Алиева Диана Наримановна
Дагестанский государственный педагогический университет
им. Р. Гамзатова

ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ДАННЫХ В ЭПОХУ ЦИФРОВИЗАЦИИ

Аннотация. В данной статье рассматриваются актуальные вопросы защиты персональных данных в условиях цифровой трансформации и влияния новых технологий на конфиденциальность и безопасность информации. Подчеркивается важность защиты персональных данных на фоне быстрого развития технологий, таких как искусственный интеллект и большие данные. Упоминается необходимость нахождения баланса между инновациями и правами граждан. В целом, статья акцентирует внимание на необходимости адаптации законодательства к новым технологическим реалиям для обеспечения эффективной защиты персональных данных граждан.

Ключевые слова: Персональные данные, цифровая трансформация, искусственный интеллект, конфиденциальность, безопасность информации, законодательство, несанкционированный сбор данных, прозрачность алгоритмов, ответственность за нарушения.

Технологии искусственного интеллекта создают новые вызовы для конфиденциальности персональных данных за счет масштабной автоматизированной обработки информации. Алгоритмы машинного обучения способны анализировать огромные массивы данных, выявляя скрытые закономерности и формируя прогнозы поведения субъектов. Это приводит к формированию цифровых профилей, содержащих не только явные, но и предполагаемые характеристики личности. Подобные практики создают риски неправомерного использования сведений без осознанного согласия субъектов. Прогнозирующие возможности ИИ ставят под вопрос традиционные подходы к защите данных, основанные на принципах изначальной определенности целей обработки [9, с. 48]. Автоматизированное принятие решений на основе анализа поведения может приводить к дискриминационным последствиям и нарушению автономии воли. Этические и правовые проблемы усугубляются отсутствием прозрачности алгоритмов, что затрудняет реализацию права субъекта на объяснение принятых в отношении него решений.

Анализ российской судебной практики выявляет системные нарушения законодательства о защите персональных данных, преимущественно связанные с несанкционированным сбором и обработкой информации. Типичными случаями остаются недостаточные меры технической защиты баз данных, приводящие к утечкам, а также несоблюдение требований о получении согласия субъектов на обработку их сведений [1, ст. 9, 18.1]. Отдельную категорию составляют нарушения при трансграничной передаче данных без предварительной локализации на территории РФ. Судебные решения демонстрируют, что операторы персональных данных нередко игнорируют требования Федерального закона № 152-ФЗ относительно уведомления регулятора о начале обработки информации [7].

Применяемые санкции за нарушения в сфере защиты персональных данных варьируются от административных штрафов по ст. 13.11 КоАП РФ [3] до уголовной ответственности по ст. 137 УК РФ [2]. Анализ практики Роскомнадзора показывает преобладание штрафных мер в отношении юридических лиц, размер которых может достигать 6 млн рублей за систематические нарушения. В случаях, повлекших существенный вред правам граждан, суды применяют дисквалификацию должностных лиц и приостановление деятельности организаций [5]. Отмечается тенденция к ужесточению ответственности за повторные нарушения, что отражает повышенное внимание законодателя к вопросам цифровой безопасности.

Стремительное развитие технологий искусственного интеллекта, интернета вещей и биометрических систем выявило неполноту регулирования в Федеральном законе № 152-ФЗ [1]. Действующие нормы не учитывают специфику автоматизированной обработки данных нейросетями и особенности сбора информации датчиками IoT [9, с. 52]. Отсутствие чётких требований к использованию биометрических идентификаторов создаёт риски несанкционированного доступа к чувствительной информации. Данные правовые пробелы затрудняют обеспечение конфиденциальности в условиях технологической трансформации.

Существующие механизмы контроля за соблюдением законодательства о персональных данных демонстрируют низкую эффективность. «Отсутствуют механизмы контроля за тем, какие способы защиты ПД используют операторы, кредитные организации и иные лица, кто обрабатывает ПД и насколько они эффективны» [8, с. 109]. Сложность доказывания фактов нарушений и недостаточная прозрачность проверок снижают действенность надзорных процедур. Применяемые меры административной ответственности не всегда соответствуют тяжести правонарушений, что не создаёт достаточных стимулов для добросовестного исполнения требований закона.

Несогласованность российского законодательства с положениями Общего регламента по защите данных ЕС (GDPR) создаёт сложности при трансграничной передаче информации [6]. Различия в подходах к получению согласия субъектов данных, определению правовых оснований обработки и реализации прав на переносимость данных осложняют взаимодействие с международными партнёрами. Отсутствие механизмов взаимного признания адекватности уровня защиты требует от компаний разработки дополнительных правовых и технических решений. Данная ситуация увеличивает операционные издержки бизнеса и снижает конкурентоспособность российских субъектов данных на глобальном рынке.

