

Сармандеева Кира Дмитриевна

студентка

Иванова Юлия Ильсуровна

студентка

Научный руководитель

Кузнецова Надежда Ильинична

канд. пед. наук, доцент

ФГБОУ ВО «Ульяновский государственный
педагогический университет им. И.Н. Ульянова»

г. Ульяновск, Ульяновская область

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

***Аннотация:** в статье исследуются правовые проблемы защиты персональных данных в условиях цифровизации общества. Рассматриваются конституционные и отраслевые основы правового режима персональных данных, анализируются принципы их обработки, закрепленные в российском законодательстве, а также изменения, вызванные распространением платформенных сервисов, технологий Big Data, цифрового профилирования и биометрической идентификации.*

***Ключевые слова:** персональные данные, цифровизация, защита информации, Big Data, цифровой профиль.*

Цифровизация общества привела к расширению сфер, в которых персональные данные выступают обязательным элементом правового и экономического оборота. Банковские сервисы, маркетплейсы, социальные сети, государственные информационные системы, дистанционные образовательные платформы, медицинские сервисы и кадровые системы используют сведения о человеке не только для идентификации, но и для автоматизированной оценки, маршрутизации обращений, прогнозирования поведения и персонализации взаимодействия. Персональные данные приобрели значение ресурса, на основе которого формируются

управленческие, коммерческие и технологические решения. По этой причине их защита рассматривается как элемент правового обеспечения автономии личности в цифровой среде. Нормативная основа такого подхода закреплена в статьях 23 и 24 Конституции Российской Федерации, которые гарантируют неприкосновенность частной жизни и запрещают сбор, хранение, использование и распространение информации о частной жизни лица без его согласия [3]. Федеральный закон №152-ФЗ определяет персональные данные как любую информацию, относящуюся прямо или косвенно к определенному или определяемому физическому лицу [6], а Федеральный закон №149-ФЗ задает общую рамку регулирования отношений, возникающих при применении информационных технологий и обеспечении защиты информации [7].

А. К Жарова, В. М. Елин обосновали, что понятия персональных данных и частной жизни в российском праве формировались во взаимосвязи, а правовой режим таких сведений следует рассматривать через более широкий институт охраны личной сферы [2, с. 69–70]. В цифровой среде личность устанавливается не только по имени, номеру документа или адресу, но и по совокупности косвенных признаков: истории действий пользователя, геолокации, транзакционным данным, параметрам устройства, визуальным и биометрическим характеристикам. Персональные данные представляют интерес для права не сами по себе, а как информационная основа принятия решений, влияющих на частную и публичную сферу жизни субъекта.

Российская модель защиты персональных данных строится на принципах законности, справедливости, целевого ограничения и минимизации обработки. Закон №152-ФЗ требует, чтобы содержание и объем обрабатываемых данных соответствовали заявленным целям обработки и не были избыточными по отношению к ним [6]. Принцип минимизации персональных данных исключает сбор сведений, не обусловленных конкретной целью обработки. Оператор вправе обрабатывать только тот объем информации, который необходим для исполнения установленной законом, договором или иной юридически значимой задачей. В

цифровой среде избыточный сбор данных повышает риск утечек, неправомерного доступа, последующей передачи третьим лицам и использования сведений за пределами первоначально заявленной цели. Роскомнадзор в рекомендациях от 8 августа 2023 г. указывает на необходимость сокращать объем собираемых данных до необходимого минимума, исключать их накопление без практической необходимости, разграничивать доступ работников к информационным массивам и закреплять ответственность за организацию обработки персональных данных [10].

Цифровая экономика создает устойчивое противоречие между законодательным требованием ограниченной обработки и технологической логикой накопления данных. Платформенные модели бизнеса ориентированы на сбор максимально полного массива сведений, поскольку их экономическая ценность раскрывается не в момент первичного получения, а на стадии последующей аналитики. В.И. Солдатова писала, что распространение цифровых технологий усилило значение персональных данных как условия функционирования сервисов и одновременно обнажило уязвимость правовых механизмов, рассчитанных на более простые модели обработки [12, с. 34–36]. Современная цифровая инфраструктура предполагает участие нескольких операторов и технических посредников в процессе обработки персональных данных. Один и тот же массив сведений может передаваться банкам, цифровым платформам, подрядным организациям, облачным сервисам и государственным информационным системам. В такой модели согласие субъекта персональных данных сохраняет значение правового основания обработки, однако не обеспечивает полноценного контроля со стороны лица, поскольку субъект не располагает исчерпывающей информацией о составе участников обработки, объеме передаваемых данных и последующих целях их использования.

Распространение технологий Big Data изменило подход к правовому регулированию персональных данных. А. И. Савельев обосновал, что ценность таких данных определяется не отдельным идентификатором, а результатом сопоставления и агрегирования различных массивов сведений [11, с. 45–47]. В цифровой

среде информация приобретает персонализирующий характер в сочетании с другими данными. Формально обезличенные сведения могут позволить идентифицировать лицо после объединения с геолокацией, историей операций, параметрами устройства и поведенческими характеристиками. Правовая оценка обработки персональных данных должна охватывать весь цикл обращения информации: сбор, систематизацию, передачу, объединение, обезличивание, повторную идентификацию, хранение и уничтожение. Правовая защита в этой сфере включает не только обеспечение конфиденциальности, но и ограничение аналитического использования сведений о человеке.

