УДК 34

Демчук А.Р.

магистрант

Институт безопасности жизнедеятельности

Санкт-Петербургский университет ГПС МЧС России

им. героя РФ генерала армии Е.Н. Зиничева

(г. Санкт-Петербург, Россия)

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

Аннотация: *в статье исследуются правовые основы защиты персональных данных в Российской Федерации в условиях цифровизации общественных отношений. Рассматриваются конституционные гарантии права на неприкосновенность частной жизни, положения Федерального закона «О персональных данных», правовой статус оператора и субъекта персональных данных, условия законной обработки, обязанности по обеспечению безопасности и уведомлению об инцидентах. Выявляются проблемы правоприменения, связанные с массовым сбором сведений, использованием цифровых платформ, передачей данных третьим лицам и недостаточной осведомленностью граждан. Обосновывается необходимость риск-ориентированного подхода, повышения прозрачности обработки и совершенствования организационных мер защиты.*

Ключевые слова: *персональные данные, защита, цифровизация, оператор, субъект, согласие, конфиденциальность, информационная безопасность.*

Введение.

Цифровизация общества сопровождается повсеместным использованием информационных технологий при оказании государственных и муниципальных услуг, осуществлении банковских операций, трудоустройстве, обучении, медицинском обслуживании, электронной торговле и повседневном общении. Для предоставления таких услуг организации собирают и обрабатывают значительные массивы сведений о физических лицах. Персональные данные

становятся важным ресурсом цифровой экономики, позволяющим идентифицировать пользователя, учитывать его запросы и обеспечивать персонализированное взаимодействие.

Одновременно расширение обработки информации повышает вероятность нарушения прав граждан. Сведения могут использоваться для целей, не соответствующих первоначально заявленным, передаваться неопределенному кругу лиц, храниться дольше необходимого либо становиться доступными вследствие технических ошибок и компьютерных атак. Последствия неправомерной обработки не ограничиваются формальной утечкой информации: они могут выражаться в мошенничестве, дискриминации, вмешательстве в частную жизнь и причинении имущественного или морального вреда.

В этой связи защита персональных данных приобретает значение одного из ключевых направлений правового обеспечения цифровой трансформации. Ее задача заключается не в запрете обработки информации как таковой, а в установлении правомерных целей, пределов и условий такой обработки, закреплении обязанностей операторов и обеспечении эффективных способов защиты прав граждан. Цель настоящей статьи состоит в анализе действующего правового регулирования защиты персональных данных в Российской Федерации и определении проблем, требующих дальнейшего совершенствования.

1. Конституционные и законодательные основы защиты персональных данных.

Правовая охрана персональных данных основывается прежде всего на конституционных гарантиях. Статья 23 Конституции Российской Федерации закрепляет право каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту чести и доброго имени, а также тайну переписки, телефонных переговоров и иных сообщений. В соответствии со статьей 24 не допускаются сбор, хранение, использование и распространение информации о частной жизни лица без его согласия, если иное не предусмотрено законом. Эти

положения формируют конституционную основу для ограничения произвольного вмешательства в частную сферу человека.

Центральным нормативным актом является Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [1]. Он регулирует отношения, связанные с обработкой персональных данных государственными органами, органами местного самоуправления, юридическими и физическими лицами. Закон устанавливает основные понятия, принципы и условия обработки, права субъектов, обязанности операторов, требования к безопасности и порядок государственного контроля.

Общие положения данного регулирования дополняются Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [2]. Он закрепляет общие правила обращения информации и обязанности по ее защите. В совокупности два федеральных закона образуют основу регулирования: Закон № 149-ФЗ определяет общие рамки информационных отношений, а Закон № 152-ФЗ устанавливает специальный режим обработки сведений, относящихся к определенному или определяемому физическому лицу.

Важное значение имеет Федеральный закон от 21 июля 2014 г. № 242-ФЗ, которым были внесены изменения, направленные, в частности, на обеспечение при сборе персональных данных граждан Российской Федерации использования баз данных, находящихся на территории России, с учетом предусмотренных законом исключений [3]. Требования о локализации обработки стали существенным элементом регулирования деятельности цифровых платформ и иностранных сервисов, взаимодействующих с российскими пользователями.

