

DOI: 10.12731/2576-9634-2025-9-2-238

EDN: TCZLPF

УДК 342.7



Научная статья

ПРОБЛЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЭПОХУ ЦИФРОВИЗАЦИИ

В.М. Пискайкина, А.Г. Монетов

Аннотация

Обоснование. В статье рассматривается проблема защиты прав человека в эпоху цифровизации, а именно безопасность и конфиденциальность персональных данных граждан Российской Федерации, в том числе биометрических персональных данных.

Цель. Целью исследования является изучение теории и правовой природы персональных данных, а также рассмотрение нормативно-правовой базы, гарантирующей защиту персональных данных в эпоху цифровизации в Российской Федерации.

Метод. В рамках данной работы использовались сравнительно-правовой и системный подходы, что дало возможность авторам углубленно изучить вопрос обеспечения защиты персональных данных граждан Российской Федерации. Проводится анализ статистических сведений об инцидентах, связанных с утечкой или неправомерным использованием персональных данных в 2024 году. Изучается структура организации персональных данных, а также определяются категории личных сведений, подлежащих особой защите, на базе изучения судебной практики. Анализируется нормативно-правовая база, регулирующая сферу персональных данных, с учетом последних изменений в законодательстве, касающихся ответственности за нарушения в соответствии со ст. 13.11 КоАП РФ и ст. 272.1 УК РФ. Отдельное внимание уделяется классификации биометрических данных, с акцентом на обеспечении защиты биометрической информации несовершеннолетних, включая анализ соответствующих судебных прецедентов.

Результаты. В ходе проведенного исследования были определены особенности и условия правового регулирования защиты института персональных данных в Российской Федерации. Кроме того, акцентируется внимание на совершенствовании российского законодательства в части административной и уголовной ответственности за совершение правонарушений данного института.

Область применения результатов. Результаты исследования можно использовать при проведении дальнейших исследований в сфере защиты прав человека.

Ключевые слова: цифровизация; защита прав человека; персональные данные; биометрические персональные данные; правовая защита

Для цитирования. Пискайкина, В. М., & Монетов, А. Г. (2025). Проблема защиты персональных данных в эпоху цифровизации. *Russian Studies in Law and Politics*, 9(2), 124–140. <https://doi.org/10.12731/2576-9634-2025-9-2-238>

Original article

THE PROBLEM OF PERSONAL DATA PROTECTION IN THE ERA OF DIGITALIZATION

V.M. Piskaikina, A.G. Monetov

Abstract

Background. The article examines the problem of human rights protection in the era of digitalization, namely the security and confidentiality of personal data of citizens of the Russian Federation, including biometric personal data.

Objective. The purpose of the research is to study the theory and legal nature of personal data, as well as to consider the regulatory framework that guarantees the protection of personal data in the era of digitalization in the Russian Federation.

Method. Within the framework of this work, comparative legal and systematic approaches were used, which enabled the authors to study in

depth the issue of ensuring the protection of personal data of citizens of the Russian Federation. Statistical data on incidents related to the leakage or misuse of personal data in 2024 is being analyzed. The structure of the organization of personal data is studied, as well as the categories of personal information subject to special protection are determined based on the study of judicial practice. The article analyzes the regulatory framework governing the sphere of personal data, taking into account recent changes in legislation regarding liability for violations in accordance with Article 13.11 of the Administrative Code of the Russian Federation and Article 272.1 of the Criminal Code of the Russian Federation. Special attention is paid to the classification of biometric data, with an emphasis on ensuring the protection of biometric information of minors, including the analysis of relevant judicial precedents.

Results. In the course of the conducted research, the specifics and conditions of the legal regulation of the protection of the institute of personal data in the Russian Federation were determined. In addition, attention is focused on improving Russian legislation regarding administrative and criminal liability for the commission of offenses of this institution.

The scope of the results. The results of the study can be used in conducting further research in the field of human rights protection.

