

Персональные данные как объект и предмет преступного посягательства

5.1.4 — Уголовно-правовые науки

Диана Нурмагомедовна Алиева¹, Надир Маликович Сафаралиев²

^{1,2} Дагестанский государственный университет, Махачкала, Российская Федерация

¹ *kurbanova.diana2020@mail.ru*

² *nadir-safaraliev@mail.ru*

Аннотация. В статье рассматриваются персональные данные как объект уголовно-правовой охраны. Актуальность исследования обусловлена постоянным ростом объемов обработки персональной информации в сети Интернет и расширением сфер ее использования. Отсутствие в уголовном законодательстве критериев категории персональных данных и специальных составов преступлений порождает сложности в квалификации деяний. Методологическую основу исследования составили общенаучные и специальные методы познания: анализ и синтез, формально-юридический, сравнительно-правовой и системный методы, анализ судебной практики. В работе использованы положения международных актов, российского законодательства, доктрины и материалы судебной практики. В результате исследования обосновано положение о самостоятельном характере объекта уголовно-правовой охраны персональных данных, отличном от объекта конкретного преступления. Выявлена тенденция к функциональному толкованию персональных данных в судебной практике. Разработаны критерии и методология разграничения смежных составов преступлений, в том числе ст. 137 и 183 УК РФ, уголовной и административной ответственности по ст. 272.1 УК РФ и ст. 13.11 КоАП РФ.

Ключевые слова: персональные данные, статья 137 УК РФ, статья 183 УК РФ, статья 13.11 КоАП РФ, конкуренция норм административного и уголовного закона, методика квалификации деяния

Для цитирования: Алиева Д.Н., Сафаралиев Н.М. Персональные данные как объект и предмет преступного посягательства // Юридический вестник ДГУ. 2026. Т. 58, № 2 (78). С.110–118. DOI: 10.21779/2224-0241-2026-58-2-110-118

Original article

Personal data as an object and subject of a criminal attack Abstract

5.1.4 — Criminal law sciences

Diana N. Aliyeva¹, Nadir M. Safaraliev²

^{1,2} Dagestan State University, Makhachkala, Russian Federation

¹ *kurbanova.diana2020@mail.ru*

² *nadir-safaraliev@mail.ru*

Abstract. The article considers personal data as an object of criminal law protection. The relevance of the research is due to the growing volume of personal information processing on the Internet and the expansion of its use. The absence in criminal legislation of clearly defined boundaries of the category of personal data and special types of crimes creates difficulties in law enforcement and qualification of acts. The methodological basis of the research was made up of general scientific and special methods of cognition: analysis and synthesis, formal legal, comparative legal and systematic methods, as well as analysis of judicial practice. The work uses the provisions of international acts, Russian legislation, doctrinal approaches and materials of law enforcement activities of courts of general jurisdiction. As a result of the conducted research, the provision on the independent nature of the object of criminal legal protection of personal data, which differs from the object of a specific crime, is substantiated. The tendency towards the functional interpretation of personal data in judicial practice has been revealed. Criteria and methodology for distinguishing related crimes have been developed, including articles 137 and 183 of the Criminal Code of the Russian Federation, as well as criminal and administrative liability under articles 272.1 of the Criminal Code of the Russian Federation and 13.11 of the Administrative Code of the Russian Federation.

Keywords: personal data, Article 137 of the Criminal Code of the Russian Federation, Article 183 of the Criminal Code of the Russian Federation, Article 13.11 of the Code of Administrative Offenses of the Russian Federation, competition of administrative and criminal law norms, methodology for qualifying an act

For citation: Aliyeva D.N., Safaraliev N.M. Personal data as an object and subject of a criminal attack Abstract. *Yuridicheskii vestnik DGU = Law Herald of DSU*, 2026, vol. 58, no. 2 (78), pp. 110–118. DOI: 10.21779/2224-0241-2026-58-2-110-118. (In Russ.).

По состоянию на конец 2025 года, согласно по данным компании Mediascope, доступ к сети Интернет в Российской Федерации имели примерно 105 миллионов человек, то есть примерно 86 % населения в возрасте старше двенадцати лет. При этом число пользователей, выходящих в сеть на ежедневной основе, достигало 103 миллионов человек. Долгое время в сети расходовалось на использование социальных медиа и коммуникационных сервисов, наиболее востребованными среди которых оставались платформы «ВКонтакте», TikTok и «Дзен», мессенджеры WhatsApp, Telegram и MAX. Функционирование цифровых сервисов напрямую связано с обработкой и хранением персональных данных пользователей в электронной форме, что обусловлено техническими и правовыми особенностями их работы¹.

