

УДК 34**Проблемные аспекты доказывания по делам о преступлениях против безопасности персональных данных****Аникевич Диана Самвеловна**

Аспирант,
Российский государственный университет правосудия,
117418, Российская Федерация, Москва, ул. Новочеремушкинская, 69;
e-mail: dia.83@list.ru

Аннотация

Цифровизация общества усиливает уязвимость персональных данных, превращая их в товар для мошенничества и краж идентичности. В российском законодательстве термин "персональные данные" определен с 1997 года, а их защита закреплена в Конституции РФ и Федеральном законе № 152-ФЗ. Актуальность темы обусловлена ростом утечек данных (197 млн записей в 2022 году) и введением в 2024 году статьи 272.1 УК РФ, криминализирующей незаконное использование, передачу, сбор или хранение компьютерной информации с персональными данными. Исследование фокусируется на проблемах доказывания по таким делам, особенно на разграничении уголовных преступлений от административных правонарушений по статье 13.11 КоАП РФ. Анализ основан на изучении норм УК РФ, КоАП РФ, Федерального закона "О персональных данных" и судебной практики. Применены методы сравнительного правового анализа, моделирования ситуаций и обобщения эмпирических данных из отчетов Роскомнадзора и судебных решений. Рассмотрены случаи утечек через Telegram-боты и "даркнет". Результаты показывают конкуренцию норм: диспозиция статьи 272.1 УК РФ не содержит четких криминообразующих признаков, что приводит к неопределенности в квалификации (например, хранение данных без согласия может подпадать под обе статьи). Выявлены две группы обстоятельств для доказывания: незаконный доступ и иные способы получения данных. Обсуждение подчеркивает необходимость корректировки статьи 272.1 УК РФ для введения квалифицирующих признаков (например, извлечение выгоды) или использования административной преюдиции, как в статье 274.2 УК РФ. Это устраним правовую неопределенность и повысит эффективность расследования. Предложения способствуют усилению защиты данных в цифровой среде.

Для цитирования в научных исследованиях

Аникевич Д.С. Проблемные аспекты доказывания по делам о преступлениях против безопасности персональных данных // Вопросы российского и международного права. 2025. Том 15. № 6А. С. 164-171.

Ключевые слова

Персональные данные, уголовная ответственность, доказывание, административная преюдиция, компьютерная информация.

Введение

Цифровые реалии, окружающие современного человека, практически не оставляют места приватности личности, обостряя проблему защиты персональных данных, которые приобрели свойства товара, который покупается и продается. Указанные данные продолжают использоваться в мошеннических схемах, в каждой из которых, в зависимости от ситуации, есть свои особенности использования той или иной личной информации гражданина. Совокупная информация о конкретной личности с помощью высоких технологий и вовсе предоставляет серьезные возможности для кражи личности.

В законодательстве Российской Федерации впервые термин «персональные данные» был определен в 1997 г. в Указе Президента РФ № 188 «Об утверждении Перечня сведений конфиденциального характера».

В Конституции Российской Федерации 1993 г. приведены понятия личной и семейной тайны, тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23) и указанная информация составляет персональные данные, что корреспондируется с нормами ст. 12 Всеобщей декларации прав человека, согласно которой, никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь.

Материалы и методы исследования

Статья 150, п. 1 Гражданского кодекса РФ признает права человека на неприкосновенность частной жизни, неприкосновенность жилища, личную и семейную тайну, принадлежащие гражданину от рождения или в силу закона, неотчуждаемыми и непередаваемыми иным способом, а в п. 1 ст. 152.2 данного кодифицированного закона отмечается, что обработка любой информации о частной жизни человека без его согласия не допускается (п. 1 ст. 152.2).

При этом, право персональных данных до недавнего времени находилось только под защитой норм административного права, в частности ст.13.11 КоАП РФ (нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных), в виду отсутствия криминализации и пенализации соответствующих деяний в нормах Уголовного кодекса РФ.