Keywords: digitalization; protection of human rights; personal data; biometric personal data; legal protection

For citation. Piskaikina, V. M., & Monetov, A. G. (2025). The problem of personal data protection in the era of digitalization. *Russian Studies in Law and Politics*, 9(2), 124–140. <https://doi.org/10.12731/2576-9634-2025-9-2-238>

Введение

Современный этап общества знаменуется вступлением в новую фазу информационной эпохи, обусловленной всеобщей диджитализацией различных сфер социальной жизни. Как следствие, отношения между государством и гражданами претерпевают изменения и переходят в цифровой формат. Активное внедрение цифровых технологий, расширяя доступ к государственным услугам, одновременно

создает серьезные риски для безопасности личных данных граждан. Участвовавшие случаи утечек, кибератак и несанкционированного сбора информации требуют разработки эффективных механизмов защиты персональных данных на основе комплексного и междисциплинарного подхода.

Результаты и обсуждение

Статистическая информация, представленная Роскомнадзором в аналитическом отчете начала 2025 года, демонстрирует существенное возрастание масштабов нарушения конфиденциальности персональных данных граждан Российской Федерации. Количественный анализ выявленных инцидентов безопасности за 2024 год свидетельствует о компрометации более 710 миллионов записей персональных данных, произошедшей вследствие 135 документированных случаев несанкционированного доступа к информационным базам [16].

Глава комитета Государственной Думы по информационной политике, информационным технологиям и связи, Сергей Боярский, подчеркивает тревожность сложившейся ситуации и рост числа нарушений. Он считает, что усиление законодательного регулирования стимулирует компании к увеличению инвестиций в обеспечение безопасности персональных данных на своих IT-платформах [2].

Кроме того, в декабре 2021 года Совет при Президенте Российской Федерации по развитию гражданского общества и правам человека опубликовал доклад, посвященный вопросам цифровой трансформации и защиты прав граждан в цифровой среде.

Масштабная программа цифровизации, являющаяся ключевым элементом национальной стратегии развития до 2030 года, требует детальной проработки механизмов защиты конституционных прав населения через установление четких законодательных границ [1].

В Российской Федерации правовое регулирование общественных отношений в сфере защиты личной информации опирается, прежде всего, на Федеральный закон «О персональных данных». В данном законе под персональными данными понимается любая информация, прямо или косвенно относящаяся к физическому лицу, которое

идентифицировано или может быть идентифицировано [21]. Данная формулировка, отличающаяся высокой степенью абстракции, создает сложности для практического применения при определении того, какие сведения о человеке подлежат защите.

Во всяком случае, для более глубокого понимания категории персональных данных необходимо рассмотреть их классификацию:

1. по степени доступа:

- конфиденциальные данные – информация, доступ к которой ограничивается законодательством и внутренними правилами организаций;
- общедоступные данные – информация, добровольно распространенная субъектом персональных данных для неограниченного круга лиц;

2. по направлению:

- обычные данные – информация, позволяющая идентифицировать человека;
- специальные данные – категории персональных данных, включающие сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни и т.п. [15].

В свою очередь, судебная практика относит к категории защищаемых персональных данных следующие сведения о личности:

– фамилию, имя, отчество, дату и место рождения, пол, адрес места жительства, сведения из документа, удостоверяющего личность, идентификационный (регистрационный, учетный) номер налогоплательщика (при наличии) [9];

– данные о телефонах, паспортных данных, ИНН, СНИЛС, уровне заработной платы, семейном положении [4];

– номер и серия паспорта; страховой номер индивидуального лицевого счета; идентификационный номер налогоплательщика; биометрические данные; банковский счет, номер банковской карты [3].

Правовое определение биометрических данных охватывает комплекс биологических и физиологических особенностей, обеспечивающих достоверное распознавание индивидуальности человека.

Открытый характер списка биометрических признаков расширяет дискреционные полномочия правоприменительных органов при квалификации информации биометрического характера. Нормативная концепция биометрии включает широкий спектр уникальных характеристик личности, позволяющих реализовать процедуру идентификации субъекта через анализ его природных особенностей [6].

Так, по мнению «Заслуженного юриста Российской Федерации» И. Л. Бачило «...сегодня нельзя обойти проблему правового режима такого класса информации, как биоинформация: отпечатки пальцев, зрачков глаз человека, его ДНК и другие элементы индивида, широко используемые в практике идентификации субъекта в самых разных областях его жизни и отношений с другими субъектами, нуждаются в установлении их правового режима, порядка использования и защиты» [5].