Внедрение принципа «подвижного целеполагания» представляет собой стратегический подход к регулированию перспективных технологий, таких как искусственный интеллект и интернет вещей. Данный принцип предполагает создание адаптивных правовых механизмов, способных эволюционировать параллельно с технологическим развитием. Его реализация требует разработки гибких нормативных рамок, предусматривающих регулярный пересмотр требований в соответствии с динамикой цифровой среды [10, с. 30]. Такой подход позволит минимизировать правовые лакуны при появлении инновационных решений. Практическое применение принципа «подвижного целеполагания» может быть реализовано через внедрение экспериментальных правовых режимов и регуляторных «песочниц». Эти механизмы обеспечат тестирование нормативных нововведений в контролируемых условиях перед их масштабированием. Особое значение приобретает создание системы мониторинга технологических трендов для прогнозирования регуляторных потребностей. Подобные меры способствуют формированию проактивной, а не реактивной правовой политики в сфере защиты данных.

Гармонизация российского законодательства с международными стандартами требует расширения прав субъектов персональных данных. «Параллельно с развитием международных стандартов происходило формирование региональных систем защиты персональных данных, наиболее развитой из которых стало европейское регулирование. Директива 95/46/ЕС заложила основы гармонизации национальных законодательств стран ЕС, а принятый в 2016 году Общий регламент по защите данных (GDPR) создал единое правовое пространство в этой сфере» [6, преамбула, ст. 1]. GDPR детализировал и усилил принципы защиты данных, а также ввел новые права для субъектов данных (такие как право на переносимость данных и «право на забвение»), установил строгие требования к трансграничным передачам и ввел значительные штрафные санкции за нарушения установленных правил. Введение аналогичных прав в российское законодательство повысит уровень защиты граждан и упростит трансграничное взаимодействие.

Создание отдельного регуляторного режима для больших данных и алгоритмических систем должно основываться на риск-ориентированном подходе. Это предполагает дифференциацию правовых требований в зависимости от потенциального вреда обработки

данных и масштабов их использования [8, с. 111]. Режим должен устанавливать специальные правила для систем, применяющих технологии машинного обучения и автоматизированного принятия решений. Ключевым аспектом становится введение обязательной оценки воздействия на защиту данных для высокорисковых проектов.

Проведённое исследование выявило значительный разрыв между динамично развивающимися технологиями обработки данных, включая искусственный интеллект и большие массивы информации, и существующими правовыми механизмами их регулирования. Анализ трансграничных утечек персональных данных и систематических нарушений конфиденциальности подтвердил неспособность текущих нормативных рамок адекватно реагировать на технологические вызовы. Это несоответствие создаёт правовые риски как для граждан, чьи права остаются недостаточно защищёнными, так и для бизнеса, сталкивающегося с неоднозначностью регуляторных требований.

Разработанные рекомендации по модернизации Федерального закона № 152-ФЗ включают внедрение риск-ориентированного подхода к регулированию, предполагающего дифференциацию требований в зависимости от масштаба и характера обработки данных. Предлагается создать механизмы превентивного контроля за алгоритмами искусственного интеллекта и усилить санкции за нарушения в сфере больших данных [9, с. 57]. Эти меры направлены на повышение адаптивности правовой системы к технологическим изменениям и обеспечение её соответствия вызовам цифровой эпохи.

Реализация предложенных мер обеспечит устойчивый баланс между интересами цифровой экономики и фундаментальными правами личности. С одной стороны, бизнес получит более чёткие регуляторные ориентиры, снижающие правовые риски, с другой – граждане смогут рассчитывать на повышенный уровень защиты своих персональных данных. Прогнозируемый социально-экономический эффект включает укрепление доверия к цифровым сервисам и создание условий для ответственного технологического развития в рамках правового поля

Список литературы:

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 30.11.2024) [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс». (Дата обращения: 05.04.2026).

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 30.11.2024) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954. (Ст. 137 «Нарушение неприкосновенности частной жизни»).

3. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 30.11.2024) // Собрание законодательства РФ. – 07.01.2002. – № 1 (ч. 1). – Ст. 1. (Ст. 13.11 «Нарушение законодательства Российской Федерации в области персональных данных»).

4. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства РФ. – 05.11.2012. – № 45. – Ст. 6257.

5. Постановление Правительства РФ от 13.02.2019 № 146 «Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных» // Собрание законодательства РФ. – 25.02.2019. – № 8. – Ст. 790.

6. Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27.04.2016 о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (Общий Регламент о защите персональных данных – GDPR) // Официальный журнал Европейского Союза. – L 119. – 04.05.2016.

7. Постановление Верховного Суда РФ от 09.02.2026 № 5-АД25-119-К2 по делу о привлечении Минтруда России к ответственности за утечку персональных данных [Электронный ресурс]. – Доступ из справ.-правовой системы «ПРАВО.Ru». (Дата обращения: 05.04.2026).

8. Исакова, Ю. И. Правовые аспекты оборота больших данных (Big Data) в эпоху цифровизации / Ю. И. Исакова // Юристъ-Правоведъ. – 2020. – № 2 (93). – С. 107–112.

9. Савельев, А. И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) / А. И. Савельев // Закон. – 2015. – № 1. – С. 43–59.

10. Терещенко, Л. К. Правовой режим информации в условиях цифровой экономики / Л. К. Терещенко // Журнал российского права. – 2020. – № 1. – С. 25–36