Сам термин «персональный» происходит от латинского «persona» - «личность» - личный, присущий каждому отдельному индивидууму.

Постоянная корректировка законодательства в выделенной области свидетельствует о признании необходимости усиления правовой охраны указанной категории, о чем свидетельствует, в том числе, дополнение Гражданского кодекса Российской Федерации статьей 152.2, запрещающей без согласия гражданина сбор, хранение, распространение и использование любой информации о его частной жизни.

Результаты и обсуждение

Персональными данными, в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), другими словами та информация, с помощью которой в отдельности или при совокупном использовании возможно определить личность конкретного гражданина.

Федеральным законом от 30 ноября 2024 г. № 421-ФЗ, в главу 28 УК РФ введена статья

272.1, предусматривающая уголовную ответственность за использование и (или) передачу (распространение, предоставление, доступ), сбор и (или) хранение компьютерной информации, содержащей персональные данные, полученной путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование, либо иным незаконным путем, а также за создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для незаконного хранения и (или) распространения персональных данных.

Актуальность введения ст. 272 УК РФ подчеркнута в Пояснительной записке к законопроекту [Пояснительная записка к проекту Федерального закона О внесении изменений в Уголовный кодекс Российской Федерации, [www](http://www.rosstat.gov.ru)], в которой обозначается широкое распространение указанных сведений, в связи с тем, что они стали постоянным «спутником» любых коммуникаций человека в сети «Интернет», что обусловило существенный рост в их отношении противоправных действий и фактов незаконного использования личной информации при совершении различных преступлений, в том числе мошенничеств.

Число утечек таких данных с января по август 2022 года в России составило 197 млн. записей, а черный рынок персональных данных постоянно растет и предоставляется как сторонними злоумышленниками, так и самими сотрудниками компаний. На декабрь 2021 года в теневом сегменте сети «Интернет» («даркнет») циркулировало более 20 000 баз данных общим объемом более 10 Тб, содержащие персональные данные о 80 % населения России.

В связи с этим в ст. 272.1 УК РФ конкретизирован специальный объект преступного посяательства для целей уголовного законодательства - компьютерная информация, содержащая персональные данные, полученная незаконным путем, посредством неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование, либо иным незаконным путем.

Серьезные основания для борьбы с незаконным оборотом компьютерной информацией, содержащей персональные данные в России стали возникать в 2020 году, когда в ресурсах сети «Интернет», таких как «Telegram» стали функционировать боты, позволяющие любому желающему за плату получить персональные данные широкого круга граждан. Ранее такие возможности были доступны спецслужбам либо лицам, обладающим специальными навыками при использовании «даркнета».

Даркнет (или Tor) – это скрытая (теневая) часть «Всемирной паутины», состоящая из связанных между собой виртуальных и зашифрованных туннелей, в которых пользователь остается полностью зашифрованным, доступ к которой нельзя получить при помощи обычных сетевых программ. Соединения «даркнет» устанавливаются только между доверенными лицами или «друзьями» при использовании засекреченных протоколов и портов.

В 2020 году стало возможно получать такую информацию в одном из самых известных «Telegram-каналах», так называемом «Глаз Бога», где любой желающий за считанные секунды и за небольшую оплату мог получить информацию самого широкого периметра (место работы, данные документов, удостоверяющих личность, регистрационные номера автомобилей, место регистрации, контактные лица в социальных сетях и др.). Для правоохранительных органов являлось очевидным, что базы данных созданы на основании «утечек» и незаконных «сбытов» персональных данных, однако такие действия не попадали в ряд криминализированных деяний, соответственно и механизмы противодействия им уголовно-правовыми методами отсутствовали.

