
АКТУАЛЬНЫЕ ТЕМЫ

DOI 10.35775/PSI.2025.76.11.005

УДК 32

А.А. ОСМАНОВА

студентка юридического факультета
Кубанского государственного аграрного университета
им. И.Т. Трубилина, Россия, г. Краснодар
E-mail: osmanova20152015@gmail.com

Д.Э. ШМАКОВА

студентка юридического факультета
Кубанского государственного аграрного университета
им. И.Т. Трубилина, Россия, г. Краснодар
E-mail: shmakova.diana1111@mail.ru

Н.В. ПАВЛОВ

кандидат юридических наук, доцент
кафедры административного и финансового права
Кубанского государственного аграрного университета
им. И.Т. Трубилина, Россия, г. Краснодар
E-mail: nik281@mail.ru

АДМИНИСТРАТИВНАЯ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВИЛ ХРАНЕНИЯ И ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

В статье исследуются особенности административной ответственности за нарушение правил хранения и использования персональных данных в условиях цифровизации общественных отношений. Авторы анализируют ключевые положения Федерального закона № 152-ФЗ «О персональных данных», статьи 13.11 КоАП РФ, а также сопутствующих норм трудового и административного законодательства, формирующих комплексный правовой механизм защиты сведений о личности. Значительное внимание уделено судебной практике, позволяющей выявить типичные составы правонарушений, в том числе отсутствие информированного согласия субъекта данных, несоблюдение установленных целей и сроков обработки, нарушение порядка передачи информации третьим лицам, а также невыполнение предписаний Роскомнадзора. На основе рассмотренных дел авторы демонстрируют устойчивую тенденцию формального подхода к соблюдению требований законодательства со стороны операторов персональных данных, включая работодателей. Отмечается недостаточная правовая и цифровая грамотность организаций, отсутствие эффективных внутренних процедур защиты информации, слабость технических мер безопасности, а также использование недопустимых способов фиксации согласия субъектов. Отдельно анализируется роль Роскомнадзора как

уполномоченного органа, обладающего широким комплексом надзорных полномочий, что усилило эффективность контроля после передачи ему полномочий по возбуждению дел об административных правонарушениях. Авторы приходят к выводу о необходимости модернизации действующей системы административной ответственности, повышения строгости санкций за грубые и повторные нарушения, а также устранения пробелов в регулировании порядка согласия и требований к обеспечению безопасности данных. Совершенствование законодательства должно быть направлено на развитие эффективного механизма защиты персональной информации в условиях нарастающих цифровых угроз.

Ключевые слова: персональные данные, административная ответственность, КоАП РФ, Федеральный закон № 152-ФЗ, Роскомнадзор, защита информации, согласие субъекта, трудовые отношения, цифровое право.

В условиях стремительной цифровизации всех сфер общественной жизни, когда обработка персональных данных становится неотъемлемым элементом функционирования практически любой организации, возрастает необходимость эффективной правовой защиты информации, касающейся частной жизни граждан. Персональные данные, отражающие сведения о личности, ее идентифицирующих признаках, социальном статусе, контактной информации и даже взглядах, при несанкционированной обработке, могут быть использованы во вред их субъекту. Проблемы несанкционированного распространения персональных данных и телефонного мошенничества приобретают всё более масштабный характер. По сведениям Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее — Роскомнадзор), только в 2024 году выявлено свыше 680 миллионов случаев утечки персональных сведений граждан Российской Федерации [5. С. 187]. Это обстоятельство обуславливает значимость государственной политики в области правового регулирования защиты персональных данных, в том числе через применение мер административной ответственности.

Административная ответственность в данном контексте представляет собой один из действенных механизмов охраны публичных интересов, направленный на предотвращение нарушений законодательства о персональных данных, а также на наказание виновных лиц. Согласно правовой доктрине, административная ответственность представляет собой меры государственного принуждения, применяемые к физическим или юридическим лицам за совершение административного правонарушения. Как справедливо отмечает И.В. Максимов, в условиях правового государства юридическая ответственность приобретает двойную направленность: с одной стороны — на защиту прав и свобод личности, с другой — на охрану общественного правопорядка от нарушений. Отсюда и необходимость развития системы правоприменения в части привлечения к ответственности за противоправные действия, связанные с персональными данными [2. С. 100].