С мнением профессора И. Л. Бачило о необходимости создания правового режима для биоинформации трудно не согласиться, так как уникальность биометрических данных, включая генетический код и дактилоскопические характеристики, создает повышенные риски при несанкционированном использовании персональных данных граждан. Отсутствие детальной законодательной регламентации может привести к существенным нарушениям конфиденциальности личных сведений. Правоохранительные структуры, активно применяющие биометрические базы данных, нуждаются в четких нормативных ограничениях для предупреждения противоправного распространения защищаемой информации. Формирование комплексного правового механизма регулирования биоинформации послужит укреплению взаимного доверия между обществом и государственными институтами, обеспечивая легитимность использования персональных данных.

Стоит отметить, что законодательная основа обработки биометрических данных граждан регламентируется специальным разрешительным порядком, установленным ч. 2 ст. 11 Федеральным законом №152-ФЗ [21].

Итак, Постановление Правительства РФ №772, принятое 30 июня 2018 года, определяет двухуровневую структуру биометри-

ческих данных, обязательных для внесения в единую биометрическую систему [13].

- данные изображения лица человека, полученные с помощью фото- и видео устройств;
- данные голоса человека, полученные с помощью звукозаписывающих устройств.

В настоящее время российские банки стремительно модернизируют технологии удаленного обслуживания клиентов путем внедрения биометрических систем идентификации личности [17]. Разделение биометрических характеристик и личных сведений граждан между отдельными защищенными базами данных обеспечивает максимальный уровень безопасности при осуществлении банковских операций.

В качестве примера проблемы неправомерного использования биометрической информации можно рассмотреть случай с пермской средней школой «Мастерград». Она была признана виновной по ч. 5 ст. 13.11 КоАП РФ за установку системы видеонаблюдения на входе и выходе из школы [8]. Это дело рассматривалось в кассационном суде, где не было представлено убедительных доказательств в поддержку решения. Суд не получил документального подтверждения согласия родителей или законных опекунов на сбор и использование персональных данных с помощью видеонаблюдения. Администрация школы утверждала, что такие согласия были оформлены, но не предоставила их в суд. Следовательно, школа «Мастерград» не позаботилась о получении необходимых согласий от родителей и законных представителей учеников перед внедрением системы видеонаблюдения для контроля доступа в школу [14].

Стоит отметить, что законодательство устанавливает особый порядок предоставления согласия на обработку персональных данных несовершеннолетних граждан, наделенными правом самостоятельного волеизъявления, что исключает необходимость получения дополнительного разрешения от их законных представителей.

- по общему правилу при достижении возраста 15 лет для получения медицинской помощи и трудоустройстве;

- при достижении возраста 16 лет для получения образовательных услуг;
- при признании полностью дееспособным в результате эмансипации или вступления в брак.

В свою очередь, основными видами нарушений, установленными судом при рассмотрении данной категории дел, являются:

- отсутствует письменное согласие законных представителей на обработку персональных данных несовершеннолетних;
- нормативные требования ст. 9 ФЗ №152-ФЗ «О персональных данных» относительно оформления разрешений на использование биометрической информации не соблюдаются надлежащим образом;
- локализация физических носителей с конфиденциальными данными не регламентирована соответствующими организационными мерами;
- система хранения документации с персональными сведениями несовершеннолетних граждан не обеспечивает должный уровень защиты от неправомерного доступа;
- руководством не назначен сотрудник, ответственный за обработку личной информации детей, либо уполномоченное лицо бездействует, что приводит к нарушениям регламента работы с персональными и биометрическими данными подопечных.