01 марта 2021 г. года вступили в силу поправки к Федеральному закону «О персональных данных», запрещающие последующую обработку общедоступных персональных данных без наличия на то законных оснований и 30 июня 2021 г. последовало обращение Федеральной

службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) в Таганский суд города Москвы [Решение Таганского районного суда города Москвы от 01 июля 2021 г. по делу 2-2418/2021] с требованием признать деятельность интернет-ресурса, который на тот момент насчитывал порядка 850 тысяч подписчиков, незаконной и нарушающей права граждан на неприкосновенность частной жизни, личную и семейную тайну, которые судом были удовлетворены. Федеральным законом от 30.12.2020 N 519-ФЗ, Федеральный закон «О персональных данных» дополнен статьей 10.1. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения, определяющей обязанность любого оператора (лица) предоставить доказательства законности последующего распространения или иной обработки персональных данных, раскрытых неопределенному кругу лиц самим субъектом персональных данных без предоставления оператору согласия (ч. 2 ст. 10.1), а также обязанность таких лиц предоставить доказательства законности последующего распространения персональных данных, оказавшихся раскрытыми неопределенному кругу лиц вследствие правонарушения, преступления или обстоятельств непреодолимой силы (ч. 3 ст. 10.1).

В дальнейшем, путем смены «бота» сервис быстро был перенесен на другой информационный ресурс и функционировал вплоть до начала 2025 года, когда у правоохранительной системы, на основании введенной ст. 272.1 УК РФ появилась возможность эффективно бороться с подобными нарушениями.

Как видется цель нормы ст. 272.1 УК РФ заключается в пресечении компьютерных преступлений, связанных с утечками и торговлей персональными данными, но не в привлечении к уголовной ответственности представителей бизнеса-операторов, допустивших обработку персональных данных в нарушение норм Федерального закона «О персональных данных».

За короткий период действия ст. 272 УК РФ практика доказывания и рассмотрения дел в суде не сформирована. Из данных, опубликованных на официальном сайте судов общей юрисдикции города Москвы известно о трех удовлетворенных судами ходатайствах о производстве обыска в жилище и одном удовлетворенном ходатайстве об избрании меры пресечения в виде заключения под стражу в рамках уголовного судопроизводства по ст. 272.1 УК РФ.

Вместе с тем, уже сейчас при исследовании и сопоставлении юридических ситуаций, возникающий при применении института доказывания по смежным составам административных правонарушений, предусмотренных ст. 13.11 Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ) с целью анализа и оценки эффективности построения модели доказывания и судебного рассмотрения уголовных дел о преступлениях, предусмотренных ст. 272 УК РФ, возможно выделение проблемной области, в частности сложность разграничения состава ст. 272.1 УК РФ от правонарушений, ответственность за которые предусмотрена ст. 13.11 КоАП РФ.

На указанное обстоятельство было обращено внимание в отзыве Верховного Суда РФ от 11.01.2023 на законопроект [Отзыв Верховного Суда Российской Федерации к проекту Федерального закона О внесении изменений в Уголовный кодекс Российской Федерации, [www](http://www.rosstat.gov.ru)], в котором подчеркнута, конкуренция ст. 272.1 УК РФ и ст. 13.11 КоАП РФ, предусматривающей административную ответственность за нарушения требований законодательства РФ в области персональных данных, в том числе связанных с обработкой таких данных, что охватывает незаконные сбор, хранение, использование и передачу как самих персональных данных, так и баз, включающих такие данные, если деяние не содержит какие-либо дополнительные признаки, повышающие его общественную опасность, например, предусмотренные частью 2 ст.

272.1 УК РФ.

В то же время, в диспозиции части 1 ст. 272.1 УК РФ отсутствует криминообразующие признаки, позволяющие отграничивать соответствующее преступление от противоправных действий, предусмотренных ст. 13.11 КоАП РФ, что может привести к конкуренции данного уголовно-правового запрета со ст. 13.11 КоАП РФ и существенно усложнить применение нормы на практике.

Действительно часть 1 ст. 13.11 КоАП РФ устанавливает административную ответственность в отношении граждан, должностных и юридических лиц за обработку персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработку, несовместимую с целями сбора персональных данных, за исключением случаев, если эти действия не содержат уголовно наказуемого деяния.

