

DOI: <http://dx.doi.org/10.21686/2411-118X-2026-2-162-169>

Юридическая ответственность за нарушение норм о персональных данных

А. М. Моисеев

кандидат юридических наук,
доцент кафедры гражданско-правовых дисциплин РЭУ им. Г. В. Плеханова;
ответственный секретарь Комиссии по законодательству
и государственному строительству Ассоциации юристов России.

Адрес: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова»,
117997, Москва, Стремянный пер., д. 36;

Комиссия по законодательству и государственному строительству Ассоциации юристов России
101000, Москва, ул. Мясницкая, д. 24/7, стрение 1
E-mail: moiseev.am@rea.ru

А. Р. Хваткова

Магистрант Высшей школы права РЭУ им. Г. В. Плеханова.

Адрес: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова»,
117997, Москва, Стремянный пер., д. 36.
E-mail: olmezovaarina@mail.ru

Legal liability for violating personal data regulations

A. M. Moiseev

PhD in Law, Associate Professor of the Department of Civil Law Disciplines of the PRUE,
Executive Secretary of the Commission on Legislation and State Construction
Associations of Lawyers of Russia

Address: Plekhanov Russian University of Economics, 36 Stremyanny Lane,
Moscow, 117997, Russian Federation;

The Commission on Legislation and State Construction Associations of Lawyers of Russia
24/7 Myasnitskaya street, Building 1, Moscow, 101000, Russian Federation
E-mail: moiseev.am@rea.ru

A. R. Khvatkova

master's student of the Higher School of Law of the PRUE.

Address: Plekhanov Russian University of Economics, 36 Stremyanny Lane,
Moscow, 117997, Russian Federation.
E-mail: olmezovaarina@mail.ru

Поступила 10.03.2026 Принята к печати 25.03.2026

Аннотация

Персональные данные всегда выступали как идентификатор личности, в связи с чем требуют надежной защиты. Объем таких данных расширяется и влечет за собой усложнение связей между субъектами правоотношений, складывающихся в области сбора, анализа, хранения и обработки персональных данных. В целях регулирования отношений между субъектами и операторами персональных данных, был разработан и принят федеральный закон № 152-ФЗ от 14 июля 2006 «О персональных данных»¹. С совершенствованием технологических систем обработки, сбора, передачи и хранения персональных данных, развиваются способы их кражи и неправомерной огласки. Актуальность данной темы заключается в том, что в эпоху информационных технологий, остро встает вопрос защиты персональных данных человека и риск ее утечки в пользование третьих лиц. Научная новизна настоящего исследования заключается в комплексном рассмотрении институ-

¹ Федеральный закон "О персональных данных" от 27 июля 2006 г. № 152-ФЗ // Принят Государственной Думой 8 июля 2006 г. // Одобрен Советом Федерации 14 июля 2006 г.

та ответственности за нарушения в сфере обработки персональных данных через призму трансформации цифровой среды и усиления трансграничного характера информационных потоков.

Ключевые слова: персональные данные, ответственность, законодательство, Роскомнадзор, Федеральный Закон, государственный орган, конфиденциальные сведения, требования, норма, принцип, правовая защита, правонарушение, обработка, сбор, хранение, судебная защита.

Abstract

Personal data has always served as an identifier, requiring reliable protection. The volume of such data is expanding, leading to increasingly complex relationships between parties in legal relationships related to the collection, analysis, storage, and processing of personal data. Federal Law No. 152-FZ of July 14, 2006, "On Personal Data," was developed and adopted to regulate the relationship between subjects and operators of personal data. As technological systems for processing, collecting, transmitting, and storing personal data improve, so do methods for its theft and unauthorized disclosure. The relevance of this topic lies in the fact that in the information technology era, the issue of protecting an individual's personal data and the risk of its leakage to third parties is becoming increasingly pressing. The subject of this study is the legal norms governing relations in the field of personal data protection in the Russian Federation. The scientific novelty of this study lies in its comprehensive examination of the institution of liability for violations in the field of personal data processing through the prism of the transformation of the digital environment and the increasing cross-border nature of information flows.

Keywords: personal data, liability, legislation, Roskomnadzor, Federal Law, government agency, confidential information, requirement, norm, principle, legal protection, violation, processing, collection, storage, judicial protection.

