информации» добавить положение о том, что «Отказ, произведенный алгоритмической системой на основании дискриминационных признаков (пол, раса, возраст, место жительства, доход и т. д.), приравнивается к отказу, совершенному должностным лицом».
- Реализация предложенных мер позволит заложить

основы для опережающего правового регулирования, обеспечивающего эффективную защиту социальных прав граждан.

Список источников

1. Вахрамеева Л. Н. Конституционно-правовой механизм охраны и защиты абсолютных прав и свобод человека и гражданина в Российской Федерации : автореф. дис. ...канд. юрид. наук. М., 2021.
2. Игнатова Т. В. и др. Инновационные технологии в государственном управлении: цифровизация процессов и их эффективность // Государственное и муниципальное управление. Ученые записки. 2024. № 3. С. 23–29.
3. Как защитить права человека в цифровой среде? // URL: <https://rg.ru/2025/10/30/reg-urfo>
4. Николаев В. А. Защита прав и свобод человека конституциями, уставами субъектов Российской Федерации : автореф. дис. ...канд. юрид. наук. Челябинск. 2023.
5. Распоряжение Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» // URL: <https://www.garant.ru/products/ipo/prime/doc/41152413>
6. Федеральный закон от 13 февраля 2025 г. № 9-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // URL: <https://www.garant.ru/products/ipo/prime/doc/41138>
7. Федеральный закон от 1 апреля 2025 г. № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» // URL: <http://www.kremlin.ru/acts/bank/51783>
8. Федеральный закон от 24 июня 2025 г. № 176-ФЗ «О внесении изменений в статью 187 Уголовного кодекса Российской Федерации» // URL: <https://rg.ru/documents/2025/06/27/fz176-dok.html?ysclid=miiyr5lynd37028777>
9. Федеральный закон от 31 июля 2025 г. № 278-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // URL: <http://www.kremlin.ru/acts/bank/52260>
10. Шалагин А. Е., Идиятуллов А. Д. Трансформация преступности в XXI веке: особенности предупреждения и противодействия // Вестник Казанского юридического



института МВД России. 2021. Т. 12. № 2 (44). С. 227–235.

11. Ходусов А. А. Цифровизация в криминалистике : современные вызовы // Информационные технологии в деятельности органов внутренних дел. Сборник научных трудов Международной научно-практической конференции. 2024. С. 297–302.

References

1. Vakhrameeva L. N. The constitutional and legal mechanism of protection and protection of the absolute rights and freedoms of man and citizen in the Russian Federation : abstract of the dissertation of the cand. legal sciences. M., 2021.
2. Ignatova T. V. et al. Innovative technologies in public administration: digitalization of processes and their effectiveness // State and Municipal Administration. Scientific notes. 2024. № 3. P. 23–29.
3. How to protect human rights in the digital environment? // URL: <https://rg.ru/2025/10/30/reg-urfo>
4. Nikolaev V. A. Protection of human rights and freedoms by constitutions, charters of subjects of the Russian Federation : abstract of the dissertation of the cand. legal sciences. Chelyabinsk, 2023.
5. Decree of the Government of the Russian Federation dated December 30, 2024 № 4154-р «On approval of the Concept of the state system for countering unlawful acts committed using information and communication technologies» //

URL: <https://www.garant.ru/products/ipo/prime/doc/411152413>

6. Federal Law № 9-FZ of February 13, 2025 «On amendments to certain legislative acts of the Russian Federation» // URL: <https://www.garant.ru/products/ipo/prime/doc/41138>
7. Federal Law № 41-FZ of April 01, 2025 «On the creation of a state information system for countering offenses committed using information and communication technologies and on amendments to certain legislative acts of the Russian Federation» // URL: <http://www.kremlin.ru/acts/bank/51783>
8. Federal Law № 176-FZ of June 24, 2025 «On amendments to Article 187 of the Criminal Code of the Russian Federation» // URL: <https://rg.ru/documents/2025/06/27/fz176-dok.html?ysclid=miiyr5lynd37028777>
9. Federal Law № 278-FZ of July 31, 2025 «On amendments to the Code of Criminal Procedure of the Russian Federation» // URL: <http://www.kremlin.ru/acts/bank/52260>
10. Shalagin A. E., Idiyatullova A. D. Transformation of crime in the 21st century: features of prevention and counteraction // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2021. Vol. 12. № 2 (44). P. 227-235.
11. Khodusov A. A. Digitalization in criminalistics : modern challenges // Information technologies in the activities of law enforcement agencies. Collection of scientific papers of the International Scientific and Practical Conference. 2024. P. 297–302.

Информация об авторе

А. А. Ходусов — заведующий кафедрой уголовно-правовых дисциплин Международного юридического института, кандидат юридических наук, доцент.

Information about the author

A. A. Khodusov — Head of the Department of Criminal Law Disciplines of the International Law Institute, Candidate of Legal Sciences, Associate Professor.

Статья поступила в редакцию 20.11.2025; одобрена после рецензирования 01.12.2025; принята к публикации 12.12.2025.

The article was submitted 20.11.2025; approved after reviewing 01.12.2025; accepted for publication 12.12.2025.