В то же время, часть 1 ст. 272.1 УК РФ предусматривает уголовную ответственность за незаконные использование и (или) передачу (распространение, предоставление, доступ), сбор и (или) хранение компьютерной информации, содержащей персональные данные, полученной путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование либо иным незаконным путем.

Без дополнительных разъяснений высших судебных инстанций о порядке применения ст. 272.1 УК РФ, которые в настоящее время отсутствуют, провести разграничение двух однородных формулировок «сбор незаконным путем персональных данных» от их «обработки в случаях не предусмотренных законодательством РФ», сложно решаемая задача, потому как обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение и т.д. (п. 3 ст. 3 Федерального закона «О персональных данных»).

С учетом действующей конструкции диспозиции ст. 272.1 УК РФ, обстоятельствами, обязательными для доказывания, будут являться две группы фактов, подтверждающих доступ к компьютерной информации, содержащей персональные данные: первые, связаны с незаконным доступом к охраняемой законом компьютерной информации, содержащей персональные данные (путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование); вторые, получение иным незаконным путем указанной компьютерной информации (кроме получения путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование).

Установив обстоятельства одной из двух группы фактов доступа к компьютерной информации, содержащей персональные данные, далее доказыванию подлежат обстоятельства использования и (или) передачи (распространения, предоставления, доступа), сбора и (или) хранения компьютерной информации, содержащей персональные данные, полученной одним из вышеуказанных двух способов.

На примере смоделированной ситуации, когда оператор, являющийся работодателем, на своем информационном ресурсе в информационной системе может хранить компьютерную информацию, содержащую персональные данные работников, без получения от них согласий на обработку персональных данных (количественные характеристики этих данных в рассматриваемом составе не имеют правового значения, поскольку не выделены в качестве криминообразующих признаков), в случаях, когда такое согласие должно быть получено на основании требований ст. 6 Федерального закона «О персональных данных», по мнению автора настоящей работы, будут образовывать состав преступления, предусмотренного ч. 1 ст. 272.1

УК РФ, поскольку в рассматриваемом случае незаконно полученные персональные данные хранятся в виде компьютерной информации.

Эти же действия при обработке персональных данных, т.е. их хранение в информационной системе без наличия согласия субъекта персональных данных также образуют состав административного правонарушения, предусмотренного ст. 13.11 КоАП РФ.

Таким образом, позиция Верховного суда РФ, представленная к законопроекту, на наш взгляд не была проработана, что действительно создает правовую неопределенность об отраслевой принадлежности рассматриваемых деяний, и может повлечь проблемы в правоприменительной практике при доказывании деяний, подпадающих под признаки состава преступления, предусмотренного ст. 272.1 УК РФ.

Вектор ужесточения законодательного регулирования оборота персональных данных, безусловно является своевременной и необходимой мерой борьбы с противоправными деяниями в этой сфере, однако, с учетом выделенной проблемной области, детерминантом преступления от административных правонарушений должны являться четко определяемые конкретные признаки уголовно-наказуемого деяния, например направленность деяния на извлечение выгод и преимуществ для себя или третьих лиц, что требует корректировки криминообразующих признаков ст. 272.1 УК РФ.

Заключение

Для разрешения указанной сложности, состав анализируемого преступления возможно сконструировать с использованием института административной преюдиции.

Согласно ст. 90 УПК РФ под преюдицией понимаются обстоятельства, установленные вступившим в законную силу приговором либо иным вступившим в законную силу решением суда, принятым в рамках гражданского, арбитражного или административного судопроизводства, которые признаются судом, прокурором, следователем, дознавателем без дополнительной проверки.

При конструировании ст. 272.1 УК РФ указанным способом, привлечение к уголовной ответственности будет возможно только при повторном и последующих нарушениях, что возможно отследить на примере ст. 274.2 УК РФ (нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования) также расположенной в гл. 28 УК РФ (преступления в сфере компьютерной информации).