Нормативную систему также составляют подзаконные акты, устанавливающие требования к защите персональных данных при их обработке в информационных системах. В частности, постановление Правительства РФ от 1 ноября 2012 г. № 1119 определяет требования к защите персональных данных при обработке в информационных системах [4]. Нормативные документы уполномоченных органов конкретизируют организационные и технические

меры, применяемые с учетом угроз безопасности и категории обрабатываемых сведений.

Таким образом, правовое регулирование защиты персональных данных имеет комплексный характер. Оно объединяет конституционные гарантии, специальные федеральные законы и подзаконные требования, обеспечивающие практическую реализацию установленных законом принципов.

2. Принципы и условия законной обработки персональных данных.

В соответствии с Федеральным законом № 152-ФЗ персональные данные определяются как любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу. К таким сведениям в зависимости от контекста могут относиться фамилия, имя, дата рождения, адрес, номер телефона, сведения о месте работы, идентификаторы учетных записей, данные о местоположении и иная информация, позволяющая установить личность человека.

Законность обработки обеспечивается соблюдением принципов, закрепленных в статье 5 Закона № 152-ФЗ. Обработка должна осуществляться на законной и справедливой основе, ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка данных, несовместимая с целями их сбора, а также объединение баз данных, обработка которых осуществляется в целях, несовместимых между собой. Содержание и объем обрабатываемых сведений должны соответствовать заявленным целям и не быть избыточными.

Одним из наиболее известных оснований обработки является согласие субъекта персональных данных. Однако согласие не выступает универсальным условием для любой обработки. Статья 6 Закона № 152-ФЗ предусматривает и другие правовые основания, в том числе необходимость исполнения обязанностей, возложенных на оператора законом, исполнения договора, стороной или выгодоприобретателем по которому является субъект, а также осуществления правосудия и выполнения отдельных публичных функций.

Следовательно, правомерность обработки должна оцениваться исходя из конкретного основания, а не только из наличия стандартной отметки о согласии.

Согласие должно быть конкретным, предметным, информированным, сознательным и однозначным. В случаях, предусмотренных законом, оно оформляется отдельно от иных документов и сведений, подтверждающих согласие лица на заключение договора или получение услуги. Практическая проблема заключается в том, что пользователи цифровых сервисов часто принимают условия обработки автоматически, не изучая объем собираемых сведений и цели их дальнейшего использования. Формальное получение согласия не должно превращаться в способ легализации избыточного или непрозрачного сбора данных.

Особые требования установлены для специальных категорий персональных данных, касающихся, в частности, расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни. Закон предусматривает специальные условия их обработки. Отдельный правовой режим установлен для биометрических персональных данных, характеризующих физиологические и биологические особенности человека и используемых для установления его личности. Распространение биометрической идентификации в цифровых сервисах требует повышенного внимания к основаниям обработки, способам хранения и предотвращению неправомерного доступа.

Важной гарантией является право субъекта получать сведения об обработке его персональных данных, требовать уточнения, блокирования или уничтожения данных в предусмотренных законом случаях, отзывать согласие, если обработка основывается на нем, и обжаловать действия оператора. Реализация этих прав обеспечивает возможность гражданина контролировать законность использования относящейся к нему информации.

3. Обязанности операторов и обеспечение безопасности персональных данных.

Оператор персональных данных занимает центральное место в системе правового регулирования. Им признается государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки, состав данных и совершаемые с ними действия. Именно оператор должен обеспечить соблюдение требований законодательства на всех этапах жизненного цикла данных.

К числу основных обязанностей оператора относится определение законной цели обработки и соответствующего правового основания, обеспечение точности и актуальности сведений, ограничение доступа к ним, соблюдение сроков хранения и прекращение обработки при достижении цели либо при наступлении иных предусмотренных законом обстоятельств. Оператор также обязан предоставлять субъекту информацию об обработке в случаях и порядке, установленных законом, и организовать рассмотрение обращений субъектов персональных данных.

В предусмотренных законом случаях оператор до начала обработки обязан направить уведомление в уполномоченный орган по защите прав субъектов персональных данных. В Российской Федерации таким органом является Роскомнадзор. Исключения из обязанности уведомления определяются законом, поэтому организациям необходимо оценивать наличие соответствующего основания, а не исходить из предположения, что уведомление требуется только отдельным категориям организаций.