В дополнение, стоит привести еще несколько примеров судебной практики о нарушении персональных данных несовершеннолетних:

• «В нарушение ч. 5 ст. 5, ст. 7 Федерального закона «О персональных данных» на официальном сайте МОБУ СОШ размещены приказы о зачислении 118 детей в 1 класс с указанием фамилий, имен и отчеств. В согласиях родителей на обработку персональных данных их детей нет разрешения на опубликование персональных данных детей на сайте. Суд квалифицирует действия ... как обработку персональных данных, несовместимую с целями сбора персональных данных ...» [11];

• «Судом установлено, что ... в информационной системе «Дневник.ру» размещены персональные данные ученика 9 «Б» класса без письменного согласия его законных представителей. Исследовав и

оценив представленные доказательства, ... суд приходит к убеждению, что совершено административное правонарушение, предусмотренное ч. 2 ст. 13.11 КоАП РФ – обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации в области персональных данных...» [10];

• «На официальном сайте МБОУ СОШ в разделе «Документы» в общем доступе размещен «Публичный доклад, содержащий персональные данные учащихся и их законных представителей (фамилия, сведения о неуспевающих учениках, оставленных на 2-ой год обучения, сведения о «слабых» учениках, переведенных в 5 класс, сведения об учениках, имеющих оценку успеваемости «3» по одному предмету, сведения об учениках, не выполнявших контрольное тестирование (с указанием причин), результаты ЕГЭ (предмет, фамилия, класс, балл) учеников, набравших максимальный/минимальный балл и получивших оценку успеваемости «2», сведения о выпускнике (имя, фамилия, класс), не получившем аттестат по результатам ЕГЭ, сведения о семьях, состоящих на учете как неблагополучные, сведения об учащихся, входящих в группу риска (фамилия, информация об уходе из дома и попытке суицида), сведения об учащихся, состоящих на учете в ОДН ГУ МО МВД России с указанием фамилий и классов учащихся, в отсутствие письменного согласия несовершеннолетних и их законных представителей, что является нарушением установленного законом порядка сбора, хранения, использования и распространения информации о гражданах (персональных данных)» [12].

Также стоит отметить, что федеральное законодательство претерпело существенные изменения благодаря подписанию 30 ноября 2024 года двух значимых нормативных актов. С 30 мая 2025 года вступает в действие Федеральный закон №420-ФЗ, регламентирующий изменения в Кодексе об административных правонарушениях [19]. Федеральный закон №421-ФЗ, затрагивающий модификации Уголовного кодекса РФ, обрел юридическую силу 11 декабря 2024 года [20].

Нововведения Федерального закона №420-ФЗ существенно расширяют список правонарушений и усиливают меры административной ответственности в области защиты персональных данных [7]. Положения Федерального закона №421-ФЗ формируют отдельную категорию уголовных преступлений касательно незаконных операций с личными данными граждан.

Масштабные преобразования ст. 13.11 КоАП РФ, внесенные Федеральным законом №420-ФЗ, значительно расширяют перечень лиц, подлежащих административной ответственности, устанавливая более строгие наказания за противоправные действия с персональными данными. Законодательные нововведения существенно увеличили денежные взыскания за несанкционированную обработку персональных данных граждан при отсутствии законных оснований или несоответствии заявленным целям сбора. Данные правовые положения не распространяются на деяния, содержащие признаки уголовно наказуемых преступлений. Нормативные изменения затронули всех участников информационного взаимодействия: физических лиц, представителей органов власти и юридических лиц.

Однако, по нашему мнению, представляется спорным отождествление результатов неправомерного сбора, хранения, использования и распространения персональных данных. Все эти действия рассматриваются как равнозначные по степени негативного воздействия и размеру ущерба для субъекта персональных данных, чьи права нарушены. При этом незаконное распространение персональных данных, безусловно, представляет большую общественную опасность, чем сбор, хранение или использование. Кроме того, установленная санкция за сбор, хранение, использование или распространение персональных данных представляется недостаточной, принимая во внимание возможный существенный вред, причиняемый правам человека.

Уголовный кодекс РФ дополнен ст. 272.1, которая касается незаконного использования и (или) передачи, сбора и (или) хранения компьютерной информации, содержащей персональные данные, а также создания и (или) обеспечения функционирования информационных ресурсов, предназначенных для ее незаконного хранения

и (или) распространения. Самое строгое наказание в виде лишения свободы на срок до 10 лет со штрафом в размере до 3 млн руб. или в размере заработной платы или иного дохода осужденного за период до 4 лет, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового установлено за преступления [18].

Тем не менее, представленная статья содержит ряд потенциальных рисков, в частности:

1. Недостаточная конкретность определений. Применение формулировки «иной незаконный путь» дает возможность для расширенного толкования содержания статьи. В реальных ситуациях это может вызвать предположение о нелегальном происхождении сведений, если не будет доказан легальный способ их получения.