Состав ст. 274.2 УК РФ предполагает возможность привлечения к уголовной ответственности только специального субъекта, подвергнутого административному наказанию за деяние, предусмотренное ч. 2 ст. 13.42 КоАП РФ, а по ч. 2 рассматриваемого состава, субъект преступления, подвергнутого административному наказанию за деяние, предусмотренное ч. 2 ст. 13.42.1 КоАП РФ.

Библиография

1. Об утверждении Перечня сведений конфиденциального характера : Указ Президента РФ от 06 марта 1997 г. № 188 // Официальный сайт Президента Российской Федерации . – URL: <http://www.kremlin.ru/acts/bank/10638> (дата обращения: 26.05.2024).
2. Словарь иностранных слов, вошедших в состав русского языка : Материалы для лексической разработки заимствованных слов в рус. Лит. Речи / Сост. под ред. А.Н. Чудинова. – Санкт-Петербург : В.И. Губинский,

1984. – [4], IV, 989, III. С.24.
3. О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон от 30 ноября 2024 г. № 421-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://publication.pravo.gov.ru/document/0001202411300012> (дата обращения, 22.02.2025).
 4. Пояснительная записка к проекту Федерального закона №502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации»: Официальный сайт Государственной Думы РФ. – URL: <https://sozd.duma.gov.ru/bill/502113-8> (дата обращения: 12.01.2025).
 5. РБК-новости. URL: https://www.rbc.ru/technology_and_media/28/02/2025/67c193df9a79475db21f4068 (дата обращения: 01.03.2025).
 6. Федеральным законом от 30.12.2020 N 519-ФЗ, Федеральный закон «О персональных данных» дополнен статьей 10.1. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения, определяющей обязанность любого оператора (лица) предоставить доказательства законности последующего распространения или иной обработки персональных данных, раскрытых неопределенному кругу лиц самим субъектом персональных данных без предоставления оператору согласия (ч. 2 ст. 10.1), а также обязанность таких лиц предоставить доказательства законности последующего распространения персональных данных, оказавшихся раскрытыми неопределенному кругу лиц вследствие правонарушения, преступления или обстоятельств непреодолимой силы (ч. 3 ст. 10.1).
 7. Решение Таганского районного суда города Москвы от 01 июля 2021 г. по делу 2-2418/2021 // Государственная автоматизированная система Российской Федерации Правосудие. – URL: <https://mosgorsud.ru/rs/taganskij/services/cases/civil/details/ed015251-d385-11eb-a05e-a51ff7a5cadf?caseNumber=2-2418/2021> (дата обращения 12.04.2023)
 8. Отзыв Верховного Суда Российской Федерации к проекту Федерального закона №502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации» : Официальный сайт Государственной Думы РФ. – URL: <https://sozd.duma.gov.ru/bill/502113-8> (дата обращения: 22.03.2025).

Problematic Aspects of Proving in Cases of Crimes Against Personal Data Security

Diana S. Anikevich

Graduate Student,
Russian State University of Justice,
117418, 69 Novocheremushkinskaya str., Moscow, Russian Federation;
e-mail: dia.83@list.ru

Abstract

The digitalization of society increases the vulnerability of personal data, turning it into a commodity for fraud and identity theft. In Russian legislation, the term "personal data" has been defined since 1997, and its protection is enshrined in the Constitution of the Russian Federation and Federal Law No. 152-FZ. The relevance of the topic is due to the increase in data leaks (197 million records in 2022) and the introduction in 2024 of Article 272.1 of the Criminal Code of the Russian Federation, which criminalizes the illegal use, transfer, collection, or storage of computer information containing personal data. The study focuses on the problems of proving such cases, particularly on distinguishing criminal offenses from administrative offenses under Article 13.11 of the Code of Administrative Offenses of the Russian Federation. The analysis is based on the study of the norms of the Criminal Code of the Russian Federation, the Code of Administrative Offenses of the Russian Federation, the Federal Law "On Personal Data," and judicial practice. Methods of comparative legal analysis, situational modeling, and generalization of empirical data from reports of Roskomnadzor and court decisions were applied. Cases of leaks through Telegram bots and the