В современных условиях полноценное участие лица в интернет-взаимодействиях практически невозможно без предоставления персональных данных, поскольку они используются для идентификации пользователя и расширения функциональных возможностей сервисов, в том числе подтверждения платежеспособности и обеспечения безопасности операций. В результате возрастает значимость вопросов, связанных с обеспечением надлежащей уголовно-правовой охраны персональных данных, предотвращением их неправомерного оборота и использования соответствующей информации в противоправных целях. Научная новизна работы заключается в разработке конкретных критериев разграничения смежных составов противоправных деяний и методологии квалификации по признаку объекта посягательства.

При подготовке публикации были использованы нормативные правовые акты, регламентирующие вопросы обработки персональных данных и ответственность за нарушение законодательства о персональных данных, судебная практика по использованию понятия персональных данных, и положения, сформулированные доктриной. Предмет исследования с учетом объема работы, сведен к сравнительному анализу статей 137 и 183 УК РФ и ст. 13.11 КоАП РФ по объекту посягательства и к выявлению методик разграничения.

Анализ положений Конституции РФ позволяет прийти к выводу о наличии в ней конституционных гарантий защиты персональных данных, несмотря на отсутствие прямого упоминания термина. Норма ст. 24 Конституции РФ закрепляет запрет на сбор, хранение, использование и распро-

странение сведений, относящихся к частной жизни лица, без его согласия². Тем самым конституционно-правовая охрана частной жизни выступает основой для последующего формирования правового режима персональных данных.

Категория «частная жизнь» в доктрине традиционно рассматривается как более широкое понятие, содержащее в себе и персональные данные. Еще до принятия специального федерального закона, посвященного регулированию соответствующих общественных отношений, И.Л. Бачило в научных трудах раскрывает содержание личной и семейной тайны и характеризует персональные данные как совокупность сведений и документов, удостоверяющих личность гражданина и отражающих его индивидуальные характеристики, в том числе данные о месте рождения и проживания, семейном положении, профессиональной ориентации и аттестации, а также иные сведения, предусмотренные законодательством и необходимые для полноценной реализации прав и свобод человека и гражданина в рамках национального и международного правопорядка [1, с. 89].

На международном уровне категория персональных данных впервые получила концептуальное оформление в Директиве «О защите неприкосновенности частной жизни и международных обменов персональными данными» от 23 сентября 1980 года³. Нормативный акт сыграл значимую роль в формировании единой позиции по правовому регулированию информационных процессов. В документе персональные данные трактовались как любая информация, относящаяся к конкретному индивиду, личность которого является установленной. В дальнейшем это заложило основу для дальнейшего развития соответствующего правового института в международной практике.

Дальнейшее закрепление указанной категории произошло в рамках Конвенции о защите физических лиц при автоматизированной обработке персональных данных, подписанной в Страсбурге 28 января 1981 года. Конвенция стала основополагающим международно-правовым актом, оказавшим существенное влияние на национальные зако-

² Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г., с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 г.) // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru> (дата обращения: 04.07.2020).

³ О защите неприкосновенности частной жизни и международных обменов персональными данными: директива ОЭСР от 23 сентября 1980 г. URL: http://www.uipdp.com/upload/legislation/international/directive_oesr1.pdf (дата обращения: 19.01.2026).

¹ Итоги 2025 года: как развивались ИТ-сфера и интернет-рынок в России. URL: <https://www.ridus.ru/itogi-2025-goda-kak-razvivayas-it-sfera-i-internet-rynok-v-rossii-771003.html> (дата обращения: 19.01.2026).

нодательства большинства государств, независимо от их формального участия в данном соглашении. Положения этого документа легли в основу формирования универсальных стандартов защиты персональной информации в условиях развития автоматизированных способов ее обработки.

В Конвенции под персональными данными понимается информация, относящаяся к определенному либо поддающемуся определению физическому лицу, которое рассматривается как субъект данных¹. Тем самым был закреплен функциональный критерий идентифицируемости личности, позволяющий отграничивать персональные данные от иных видов информации и обеспечивать их особый правовой режим в системе защиты прав и свобод человека.

Термин «персональные данные» был внедрен в российскую правовую систему сравнительно поздно. Его нормативное закрепление впервые произошло в Федеральном законе 1995 года «Об информации, информатизации и защите информации»², в котором персональные данные рассматривались как сведения о гражданах, отнесенные к конфиденциальной информации. Закон устанавливает общее правило, согласно которому любые действия по сбору, хранению, использованию и распространению информации, затрагивающей частную жизнь лица и нарушающей личную, семейную тайну и тайну переписки и иных сообщений, допускаются исключительно с согласия соответствующего субъекта либо на основании судебного решения. Вместе с тем, из содержания данного нормативного акта следовало, что конкретизация состава персональных данных должна осуществляться на уровне федерального закона (ч. 1 ст. 11). Однако на практике правовое регулирование было реализовано посредством подзаконного акта – Указа Президента Российской Федерации от 6 марта 1997 года № 188³, в котором персональные данные определялись как сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие установить его личность. Из сказанного можно сделать вывод о формировании правового режима персональных данных преимущественно административно-правовыми средствами на первоначальном этапе развития соответствующего института.