В условиях динамичного развития законодательства, регулирующего отношения в сфере обработки персональных данных, наблюдается тенденция к расширению полномочий органов государственного контроля. Усиление нормативного регулирования направлено на повышение эффективности надзора за деятельностью операторов персональных данных, однако одновременно приводит к увеличению правовых рисков для хозяйствующих субъектов и иных участников предпринимательской деятельности. Одним из ключевых органов, осуществляющих государственный контроль в данной области, выступает Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), наделенная значительным объемом контрольных и надзорных полномочий [4. – С. 91].

В рамках реализации возложенных на него функций данный орган вправе инициировать внеплановые проверки деятельности организаций, в том числе без предварительного уведомления проверяемого субъекта. Помимо этого, Роскомнадзор обладает возможностью получать доступ к информационным системам операторов персональных данных в целях проведения контрольных мероприятий [4. – С. 1]. В случае выявления нарушений уполномоченный орган может применять меры ограничительного характера, включая ограничение доступа к интернет-ресурсам, функционирование которых осуществляется с наруше-

нием требований законодательства о защите персональных данных.

Усиление государственного контроля, расширение полномочий надзорных органов, а также развитие института ответственности свидетельствуют о стремлении законодателя сформировать комплексную систему обеспечения информационной безопасности в условиях цифровизации общественных отношений.

Актуальность рассматриваемой проблематики обусловлена тем, что в условиях цифровизации общественных отношений обработка персональных данных все чаще осуществляется с использованием автоматизированных технологий. Одним из наиболее распространенных примеров выступает применение работодателями систем аудио- и видеонаблюдения за работниками в процессе осуществления ими трудовой деятельности. Использование подобных средств контроля потенциально затрагивает сферу конституционных прав граждан и при определенных условиях может привести к их ограничению.

К числу таких прав относится право на неприкосновенность частной жизни, а также право на личную и семейную тайну, закрепленные в статье 23 Конституции Российской Федерации. Кроме того, Конституция гарантирует каждому человеку тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. В то же время в судебной практике нередко подчеркивается, что тайна связи обладает самостоя-

тельным правовым режимом и отличается по своему юридическому содержанию от института защиты персональных данных. Дополнительно статья 24 Конституции Российской Федерации устанавливает запрет на сбор, хранение, использование и распространение сведений о частной жизни лица без его согласия¹.

Нормативное регулирование отношений, возникающих в связи с обработкой персональных данных, строится на основе системы основополагающих принципов, обязательных для соблюдения всеми операторами персональных данных. Реализация данных принципов направлена на обеспечение законности обработки информации о личности, а также на защиту прав субъектов персональных данных от неправомерного использования, утечки либо передачи информации третьим лицам [1. – С. 103].

Вместе с тем субъекты персональных данных обладают правом на защиту своих интересов в судебном порядке. В частности, они вправе требовать восстановления нарушенных прав, а также предъявлять требования о возмещении имущественного ущерба и компенсации морального вреда в соответствии с нормами гражданского законодательства.

Основные принципы обработки персональных данных закреплены в статье 5 Федерального закона «О персональных данных». К их числу относится осуществление обработки персональных данных на законной и добросовестной основе, соответствие целей обработки тем задачам, ради которых осуществлялся сбор информации, а также недопустимость обработки избыточных сведений. Кроме того, законодатель устанавливает требование соразмерности объема обрабатываемых данных заявленным целям их использования.

Наряду с этим закон запрещает объединение баз данных, созданных для различных целей обработки информации. Также устанавливаются требования к срокам хранения персональных данных, а по достижении целей обработки предусматривается обязанность их уничтожения либо обезличивания.

Указанные принципы носят универсальный характер и распространяются на деятельность всех

операторов персональных данных независимо от их организационно-правовой формы. Они применяются при регулировании различных видов правоотношений, включая гражданские, административные, уголовно-процессуальные и трудовые отношения. Нарушение этих требований способно повлечь наступление различных видов юридической ответственности, среди которых выделяются гражданско-правовая, административная, дисциплинарная и уголовная ответственность².

Согласно статье 24 Федерального закона «О персональных данных» лица, допустившие нарушение требований законодательства в сфере обработки персональных данных, подлежат привлечению к ответственности в соответствии с законодательством Российской Федерации.