В основе правового регулирования ответственности за нарушение порядка хранения и использования персональных данных лежит Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — Закон о персональ-

ных данных) [3], который содержит как принципы обработки данных, так и конкретные требования к субъектам, осуществляющим такую деятельность. Отмеченный нормативно-правовой акт устанавливает необходимость получения согласия субъекта персональных данных на их обработку, ограничение целей обработки, обеспечение безопасности информации, а также закрепляет права субъектов на доступ, уточнение и уничтожение своих данных. Он формирует базовую нормативную рамку, внутри которой должна выстраиваться как профилактическая, так и карательная деятельность государства.

Одновременно с этим административная ответственность непосредственно предусмотрена статьей 13.11 КоАП РФ [1], которая включает более десятка составов правонарушений в области персональных данных. К числу наиболее распространенных можно отнести обработку данных без согласия субъекта, несоблюдение сроков и целей хранения, передачу данных третьим лицам без правовых оснований, отсутствие уведомления Роскомнадзора о начале обработки, а также невыполнение предписаний уполномоченного органа. При этом наказания варьируются от предупреждения до значительных административных штрафов, размер которых может достигать 500 тысяч рублей для юридических лиц в случае повторных нарушений.

Необходимо отметить, что в сфере трудовых правоотношений вопросы обработки персональных данных приобретают дополнительную значимость. Согласно статье 86 ТК РФ [10], работодатель обязан обеспечить соблюдение прав работников при обработке их персональных данных, включая защиту от неправомерного использования и утечки. При этом нередко встречаются случаи формального подхода со стороны работодателей, когда отсутствуют необходимые локальные нормативные акты, не обеспечивается информированность работников, а персональные данные хранятся без должного уровня защиты. Как справедливо подчеркивает И.А. Трофимова, работодатель зачастую не придает должного значения своим обязанностям по защите персональных данных, что приводит к массовым нарушениям, особенно при отсутствии правовой грамотности в данной сфере [9. С. 161].

Кроме того, действующее законодательство предусматривает ответственность и за отказ в предоставлении сведений по запросам государственных органов. Например, непредоставление информации, необходимой для надзорных мероприятий Роскомнадзора, может быть квалифицировано по статьям 19.4 или 19.7 КоАП РФ, что также подчеркивает важность сотрудничества операторов персональных данных с контролирующими органами.

Судебная практика в сфере привлечения к административной ответственности за нарушение правил хранения и использования персональных данных позволяет выявить ряд устойчивых тенденций и типовых правонарушений, наиболее часто встречающихся как в коммерческом, так и в государственном секторе. Одним из ключевых источников информации о таких правонарушениях являются материалы дел, возбуждаемых по статье 13.11 КоАП РФ. Судебные решения, как правило, фиксируют факты отсутствия согласия на обработку персональных данных, нарушения установленного порядка их хранения, использования или

передачи третьим лицам, а также непредоставления субъекту сведений о целях и способах обработки его данных.

Характерным примером выступает дело в отношении ООО «Мираж», рассмотренное в рамках производства по части 1 статьи 13.11 КоАП РФ.

В ходе проверки было установлено, что организация осуществляла обработку персональных данных работников без их письменного согласия. В результате суд признал юридическое лицо виновным и назначил наказание в виде предупреждения. Несмотря на мягкость санкции, дело показательным с точки зрения системного нарушения базовых принципов обработки персональных данных, установленных в статье 6 и пункте 1 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» [6].

Схожие обстоятельства были установлены в деле ООО АНО ДПО «Учебный Центр Газ-Нефть», где отсутствовало согласие субъектов персональных данных на передачу информации третьим лицам. Кроме того, выяснилось, что работники не были ознакомлены под роспись с локальными актами, регламентирующими обработку и защиту персональных данных. Данные действия также были квалифицированы по статье 13.11 КоАП РФ. В решении суда подчеркивается, что нарушение порядка сбора персональных данных без получения согласия в письменной форме является достаточным основанием для привлечения к административной ответственности [7].

Не менее важным элементом правоприменения в сфере административной ответственности является контроль за выполнением требований надзорных органов. Согласно статье 3 Закона о персональных данных, надзор за соблюдением законодательства осуществляет Роскомнадзор. До 1 июля 2017 года возбуждать дела об административных правонарушениях в сфере персональных данных могли только прокуроры. Однако с указанной даты соответствующие полномочия были переданы и должностным лицам Роскомнадзора, что существенно усилило эффективность надзорной функции.