2. Трансграничная передача данных. Организации, прибегающие к услугам зарубежных облачных платформ или пересылающие информацию за рубеж, могут столкнуться с ощутимыми проблемами, если эти действия будут квалифицированы как противозаконные.

3. Особенности работы в сфере юриспруденции. Специалисты в области права, собирающие личную информацию для составления исков или защиты интересов заказчиков, должны проявлять повышенную бдительность. Использование источников информации с сомнительной репутацией, таких как автоматизированные системы поиска данных, теперь может повлечь за собой уголовное преследование.

4. Конкуренция с другими статьями УК РФ. Остается неясным, каким образом ст. 272.1 будет взаимодействовать со ст. 137 УК РФ, регулирующей защиту частной жизни. Вполне вероятно, что ст. 137 потеряет свою актуальность в связи с более широким охватом новой законодательной нормы.

Заключение

Подводя итоги вышеизложенному, можно сделать вывод, что стремительная эволюция общественных процессов формирует необходимость масштабного применения персональных и биометрических данных граждан. Прогрессирующая цифровизация социума,

внедрение передовых технологических решений и систем искусственного интеллекта многократно расширяют массивы обрабатываемых личных сведений. Модернизация технической инфраструктуры и законодательного фундамента защиты персональных данных требует государственного участия при сохранении баланса между инновационным развитием и обеспечением конфиденциальности. Динамичная трансформация цифрового пространства обуславливает потребность в опережающей адаптации нормативно-правовой базы для эффективного обеспечения прав граждан. Конструктивное взаимодействие государственных институтов и общественных организаций создает основу для выработки сбалансированных решений в сфере защиты персональных данных. Комплексный подход к регулированию информационной безопасности способствует формированию защищенной цифровой среды, обеспечивающей права граждан при сохранении технологического прогресса общества.

Список литературы

1. Абрамова, А. Г. (2020). Современные проблемы осуществления защиты персональных данных в сети: основополагающие принципы защиты персональных данных. *Регион и мир*, 11(4), 21–25. EDN: <https://elibrary.ru/EVEAYH>
2. Алимбаев, В. В., & Листопадова, Е. В. (2022). Организация защиты персональных данных и ответственность за несоблюдение требований законодательства в области защиты персональных данных. В сборнике: *Природа. Человек. Культура: Материалы Третьего Международного научно-просветительского форума* (с. 176–182). Кисловодск: Дальневосточный государственный университет путей сообщения. EDN: <https://elibrary.ru/UZCBTZ>
3. Апелляционное определение Новосибирского областного суда от 4 июля 2017 г. по делу № 33-6394/2017. Справочная правовая система КонсультантПлюс.
4. Апелляционное определение Санкт-Петербургского городского суда от 11 октября 2017 г. № 33-19446/2017 по делу № 2-2998/2017. Справочная правовая система КонсультантПлюс.

5. Бачило, И. Л. (2013). *Информационное право. Учебник для магистров* (3-е изд.). Москва: Юрайт. 576 с. ISBN: 978-5-9916-2677-4 EDN: <https://elibrary.ru/VTTQMR>
6. Вронская, М. В., & Виничук, П. В. (2024). Биометрические данные как объект правовой охраны и защиты: актуальные проблемы. *МНИЖ*, (142), 109. <https://doi.org/10.23670/IRJ.2024.142.109> EDN: <https://elibrary.ru/KRKPGM>
7. Занина, Т. М., & Караваев, А. А. (2013). Административная ответственность за правонарушения в сфере охраны конфиденциальной информации. *Вестник ВИ МВД России*, (3).
8. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 29.10.2024, с изм. от 06.11.2024). Справочная правовая система КонсультантПлюс.
9. Постановление Девятнадцатого арбитражного апелляционного суда от 10 марта 2017 г. № 19АП-126/2017 по делу № А48-4470/2016. Справочная правовая система КонсультантПлюс.
10. Постановление Мирowego судьи Княгининского судебного района Нижегородской области по делу № 5-521/2017. Справочная правовая система КонсультантПлюс.
11. Постановление Мирowego судьи судебного участка № 40 города Якутска Республики Саха (Якутия) по делу № 5-258/45-2018. Справочная правовая система КонсультантПлюс.
12. Постановление Мирowego судьи судебного участка № 3 г. Можга по делу № 5-44/17. Справочная правовая система КонсультантПлюс.
13. Постановление Правительства РФ от 30.06.2018 № 772 (ред. от 23.03.2024) «Об определении состава сведений, размещаемых в единой биометрической системе, в том числе в ее региональных сегментах, а также о внесении изменений в некоторые акты правительства Российской Федерации». Справочная правовая система КонсультантПлюс.
14. Постановление Седьмого кассационного суда общей юрисдикции от 24 июля 2020 г. по делу № 16-2185/2020. Справочная правовая система КонсультантПлюс.
15. Сабаева, Т. А. (2023). Биометрические персональные данные: понятие и особенности защиты. *Молодой ученый*, (50), 297–298. Получено