Гражданско-правовая ответственность в рассматриваемой сфере может наступать при нарушении положений Федерального закона № 152-ФЗ «О персональных данных», а также норм Гражданского кодекса Российской Федерации. В случаях, когда противоправные действия, связанные с незаконным использованием или распространением персональных данных, повлекли причинение гражданину морального вреда, суд вправе возложить на нарушителя обязанность по выплате денежной компенсации. Данная возможность предусмотрена статьей 151 Гражданского кодекса Российской Федерации, устанавливающей механизм компенсации морального вреда при посягательстве на личные неимущественные права и иные нематериальные блага³.

Дополнительным механизмом защиты прав личности выступает статья 152 Гражданского кодекса Российской Федерации, согласно которой гражданин вправе требовать опровержения сведений, порочащих его честь, достоинство или деловую репутацию. При этом обязанность доказать достоверность распространенной информации возлагается на лицо, распространившее такие сведения. На практике подобные ситуации нередко возникают в результате утечки конфиденци-

1 Конституция РФ от 12 декабря 1993 г. (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30 декабря 2008 г. № 6-ФКЗ, от 30 декабря 2008 г. № 7-ФКЗ, от 05 февраля 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ)

2 "Уголовный кодекс Российской Федерации" от 13 июня 1996 г. № 63-ФЗ (ред. от 20 февраля 2026) // Принят Государственной Думой 24 мая 1996 г. // Одобрен Советом Федерации 5 июня 1996 г.

3 Гражданский кодекс Российской Федерации от 30 ноября 1994 г. № 51-ФЗ // принят Государственной Думой 21 октября 1994 г.

альных сведений либо неправомерного распространения персональных данных третьими лицами¹. Для физических лиц это влечет за собой моральный вред, а компании могут понести убытки и репутационные риски, а также потерять доверие со стороны деловых партнеров и клиентов.

Так, Публичное акционерное общество Сбербанк обратилось в суд с иском к гражданину Бутурлакину А. С., ссылаясь на то, что в период с 1 по 10 октября 2019 г. Бутурлакин А. С. скопировал со своего служебного компьютера данные клиентов ПАО Сбербанк (далее – Банк), составляющие банковскую тайну, которые пытался сбить за денежное вознаграждение на интернет-форуме «Dublik.at». Данные действия Бутурлакина А. С. были обнаружены сотрудниками ООО «Биозон», осуществлявшими на основании заключенного с Банком агентского договора мониторинга информации о возможных незаконных фактах размещения в сети «Интернет» объявлений, содержащих сведения, составляющие банковскую тайну. 23 октября 2019 г. средствами массовой информации (далее – СМИ) стало известно об утечке персональных данных о клиентах банка и о том, что похищенные данные выставлены на продажу. Согласно экономическому отчету от 7 июля 2020 г., а также рецензии, выполненной ООО "Профессиональная Группа Оценки", ущерб от публикаций в связи с утечкой данных о клиентах ПАО Сбербанк составляет 3 535 610 руб.

Приговором суда установлено, что 17 октября 2019 г. в вечернее время Бутурлакин А. С. умышленно, из корыстной заинтересованности, через систему мгновенных сообщений направил в ООО «Бизон» фрагмент ранее скопированного файла, содержащий сведения о персональных данных 2013 должников - клиентов ПАО Сбербанк, а именно личные и паспортные данные клиентов, данные об их задолженности и номера банковских счетов, являющихся в соответствии со статьей 26 Федерального закона от 2 декабря 1990 г. № 395-І «О банках и банковской деятельности» банковской тайной, тем самым разгласив указанные сведения лицу, не имеющему к ним доступа

на законном основании². Так Банк претерпел репутационные риски и потерял клиентское доверие, тем самым ему был причинен существенный вред.

Значительное количество норм, устанавливающих ответственность за нарушения в сфере обработки персональных данных, содержится в Кодексе об административных правонарушениях Российской Федерации. Данный нормативный акт наделяет должностных лиц Роскомнадзора полномочиями возбуждать дела об административных правонарушениях. Как правило, ответственность наступает за совершение операторами персональных данных противоправных действий либо за неисполнение обязанностей, предусмотренных законодательством.

Так, в соответствии с частью 1 статьи 13.11 КоАП Российской Федерации ответственность может наступать в случаях обработки персональных данных с нарушением целей их первоначального сбора либо с несоблюдением требований законодательства³. Кроме того, часть 2 указанной статьи предусматривает ответственность за обработку персональных данных без получения письменного согласия субъекта в тех ситуациях, когда такое согласие является обязательным условием законности обработки.