Статья 19 Закона № 152-ФЗ возлагает на оператора обязанность принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий [1]. К таким мерам на практике относятся разграничение прав доступа, учет действий пользователей,

применение средств защиты информации, резервное копирование, контроль актуальности программного обеспечения, внутренние регламенты и обучение работников.

Особое значение имеет реагирование на инциденты, связанные с неправомерной или случайной передачей персональных данных, повлекшей нарушение прав субъектов. Закон предусматривает обязанность оператора уведомить уполномоченный орган в течение 24 часов с момента выявления соответствующего инцидента, а затем, в течение 72 часов, сообщить результаты внутреннего расследования в предусмотренном законом объеме. Указанные сроки требуют от организации заранее установленного порядка обнаружения инцидентов, фиксации обстоятельств, определения ответственных лиц и подготовки уведомлений.

Ответственность за нарушение законодательства может быть административной, гражданско-правовой, дисциплинарной, а в предусмотренных законом случаях уголовной. Статья 13.11 Кодекса Российской Федерации об административных правонарушениях предусматривает административную ответственность за различные нарушения законодательства о персональных данных, включая обработку без законного основания, невыполнение требований к защите и нарушение обязанностей при утечке сведений [5]. Применение мер ответственности направлено не только на наказание нарушителя, но и на предупреждение аналогичных нарушений в будущем.

Наличие локальных документов само по себе не гарантирует соблюдение закона. Политика обработки персональных данных, положение о защите информации, формы согласий и договоры с лицами, осуществляющими обработку по поручению оператора, должны соответствовать реальным процессам организации. Если фактические действия сотрудников и используемые информационные системы расходятся с локальными документами, формальное наличие таких документов не обеспечивает должного уровня правовой защиты.

4. Проблемы защиты персональных данных в цифровом обществе.

Одной из наиболее значимых проблем является масштабирование сбора сведений. Цифровые сервисы часто стремятся получать больше информации, чем необходимо для непосредственного оказания услуги. Избыточный сбор повышает риски неправомерного использования и увеличивает последствия возможного инцидента. Принцип минимизации данных предполагает, что оператор должен обосновать необходимость каждого вида собираемой информации с учетом конкретной цели обработки.

Другой проблемой выступает непрозрачность цифровых экосистем. Пользователь может взаимодействовать с одной платформой, тогда как техническая обработка осуществляется несколькими подрядчиками и поставщиками инфраструктуры. В результате гражданину трудно установить, кто именно обладает его сведениями, кому они передаются и кто отвечает за соблюдение требований закона. Для устранения данной проблемы необходимы понятные уведомления о целях обработки, ясное распределение обязанностей в договорах и контроль за лицами, действующими по поручению оператора.

Существенные риски возникают при использовании облачных сервисов, мобильных приложений, систем аналитики и технологий искусственного интеллекта. Такие инструменты могут предполагать объединение массивов данных, автоматизированное профилирование и выводы о поведении или предпочтениях человека. При этом пользователь не всегда понимает, какие именно сведения используются для формирования рекомендаций или принятия решений. Правовая оценка подобных процессов должна учитывать не только первоначально собранные данные, но и новые сведения, получаемые путем их сопоставления и анализа.

Отдельного внимания заслуживает проблема утечек. Даже при наличии технических средств защиты причиной инцидента могут стать ошибки персонала, неправильно настроенные права доступа, использование незащищенных каналов связи или недостаточный контроль подрядчиков. Поэтому обеспечение безопасности требует комплексного подхода,

включающего оценку угроз, регулярную проверку мер защиты, обучение сотрудников и отработку действий при нарушениях.

Наконец, сохраняется проблема недостаточной осведомленности граждан о собственных правах. Пользователи нередко не знают, как запросить сведения об обработке, потребовать исправления неточной информации или обратиться с жалобой. Повышение правовой грамотности должно рассматриваться как самостоятельное направление защиты персональных данных наряду с совершенствованием законодательства и технических средств.

5. Направления совершенствования правового регулирования.

Первым направлением совершенствования представляется повышение прозрачности обработки персональных данных. Информация о целях, правовых основаниях, составе данных, сроках хранения и категориях получателей должна излагаться понятным языком и быть доступной до начала обработки. Сложные многостраничные документы, формально размещенные на сайте, не всегда обеспечивают реальную информированность субъекта.