- с <https://moluch.ru/archive/497/109171> (дата обращения: 30.03.2025).
EDN: <https://elibrary.ru/XAVFHK>
16. Савельева, М. В. (2023). Правовая безопасность и защита персональных данных в эпоху цифровизации. В сборнике: *Государство и право: эволюция, современное состояние, перспективы развития (к 25-летию Санкт-Петербургского университета МВД России): Материалы XX международной научно-теоретической конференции* (с. 747–753). Санкт-Петербург: Санкт-Петербургский университет МВД России. EDN: <https://elibrary.ru/SADZLF>
 17. Талапина, Э. В. (2018). Защита персональных данных в цифровую эпоху. Российское право в европейском контексте. *Труды Института государства и права РАН*, 13(5), 117–150. EDN: <https://elibrary.ru/YPTTOP>
 18. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.02.2025). Справочная правовая система Консультант-Плюс.
 19. Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» от 30.11.2024 № 420-ФЗ (последняя редакция). Справочная правовая система КонсультантПлюс.
 20. Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации» от 30.11.2024 № 421-ФЗ (последняя редакция). Справочная правовая система КонсультантПлюс.
 21. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Справочная правовая система КонсультантПлюс.

References

1. Abramova, A. G. (2020). Current problems of personal data protection in the network: fundamental principles of personal data protection. *Region and the World*, 11(4), 21–25. EDN: <https://elibrary.ru/EVEAYH>
2. Alimbayev, V. V., & Listopadova, E. V. (2022). Organization of personal data protection and liability for non-compliance with the requirements of legislation on personal data protection. In *Proceedings of the Third International Scientific and Educational Forum “Nature. Man. Culture”*

- (pp. 176–182). Kislovodsk: Far Eastern State University of the Railway Transport. EDN: <https://elibrary.ru/UZCBTZ>
3. Appellate Determination of the Novosibirsk Regional Court of July 4, 2017 in case No. 33-6394/2017. *ConsultantPlus Legal Information System*.
 4. Appellate Determination of the St. Petersburg City Court of October 11, 2017 No. 33-19446/2017 in case No. 2-2998/2017. *ConsultantPlus Legal Information System*.
 5. Bachiho, I. L. (2013). *Information Law. Textbook for Master's Degree Students* (3rd ed.). Moscow: Yurayt. 576 p. ISBN: 978-5-9916-2677-4 EDN: <https://elibrary.ru/VTTQMR>
 6. Vronskaya, M. V., & Vinichuk, P. V. (2024). Biometric data as an object of legal protection and protection: current problems. *MNIZH, (142)*, 109. <https://doi.org/10.23670/IRJ.2024.142.109> EDN: <https://elibrary.ru/KRKPGM>
 7. Zanina, T. M., & Karavaev, A. A. (2013). Administrative liability for offenses in the field of confidential information protection. *Bulletin of the VI of the Ministry of Internal Affairs of Russia, (3)*.
 8. *Code of Administrative Offenses of the Russian Federation* of December 30, 2001 No. 195-FZ (as amended on October 29, 2024, with amendments as of November 6, 2024). *ConsultantPlus Legal Information System*.
 9. Decision of the Nineteenth Arbitration Appeal Court of March 10, 2017 No. 19AP-126/2017 in case No. A48-4470/2016. *ConsultantPlus Legal Information System*.
 10. Decision of the World Judge of the Knyagininsky Judicial District of the Nizhny Novgorod Region in case No. 5-521/2017. *ConsultantPlus Legal Information System*.
 11. Decision of the World Judge of the Judicial District No. 40 of the city of Yakutsk of the Republic of Sakha (Yakutia) in case No. 5-258/45-2018. *ConsultantPlus Legal Information System*.
 12. Decision of the World Judge of the Judicial District No. 3 of Mozhga in case No. 5-44/17. *ConsultantPlus Legal Information System*.
 13. Decree of the Government of the Russian Federation of June 30, 2018 No. 772 (as amended on March 23, 2024) “On the determination of the