Верховный суд в своем Постановлении от 21 января 2026 г. № 5-АД25-119-К2 назначил административное наказание Учреждению в пределах санкции части 1 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях. Как следует из материалов дела, 27 ноября 2023 г. в 09 часов 30 минут Министерство труда и социальной защиты Российской Федерации, являясь оператором персональных данных, предоставило неправомерный открытый доступ к информационным системам персональных данных Министерства. Это привело к нарушению прав субъектов персональных данных: персональные данные работников и их родственников стали доступны неограниченному кругу лиц по нескольким адресам в сети «Интернет». Министерство труда и социальной защиты Российской Федерации совершило административное право-

¹ Информационные технологии в управлении персоналом [Электронный ресурс]: электрон. учеб. пособие / ТГУ ; Ин-т финансов, экономики и управления ; каф. «Менеджмент организации» ; сост. Л. В. Сергеева, С. Д. Сыротюк. - Тольятти : ТГУ, 2014. – С. 143.

² Определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 13 февраля 2024 г. № 16-КГ23-70-К4

³ Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. от 20 февраля 2026 г.) (с изм. и доп., вступ. в силу с 03 марта 2026 г.)

нарушение, предусмотренное частью 1 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях, что подтверждается собранными по делу доказательствами, получившими оценку с точки зрения их относимости, допустимости и достаточности, по правилам статьи 26.11 Кодекса Российской Федерации об административных правонарушениях¹.

К числу административных правонарушений также относится несоблюдение требований о публичности политики оператора в сфере обработки персональных данных, выражающееся в отсутствии свободного доступа к соответствующему документу. Кроме того, ответственность может наступать за нарушение сроков обработки персональных данных, а также за непредоставление субъекту информации о целях и способах обработки его персональных данных.

Отдельный акцент в законодательстве сделан на обеспечение сохранности персональных данных в тех случаях, когда их обработка осуществляется без применения автоматизированных средств. Речь идет прежде всего о работе с материальными носителями информации, для которых должны быть созданы условия, исключающие утрату данных или доступ к ним посторонних лиц. На практике это означает обязанность оператора организовать хранение таким образом, чтобы исключить возможность несанкционированного ознакомления, копирования или изменения сведений. Если подобные требования не соблюдаются и это приводит к утрате, искажению либо распространению персональных данных, такие действия образуют состав административного правонарушения [4. – С. 88].

Помимо общих требований, законодатель выделяет и ряд специальных обязанностей, возлагаемых на операторов. В частности, для государственных и муниципальных органов предусмотрена необходимость проведения процедур обезличивания персональных данных в установленных законом ситуациях². Отдельные требования каса-

ются и обработки информации в сети «Интернет»: оператор, осуществляющий сбор данных таким способом, обязан обеспечить их фиксацию, систематизацию и хранение с использованием технической инфраструктуры, расположенной на территории Российской Федерации. Повторное игнорирование данных требований, как правило, влечет ужесточение мер ответственности.

Как показывает практика, наиболее распространенной формой привлечения к ответственности в данной сфере остаются административные меры – предупреждение либо штраф. При этом нельзя не отметить, что за последние годы соответствующие нормы административного законодательства были существенно переработаны: уточнены признаки правонарушений, а также пересмотрены размеры санкций в сторону их увеличения.

Особое место вопросы защиты персональных данных занимают в трудовых отношениях. Уже на этапе приема на работу работодатель получает значительный объем сведений о работнике, включая документы личного характера. В этой связи на него возлагается обязанность не только использовать такие данные в рамках закона, но и обеспечить их надежную защиту от неправомерного доступа³. Соответствующие требования закреплены в трудовом законодательстве и подлежат обязательному соблюдению.

Ответственность за соблюдение режима конфиденциальности внутри организации, как правило, распределяется между несколькими субъектами: руководителем, сотрудниками кадровых служб, а также иными работниками, имеющими доступ к персональным данным. Разглашение такой информации может повлечь применение дисциплинарных мер, предусмотренных трудовым законодательством, вплоть до увольнения [2. – С. 300].

При этом, если неправомерное распространение персональных данных повлекло причинение работнику морального вреда, работодатель обязан выплатить компенсацию в установленном порядке. Таким образом, защита персональных данных в трудовых отношениях имеет не только организационный, но и имущественный аспект.