"darknet" were considered. The results show competition between norms: the disposition of Article 272.1 of the Criminal Code of the Russian Federation does not contain clear criminogenic features, which leads to uncertainty in qualification (for example, storing data without consent may fall under both articles). Two groups of circumstances to be proven were identified: illegal access and other methods of obtaining data. The discussion emphasizes the need to adjust Article 272.1 of the Criminal Code of the Russian Federation to introduce qualifying features (for example, deriving benefits) or to use administrative prejudiciality, as in Article 274.2 of the Criminal Code of the Russian Federation. This would eliminate legal uncertainty and increase the effectiveness of investigations. The proposals contribute to strengthening data protection in the digital environment.

For citation

Anikevich D.S. (2025) Problemnyye aspekty dokazyvaniya po delam o prestupleniyakh protiv bezopasnosti personal'nykh dannykh [Problematic Aspects of Proving in Cases of Crimes Against Personal Data Security]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (6A), pp. 164-171.

Keywords

Personal data, criminal liability, proving, administrative prejudiciality, computer information.

References

1. On approval of the List of confidential information : Decree of the President of the Russian Federation dated March 06, 1997 No. 188 // Official website of the President of the Russian Federation. – URL: <http://www.kremlin.ru/acts/bank/10638> (date of reference: 05/26/2024).
2. Dictionary of foreign words included in the Russian language : Materials for the lexical development of borrowed words in Russian. Lit. Speeches / Comp. edited by A.N. Chudinov. Saint Petersburg : V.I. Gubinsky, 1984. [4], IV, 989, III. p.24.
3. On Amendments to the Criminal Code of the Russian Federation : Federal Law No. 421-FZ of November 30, 2024 // Official Internet Portal of Legal Information. – URL: <http://publication.pravo.gov.ru/document/0001202411300012> (date of application, 02/22/2025).
4. Explanatory Note to the draft Federal Law No. 502113-8 "On Amendments to the Criminal Code of the Russian Federation": Official website of the State Duma of the Russian Federation. – URL: <https://sozd.duma.gov.ru/bill/502113-8> (date of request: 12.01.2025).
5. RBC-news. URL: https://www.rbc.ru/technology_and_media/28/02/2025/67c193df9a79475db21f4068 (date of request: 03/01/2025).
6. Federal Law No. 519-FZ of 12/30/2020, the Federal Law "On Personal Data" was supplemented by Article 10.1. Specifics of processing personal data authorized by a personal data subject for dissemination, which defines the obligation of any operator (person) to provide evidence of the legality of subsequent dissemination or other processing of personal data disclosed to an unspecified group of persons by the personal data subject himself without giving the operator consent (part 2 of art. 10.1), as well as the obligation of such persons to provide evidence of the legality of the subsequent dissemination of personal data disclosed to an unspecified group of persons as a result of an offense, crime, or force majeure (Part 3 of Article 10.1).
7. Decision of the Tagansky District Court of Moscow dated July 01, 2021 in case 2-2418/2021 // The State automated system of the Russian Federation Justice. – URL: <https://mosgorsud.ru/rs/taganskij/services/cases/civil/details/ed015251-d385-11eb-a05e-a51ff7a5cadf?caseNumber=2-2418/2021> (accessed 12.04.2023)
8. Review of the Supreme Court of the Russian Federation on the draft Federal Law No. 502113-8 "On Amendments to the Criminal Code of the Russian Federation" : Official website of the State Duma of the Russian Federation. – URL: <https://sozd.duma.gov.ru/bill/502113-8> (date of request: 03/22/2025).