- composition of information placed in the unified biometric system, including in its regional segments, as well as on amendments to some acts of the Government of the Russian Federation”. *ConsultantPlus Legal Information System*.
14. Decision of the Seventh Cassation Court of General Jurisdiction of July 24, 2020 in case No. 16-2185/2020. *ConsultantPlus Legal Information System*.
 15. Sabaeva, T. A. (2023). Biometric personal data: concept and protection features. *Young Scientist*, (50), 297–298. Retrieved from <https://moluch.ru/archive/497/109171> (accessed: March 30, 2025). EDN: <https://elibrary.ru/XAVFHK>
 16. Savelyeva, M. V. (2023). Legal security and protection of personal data in the era of digitalization. In *Proceedings of the XX International Scientific and Theoretical Conference “State and Law: Evolution, Current State, Prospects for Development” (dedicated to the 25th anniversary of the St. Petersburg University of the Ministry of Internal Affairs of Russia)* (pp. 747–753). Saint Petersburg: St. Petersburg University of the Ministry of Internal Affairs of Russia. EDN: <https://elibrary.ru/SADZLF>
 17. Talapina, E. V. (2018). Personal data protection in the digital age. *Russian Law in the European Context. Proceedings of the Institute of State and Law of the Russian Academy of Sciences*, 13(5), 117–150. EDN: <https://elibrary.ru/YPTTOP>
 18. *Criminal Code of the Russian Federation* of June 13, 1996 No. 63-FZ (as amended on February 28, 2025). *ConsultantPlus Legal Information System*.
 19. Federal Law “On Amendments to the Code of Administrative Offenses of the Russian Federation” of November 30, 2024 No. 420-FZ (latest edition). *ConsultantPlus Legal Information System*.
 20. Federal Law “On Amendments to the Criminal Code of the Russian Federation” of November 30, 2024 No. 421-FZ (latest edition). *ConsultantPlus Legal Information System*.
 21. Federal Law of July 27, 2006 No. 152-FZ “On Personal Data”. *ConsultantPlus Legal Information System*.

ДАННЫЕ ОБ АВТОРАХ

Пискайкина Виктория Михайловна, студент 2 курса юридического института
Рязанский государственный университет имени С. А. Есенина
ул. Семинарская, 15, г. Рязань, Рязанская область, 390000,
Российская Федерация
pvm8420@yandex.ru

Монетов Антон Геннадиевич, научный руководитель, преподаватель кафедры теории права и публично-правовых дисциплин юридического института
Рязанский государственный университет имени С. А. Есенина
ул. Семинарская, 15, г. Рязань, Рязанская область, 390000,
Российская Федерация
monetov62@mail.ru

DATA ABOUT THE AUTHORS

Victoria M. Piskaikina, 2nd year student at the Law Institute
Ryazan State University named after S. A. Yesenin
15, Seminary Str., Ryazan, Ryazan region, 390000, Russian Federation
pvm8420@yandex.ru

Anton G. Monetov, Research Supervisor, Lecturer at the Department of Theory of Law and Public Law Disciplines at the Law Institute
Ryazan State University named after S. A. Yesenin
15, Seminary Str., Ryazan, Ryazan region, 390000, Russian Federation
monetov62@mail.ru

Поступила 28.05.2025
После рецензирования 14.06.2025
Принята 19.06.2025

Received 28.05.2025
Revised 14.06.2025
Accepted 19.06.2025