¹ Постановление Верховного суда РФ от 21 января 2026 г. № 5-АД25-119-К2

² Постановление Правительства РФ от 21 марта 2012 г. № 211 (ред. от 15 апреля 2019 г.) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

³ Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ // Принят Государственной Думой 21 декабря 2001 г. // Одобрен Советом Федерации 26 декабря 2001 г.

Следует учитывать, что нормы трудового права направлены также на охрану служебной и коммерческой тайны, тесно связанной с персональными данными работников. Нарушение установленного режима конфиденциальности рассматривается как дисциплинарный проступок и может повлечь наиболее строгие меры воздействия [3. – С. 346].

В тех случаях, когда незаконное обращение с персональными данными выходит за рамки административного правонарушения, речь может идти уже о наступлении уголовной ответственности. В частности, уголовное законодательство предусматривает наказание за незаконное получение или распространение сведений о частной жизни лица без его согласия, если такие сведения относятся к личной или семейной тайне.

Перечень возможных санкций в данном случае достаточно широк и включает как имущественные меры, так и различные виды работ, а также лишение свободы. Более строгий подход применяется к ситуациям, когда противоправные действия совершаются с использованием служебного положения: в таких случаях увеличивается как размер штрафа, так и максимальные сроки наказания, а также может вводиться запрет на осуществление определенной деятельности¹.

Отдельного внимания заслуживает деятельность уполномоченного органа, осуществляющего контроль в сфере обработки персональных данных. В течение длительного времени формируется и ведется специализированный реестр операторов, позволяющий систематизировать сведения о субъектах, осуществляющих обработку данных, и отслеживать их деятельность.

Поскольку информация, включаемая в данный реестр, в значительной степени является открытой, любые нарушения требований законодательства становятся известны широкому кругу лиц. В результате негативные последствия для организаций не ограничиваются только юридической ответственностью. Утечка данных или несоблюдение правил их обработки зачастую приводит к снижению доверия со стороны клиентов и партнеров, что непосредственно отражается на деловой репутации.

Социологические данные также подтверждают наличие проблем в рассматриваемой сфере. Согласно результатам исследований, лишь ограниченное число граждан оценивает уровень защищенности своих персональных данных как достаточный. Подобная оценка указывает на сохраняющийся разрыв между формально установленными гарантиями и их практической реализацией [2. С. – 300].

Несмотря на то, что действующее законодательство предоставляет возможность защиты нарушенных прав в судебном порядке, включая взыскание убытков и компенсацию морального вреда, реализация этих механизмов на практике сопряжена с рядом сложностей. Наиболее существенной из них является необходимость доказать как сам факт причинения вреда, так и его размер. Кроме того, судебная практика показывает, что размеры присуждаемых компенсаций, как правило, остаются незначительными [1. – С. 101].

Так, судебная коллегия рассмотрела в открытом судебном заседании гражданское дело по иску Поздеева А. Н. к публичному акционерному обществу «Балтийский Банк» о защите прав потребителя. В результате необоснованного отказа в реструктуризации долга, раскрытия сведений о заемщике третьему лицу, Поздееву А. Н. причинены нравственные страдания, в связи с чем просил о компенсации морального вреда в размере 50 000 руб. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Суд первой инстанции отказал в удовлетворении иска, сославшись на соответствие отказа в реструктуризации закону (так как это не является обязанностью банка), а также правомерность передачи персональных данных, как необходимых для исполнения агентского договора. Судебная коллегия по гражданским делам Верховного Суда Российской Федерации Определением от 01 августа 2017 г. № 78-КГ17-45 вернула дело на новое рассмотрение, отметив отсутствие согласия истца на предоставление своих персональных данных (номер телефона и адрес проживания). В результате Апелляционным определением Санкт-Петербургского городского суда от 12 октября 2017 г. № 33-21816/2017 по делу № 2-6298/2016 в пользу истца были взысканы 10 000 рублей на основании нарушения законодательства о персональных данных.

¹ Информационные технологии в управлении персоналом [Электронный ресурс]: электрон. учеб. пособие / ТГУ ; Ин-т финансов, экономики и управления ; каф. "Менеджмент организации" ; сост. Л. В. Сергеева, С. Д. Сыротюк. - Тольятти : ТГУ, 2014. – С. 90.

Дополнительные проблемы возникают в ситуациях, когда нарушителями выступают иностранные компании, не имеющие юридического присутствия в Российской Федерации. Отсутствие у таких субъектов имущества и представительств существенно ограничивает возможности применения к ним мер принудительного характера. В подобных условиях одним из немногих доступных инструментов остается ограничение доступа к соответствующим интернет-ресурсам, однако данная мера не всегда позволяет в полной мере восстановить нарушенные права.