Полномочия Роскомнадзора включают проведение плановых и внеплановых проверок операторов персональных данных, направление предписаний об устранении выявленных нарушений, возбуждение дел об административных правонарушениях, а также представление интересов государства в суде [4. С. 153]. Кроме того, Роскомнадзор вправе использовать инструменты предварительного контроля, включая обязательную регистрацию операторов в реестре, уведомление о начале обработки, а также согласование трансграничной передачи персональных данных.

Важным направлением правоприменительной практики является защита субъектов данных трудовых отношениях. Например, в деле, рассмотренном Центральным районным судом г. Хабаровска (дело № 12-538/2017), акционеры общества потребовали предоставления копии трудового договора с генеральным директором. Суд отказал в удовлетворении требования, сославшись на положения статьи 88 ТК РФ, устанавливающей запрет на передачу персональных данных работника третьим лицам без его письменного согласия, а также на статью 90 ТК РФ, предусматривающую административную и гражданско-пра-

вовую ответственность за нарушения порядка хранения и передачи персональных данных [8].

Сложности при квалификации административных правонарушений возникают и в тех случаях, когда нарушается порядок хранения персональных данных. Закон обязывает оператора принимать меры, направленные на предотвращение несанкционированного доступа, уничтожение или изменение данных. Однако на практике встречаются случаи, когда материальные носители с персональными данными хранятся без должной защиты, отсутствует разграничение прав доступа, не ведется журнал регистрации действий с данными. Такие факты были выявлены, например, при проверке в ООО «Дяппе», где не были представлены доказательства, подтверждающие, что инструкции и журналы инструктажа сотрудников содержали персональные данные и что доступ к ним был надлежащим образом ограничен. Суд расценил это как нарушение требований хранения персональных данных и признал в действиях должностных лиц состав административного правонарушения [7].

Анализ российского законодательства и практики его применения в сфере административной ответственности за нарушение порядка хранения и использования персональных данных позволяет выявить целый ряд системных проблем, свидетельствующих о необходимости его доработки как на уровне нормативного регулирования, так и в части административного правоприменения.

Одной из ключевых проблем является отсутствие четких и единообразных критериев, позволяющих однозначно квалифицировать деяние как административное правонарушение. Законодательство формулирует общие обязанности операторов и устанавливает запреты (например, на обработку без согласия, нарушение целей хранения и передачи данных), однако на практике правоприменителям приходится сталкиваться с пробелами в толковании: что является достаточной степенью защиты, в каких случаях можно считать согласие информированным, как разграничивать дисциплинарную и административную ответственность.

Так, в большинстве рассмотренных примерах судебных дел, санкции ограничиваются предупреждением или минимальным штрафом. Это снижает превентивную эффективность института административной ответственности. Подобный подход делает правоприменение формальным, поскольку не обеспечивает достаточного уровня защиты прав субъектов персональных данных, особенно в случаях, когда ущерб не является материально выраженным, но очевидно нарушает частную сферу личности.

Следующей важной проблемой является слабая осведомленность операторов персональных данных, особенно субъектов малого и среднего бизнеса, о содержании и объеме их обязанностей. Многие организации рассматривают меры по обеспечению защиты данных как дополнительную, не имеющую приоритета обязанность, выполнение которой откладывается или формализуется. Это приводит к массовым нарушениям, в том числе непреднамеренным. Отсутствие штатных специалистов по защите информации и правовых консультантов усугубляет ситуацию.

Значительный пробел связан с отсутствием механизма юридически значимой фиксации согласия субъекта данных. Несмотря на наличие нормативного регулирования, прежде всего в Законе о персональных данных и статье 13.11 КоАП РФ, существующая правоприменительная практика указывает на целый ряд проблем: формальный подход к ответственности, неэффективность санкций, пробелы в регулировании порядка согласия и хранения данных, а также низкий уровень правовой осведомленности операторов. В некоторых случаях используется «встроенное согласие» в тексте договора, что противоречит духу законодательства и позициям Роскомнадзора.

Не менее важной проблемой остается техническая слабость мер защиты, используемых многими организациями. Несмотря на формальное наличие положений об ограничении доступа к информации, в реальности журналы доступа не ведутся, меры шифрования не применяются, а доступ к базам данных может быть осуществлен без соответствующего разграничения прав.

Административная ответственность за нарушение правил хранения и использования персональных данных является важным инструментом обеспечения права граждан на неприкосновенность частной жизни в условиях цифровизации. Несмотря на наличие нормативного регулирования, прежде всего в Законе о персональных данных и статье 13.11 КоАП РФ, существующая правоприменительная практика указывает на целый ряд проблем: формальный подход к ответственности, неэффективность санкций, пробелы в регулировании порядка согласия и хранения данных, а также низкий уровень правовой осведомленности операторов.