Вторым направлением является развитие риск-ориентированного подхода. Меры защиты должны учитывать характер обрабатываемых данных, масштаб обработки, возможные последствия нарушения прав субъектов и особенности используемых технологий. Обработка общедоступных контактных сведений и обработка биометрических или специальных категорий данных объективно требуют различного уровня организационных и технических гарантий.

Третье направление связано с усилением контроля за лицами, которым оператор поручает обработку данных. Договоры должны определять перечень операций, цели обработки, требования конфиденциальности, меры безопасности, порядок сообщения об инцидентах и обязанности по возврату или уничтожению данных после завершения поручения. Оператору необходимо проверять не только наличие договорных условий, но и фактическое исполнение требований контрагентом.

Четвертое направление предполагает развитие механизмов реализации прав субъектов. Организациям целесообразно создавать доступные каналы для подачи запросов, обеспечивать регистрацию обращений и контроль сроков ответа. Внутренние процедуры должны позволять оперативно находить данные конкретного лица, проверять основания их обработки, исправлять неточности и прекращать обработку при наличии законных оснований.

Пятое направление состоит в регулярном обучении работников. Персонал должен понимать, какие сведения относятся к персональным данным, в каких случаях допустима их передача, как следует обращаться с электронными документами и куда сообщать о подозрительных событиях. Обучение должно учитывать должностные обязанности сотрудников и сопровождаться практическими инструкциями, а не ограничиваться формальным ознакомлением с локальным актом.

Наконец, правовое регулирование должно развиваться с учетом новых технологий. Использование искусственного интеллекта, биометрических систем и автоматизированного анализа информации требует оценки возможного воздействия на права человека. При разработке цифровых продуктов целесообразно заранее учитывать требования конфиденциальности и безопасности, минимизировать объем собираемых данных и предусматривать возможность проверки законности автоматизированных процессов.

Заключение.

Проведенное исследование позволяет сделать вывод о том, что защита персональных данных является необходимым условием устойчивого развития цифрового общества. Ее правовая основа в Российской Федерации формируется конституционными гарантиями неприкосновенности частной жизни, положениями Федерального закона № 152-ФЗ, общими нормами информационного законодательства и подзаконными требованиями к обеспечению безопасности обработки.

Законодательство закрепляет принципы целевого и соразмерного сбора данных, определяет правовые основания обработки, устанавливает права субъектов и обязанности операторов, предусматривает меры защиты и юридическую ответственность за нарушения. Вместе с тем эффективность этих механизмов зависит от их практической реализации: достоверности локальных документов, контроля подрядчиков, готовности к реагированию на инциденты и уровня правовой грамотности работников и граждан.

В условиях дальнейшей цифровизации приоритетными задачами выступают повышение прозрачности обработки, минимизация собираемых сведений, развитие риск-ориентированных мер безопасности, совершенствование договорного контроля и обеспечение реальной возможности субъектов реализовывать свои права. Только комплексное сочетание правовых, организационных и технических мер позволяет обеспечить баланс между использованием данных для развития цифровых сервисов и охраной частной жизни человека.

СПИСОК ЛИТЕРАТУРЫ:

1. «О персональных данных»: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 26.07.2026)
2. «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 27.07.2006 № 149-ФЗ
3. «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»: Федеральный закон от 21.07.2014 № 242-ФЗ
4. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 01.11.2012 № 1119

5. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ст. 13.11)
6. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с учетом действующих поправок)

Demchuk A.R.
master's degree student
Institute of Life Safety
St. Petersburg University of State Fire Service of EMERCOM of Russia
named after E.N. Zinichev
(St. Petersburg, Russia)

LEGAL REGULATION OF PERSONAL DATA PROTECTION AMID SOCIETAL DIGITALIZATION

Abstract: *this article examines the legal foundations of personal data protection in Russia amid the digitalization of social relations. It considers constitutional guarantees of the right to privacy, provisions of Federal Law «On Personal Data», the legal status of personal data operators and data subjects, conditions for lawful processing, and obligations to ensure data security and report incidents. It identifies enforcement challenges associated with large-scale data collection, the use of digital platforms, transfers of data to third parties, and limited public awareness. It argues for a risk-based approach, greater transparency in data processing, and improved organizational safeguards.*

Keywords: *personal data, protection, digitalization, operator, data subject, consent, confidentiality, information security.*