Вместе с тем в российской практике уже имели место случаи привлечения к ответственности крупных зарубежных цифровых платформ за несоблюдение требований о локализации персональных данных. Такие компании обязаны обеспечивать хранение информации о российских пользователях на территории Российской Федерации [1. – С. 102]. Однако фактическое отсутствие полноценного правового присутствия в национальной юрисдикции продолжает создавать препятствия для эффективного правоприменения.

В целях устранения существующего дисбаланса в регулировании деятельности отечественных и зарубежных компаний в 2019 г. автономной некоммерческой организацией «Цифровая экономика» была выдвинута инициатива по ограничению доступа к персональным данным российских граждан для иностранных организаций, не имеющих юридического присутствия в Российской Федерации. Данное предложение было обусловлено необходимостью обеспечения равных условий конкуренции, поскольку российские компании обязаны соблюдать более строгие требования законодательства по сравнению с иностранными участниками цифрового рынка [5. – С.750].

В рамках этой инициативы подчеркивалась недопустимость ситуации, при которой иностранные компании, не исполняющие требования российского законодательства, получают конкурентные преимущества за счет более мягкого регулирования. Предполагалось, что установление дополнительных ограничений позволит устранить подобный дисбаланс и повысить эффективность защиты персональных данных [2. – С. 299].

Рассматриваемая проблема затронула и крупные российские технологические компании с иностранной юрисдикцией регистрации. В частности,

внимание было обращено на деятельность компании «Яндекс», головная структура которой зарегистрирована за пределами Российской Федерации. В связи с этим в 2019 г. был предложен законопроект, предусматривающий введение ограничений на долю иностранного участия в компаниях, признанных значимыми для российского информационного пространства. В качестве одного из критериев значимости рассматривалось количество пользователей на территории Российской Федерации [5. – С. 747].

Несмотря на наличие иностранной юрисдикции, компании, осуществляющие деятельность на территории Российской Федерации через зарегистрированные юридические лица, обязаны соблюдать требования национального законодательства. В частности, на них распространяются положения о защите персональных данных, а также контрольные полномочия уполномоченных органов, включая Роскомнадзор.

Таким образом, несоблюдение требований законодательства в сфере защиты персональных данных формирует для организаций комплекс рисков, включающих как финансовые потери, связанные с применением штрафных санкций, так и репутационные издержки, оказывающие негативное влияние на деловую репутацию и конкурентоспособность хозяйствующих субъектов. Проблема наступления ответственности за нарушение норм в сфере персональных данных заключается в основном в доказывании незаконной утечки конфиденциальных сведений в пользование третьих лиц, а именно то, что эти сведения не были общедоступными или на их обработку не было дано письменного согласия субъекта персональных данных. Иной проблемой выступает доказывание субъектом персональных данных размера причиненного ему морального вреда в случае распространения сведений о нем.

Дальнейшее развитие института защиты персональных данных должно осуществляться с учетом баланса интересов личности, общества и государства. Только при условии системного подхода, сочетающего нормативное регулирование, эффективное правоприменение и современные технологические решения, возможно достижение высокого уровня защиты персональных данных и обеспечение доверия граждан к цифровой среде [1. – С. 100].

Список литературы

1. *Мачульская Е. Е.* Правовое регулирование персональных данных работника в Российской Федерации и государствах-участниках СНГ. – М. : МГУ им. Ломоносова, 2005. – 103 с.
2. *Саматов К. М.* Персональные данные как институт права // Новые вопросы в современной науке. Материалы Международной (заочной) научно-практической конференции под общей редакцией А. И. Вострецова. – 2017. – С. 297–300.
3. *Сергеевич В. А., Смолькова И. В.* Проблемы становления и развития института «право быть забытым» // Проблемы охраняемой законом тайны в уголовном процессе. – М. : 2020. – 346 с.
4. *Степанов Е.* Персональные данные и их защита // Кадровое дело. – 2007. – № 9. – С. 86–102.
5. *Тимиршяхов С. Ю., Тимиршяхова Ю. В.* Правовые проблемы защиты информации при обработке персональных данных // Правозащитная деятельность в современной России: проблемы и их решение Сборник научных трудов III Международной научно-практической конференции. – 2017. – С. 747–750.