А.Н. Мочалов писал, что цифровой профиль создает риски для конституционных прав человека, поскольку объединение разнородных сведений в единую систему повышает вероятность принятия решений на основе неполной, недостоверной или непрозрачной информации [5, с. 90–92]. Цифровой профиль представляет собой обработанный массив данных, способный влиять на правовое положение человека. Ошибки в таком массиве могут отражаться на кредитной оценке, доступе к сервисам и иных юридически значимых решениях. Риск связан не только с утечкой сведений, но и с использованием личной информации для скрытой классификации субъекта.

Биометрические персональные данные требуют специального правового регулирования, поскольку используются для идентификации личности и связаны с устойчивыми характеристиками человека. М.С Кривогин. отметил, что их выделение в самостоятельную категорию обусловлено целями обработки и последствиями неправомерного использования [4, с. 82–84]. Специальный режим таких данных закреплен в Федеральном законе №572-ФЗ [9]. И.М.Рассолов, С.Г. Чубукова и И.В. Микурова обозначили, что биометрические данные требуют особого правового подхода, поскольку затрагивают фундаментальные интересы личности [1, с. 110–112]. Это предполагает более строгие требования к основаниям обработки, объему собираемых сведений, срокам хранения и контролю доступа.

Современное регулирование защиты персональных данных ориентировано на управление инцидентами. Роскомнадзор предусматривает обязанность уведомления о неправомерной или случайной передаче, предоставлении, распространении либо доступе к персональным данным, повлекших нарушение прав субъектов, а также направление сведений о результатах внутреннего расследования в течение 72 часов [13].

Доктрина информационной безопасности Российской Федерации относит защищенность информационной сферы к числу условий обеспечения национальной безопасности [8]. По этой причине защита персональных данных имеет двойственную правовую природу. Она направлена на охрану частной жизни конкретного человека и одновременно затрагивает публичные интересы, поскольку массовые утечки, незаконный оборот клиентских баз, атаки на цифровую инфраструктуру и системное недоверие к электронным сервисам влияют на устойчивость государственного и коммерческого управления [8]. Межотраслевой характер рассматриваемого института проявляется в сочетании конституционных гарантий, норм информационного и административного права, процедурного контроля, организационных обязанностей оператора и технических мер защиты. Эффективность регулирования зависит не от количества специальных норм, а от того, в какой степени право способно ограничить избыточный информационный контроль над человеком.

Цифровизация изменила правовой режим персональных данных, расширив не только объем их обработки, но и круг связанных с ней рисков. Нарушение прав субъекта связано сегодня не только с разглашением сведений, но и с профилированием, повторной идентификацией, алгоритмической обработкой и иными формами использования данных вне прозрачного контроля со стороны лица. Базовые принципы российского законодательства – законность, целевое ограничение и минимизация обработки – сохраняют основополагающее значение, однако в условиях платформенной экономики требуют более строгого применения. Развитие регулирования биометрических данных и процедур уведомления об инцидентах показывает переход к более дифференцированной и риск-ориентированной

модели правовой защиты. Защита персональных данных в цифровом обществе представляет собой не только средство охраны частной жизни, но и механизм ограничения информационного контроля над личностью.

Список литературы

1. Биометрия в контексте персональных данных и генетической информации: правовые проблемы / И.М. Рассолов, С.Г. Чубукова, И.В. Микурова // Lex Russica. – 2019. – №1. – С. 108–118. DOI 10.17803/1729-5920.2019.146.1.108-118. EDN YVPCZF

2. Жарова А.К. Источники понятий «персональные данные» и частная жизнь лица в российском праве / А.К. Жарова, В.М. Елин // Вестник Академии права и управления. – 2017. – №1 (64). – С. 69–78. EDN YIEDPZ

3. Конституция Российской Федерации: принята всенародным голосованием 12 дек. 1993 г. (с учетом поправок, внесенных законами о поправках к Конституции Российской Федерации, в т. ч. Законом от 14 марта 2020 г. №1-ФКЗ, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // Собрание законодательства Российской Федерации. – 2020. – №31 (ч. I). – Ст. 5054.

4. Кривогин М.С. Особенности правового регулирования биометрических персональных данных / М.С. Кривогин // Право. Журнал Высшей школы экономики. – 2017. – №2. – С. 80–89. DOI 10.17323/2072-8166.2017.2.80.89. EDN ZFCIZT

5. Мочалов А.Н. Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности / А.Н. Мочалов // Lex Russica. – 2021. – Т. 74. №9. – С. 88–101. DOI 10.17803/1729-5920.2021.178.9.088-101. EDN QFEDZO

6. О персональных данных: федер. закон от 27 июля 2006 г. №152-ФЗ.

7. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. №149-ФЗ.

8. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 дек. 2016 г. №646.

9. Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации: федеральный закон от 29 дек. 2022 г. № 572-ФЗ // Собрание законодательства РФ. – 2023. – №1 (ч. I). – Ст. 1.

10. Рекомендации Роскомнадзора операторам персональных данных по реализации положений Федерального закона от 29.12.2022 №572-ФЗ. – URL: <https://pd.rkn.gov.ru> (дата обращения: 08.04.2026).

11. Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) / А.И. Савельев // Право. Журнал Высшей школы экономики. – 2015. – №1. – С. 43–66. EDN WYYJPP

12. Солдатова В.И. Защита персональных данных в условиях применения цифровых технологий / В.И. Солдатова // Lex Russica. – 2020. – Т. 73. №2. – С. 33–43. DOI 10.17803/1729-5920.2020.159.2.033-043. EDN XGEKFD

13. Уведомление о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных. – URL: <https://pd.rkn.gov.ru/incidents/form/> (дата обращения: 08.04.2026).