Судебная практика показывает устойчивое распространение нарушений, особенно в трудовых отношениях, тогда как применяемые меры воздействия зачастую не обеспечивают должного превентивного эффекта. Надзорная деятельность Роскомнадзора требует дальнейшего усиления и цифровизации.

В целях повышения эффективности административной ответственности необходимо усилить санкции за грубые и повторные нарушения, имеющие признаки нарушения правил хранения и использования персональных данных, обеспечить нормативную ясность и унификацию практики. Совершенствование законодательства должно быть направлено на формирование устойчивой системы защиты персональных данных, способной эффективно реагировать на вызовы цифровой эпохи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства Российской Федерации. 2002. № 1 (часть I). Ст. 1.
2. **Максимов И.В.** Административные наказания. М., 2009.
3. О персональных данных: федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства Российской Федерации. 2006. № 31 (часть I). Ст. 3451.

4. **Останина А.М., Павлов Н.В.** Утечка персональных данных и телефонное мошенничество: проблемные вопросы и пути решения // Международный журнал гуманитарных и естественных наук. 2025. № 1-4 (100).
5. **Останина А.М., Павлов Н.В.** Контроль и надзор как основные способы обеспечения законности в административно-публичной деятельности // Евразийский юридический журнал. 2024. № 2 (189).
6. Постановление мирового судьи судебного участка № 12 Зуевского судебного района Кировской области от 08.04.2015 по делу № 5-199/15 // СПС «КонсультантПлюс» // <http://www.consultant.ru/document/>.
7. Постановление мирового судьи судебного участка № 8 Советского района г. Уфы Республики Башкортостан по делу № 5-203/2015 // СПС «КонсультантПлюс» // <http://www.consultant.ru/document/>.
8. Решение по делу № 12-538/2017 Центрального районного суда г. Хабаровска от 17.07.2017 // СПС «КонсультантПлюс» // <http://www.consultant.ru/document/>.
9. **Трофимова И.А.** Административная ответственность за нарушение правил обработки и хранения персональных данных // Закон и право. 2018. № 9.
10. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ // Парламентская газета. 2002. № 2-5.

A.A. OSMANOVA

Student, Faculty of Law, Kuban State
Agrarian University named after I.T. Trubilin,
Krasnodar, Russia

D.E. SHMAKOVA

Student, Faculty of Law, Kuban State
Agrarian University named after I.T. Trubilin,
Krasnodar, Russia

N.V. PAVLOV

Candidate of Law, Associate Professor
of the Department of Administrative and Financial Law,
Kuban State Agrarian University named
after I.T. Trubilin, Krasnodar, Russia

ADMINISTRATIVE LIABILITY FOR VIOLATING THE RULES OF STORAGE AND USE OF PERSONAL DATA

The article examines the specifics of administrative liability for violating the rules governing the storage and use of personal data in the context of the digitalization of social relations. The authors analyze the key provisions of Federal Law № 152-FZ «On Personal Data» Article 13.11 of the Code of Administrative Offenses of the Russian Federation, as well as related norms of

labor and administrative legislation that form a comprehensive legal mechanism for protecting personal information. Particular attention is paid to judicial practice, which makes it possible to identify typical offenses, including the absence of informed consent from the data subject, failure to comply with the established purposes and terms of data processing, violations related to transfers of information to third parties, and failure to comply with the orders of Roskomnadzor. Based on reviewed cases, the authors demonstrate a persistent trend toward a formal approach to complying with legal requirements by personal data operators, including employers. The analysis notes insufficient legal and digital literacy among organizations, the lack of effective internal procedures for data protection, weak technical security measures, and the use of improper methods for obtaining and recording consent. The role of Roskomnadzor as the authorized supervisory body is examined separately, emphasizing the increased effectiveness of oversight following the expansion of its powers to initiate administrative proceedings. The authors conclude that the existing system of administrative liability requires modernization, stricter sanctions for severe and repeated violations, and the elimination of regulatory gaps concerning consent procedures and data security requirements. Legislative improvements should be aimed at developing an effective mechanism for protecting personal information amid growing digital threats.

Key words: personal data, administrative liability, Code of Administrative Offenses of the Russian Federation, Federal Law № 152-FZ, Roskomnadzor, information protection, consent of the data subject, labor relations, digital law.