Определение персональных данных закреплено в статье 3 действующего Федерального закона «О персональных данных», согласно которому

к ним относится любая информация, имеющая отношение к физическому лицу, которое может быть установлено прямо либо опосредованно и выступает субъектом соответствующих данных⁴. В основу правового регулирования положена позиция, ориентированная на возможность идентификации личности на основании имеющейся информации.

Первоначальная редакция упомянутого федерального закона характеризовалась значительно более детализированным и казуистичным изложением рассматриваемого понятия. В ней персональные данные раскрывались через перечисление различных видов сведений, позволяющих установить личность субъекта, в том числе данные, содержащиеся в официальных документах, удостоверяющих личность, и информацию о гражданском состоянии, месте проживания, социальном и имущественном положении, уровне образования, профессиональной деятельности, доходах и иных характеристиках, способных индивидуализировать физическое лицо⁵.

Переход к более обобщенной формуле определения персональных данных свидетельствует о развитии законодательства в сторону новых способов сбора, хранения и обработки информации. В этой связи особую актуальность приобретает дальнейшее совершенствование правовых механизмов обеспечения безопасности персональных данных в сети Интернет, которое обусловлено масштабной цифровизацией общественных отношений. Указанная задача реализуется, в том числе, в рамках Программы «Цифровая экономика Российской Федерации»⁶, положения которой ориентированы на формирование современной нормативно-правовой базы, регулирующей обработку больших массивов данных, включая сведения персонального характера, с учетом рисков, связанных с их неправомерным использованием и распространением в цифровой среде.

Анализ судебной практики позволяет сделать обобщенные выводы о том, как интерпретируется категория «персональные данные». Прежде всего, суды последовательно исходят из максимально широкого понимания персональных данных как любых сведений, позволяющих идентифицировать конкретное физическое лицо либо относящихся к его частной жизни. К примеру, в решении Центрального районного суда г. Читы от 23 июня 2025 г. по делу № 2А-3254/2025 суд относит к персональным данным и анкетные сведения, и информацию, раскры-

¹ Конвенция о защите физических лиц при автоматизированной обработке персональных данных: заключена в г. Страсбурге 28.01.1981 г. // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>. (дата обращения: 19.01.2026).

² Об информации, информатизации и защите информации: Федеральный закон (утратил силу) от 20.02.1995 г. №24-ФЗ // СЗ РФ. 1995. №8, ст. 609.

³ Об утверждении перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 г. №188 // СЗ РФ. 1997. №10, ст. 1127.

⁴ О персональных данных: Федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. от 24.06.2025 г.) // СЗ РФ. 2006. № 31 (ч. I), ст. 3451.

⁵ О персональных данных: Федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. от 24.06.2025 г.) // СЗ РФ. 2006. № 31 (ч. I), ст. 3451.

⁶ Об утверждении программы «Цифровая экономика Российской Федерации»: распоряжение Правительства РФ от 28.07.2017 г. № 1632-р // СЗ РФ. 2017. № 32, ст. 5138.

вающую принадлежность лица к определенной социальной или профессиональной группе, в частности, сведения о личном составе Вооруженных Сил Российской Федерации. Суд признал данные объектом правовой охраны вне зависимости от формы их распространения в сети Интернет¹.

Советский городской суд Калининградской области в приговоре от 10 июня 2025 г. по делу № 1-37/2025 указал, что сведениями, содержащими в ведомственных информационных системах МВД России – паспортные данные, адреса регистрации и проживания, информация о транспортных средствах, контактных номерах телефонов, данные о привлечении к ответственности, – являются совокупность персональных данных, относящихся к частной жизни гражданина и подлежащих особой правовой охране. Суд отметил, что служебный доступ к сведениям не исключает их персонального характера и не устраняет необходимости соблюдения режима конфиденциальности².

Городецкий городской суд Нижегородской области в постановлении от 27 марта 2025 г. по делу № 1-66/2025 признал персональными данными установочные сведения пациента, фамилию, имя, отчество и адрес проживания, указав, что данные одновременно составляют врачебную тайну и личную и семейную тайну даже после смерти лица. Тем самым суд подтвердил, что персональные данные могут сохранять охраняемый характер, даже если их распространение затрагивает права и законные интересы близких родственников³.

Особо показательной является позиция Перовского районного суда г. Москвы, выраженная в приговоре от 17 марта 2025 г. по делу № 01-0170/2025, в котором паспортные данные и сведения об адресе регистрации и проживания абонента оператора связи были квалифицированы как персональные данные, составляющие личную тайну. Суд связал неправомерный доступ к компьютерной информации с последующим незаконным оборотом персональных данных, выделив их самостоятельную ценность как объекта уголовно-правовой охраны независимо от целей их использования⁴.

Судебная практика позволяет сделать вывод о том, что суды воспринимают персональные данные как межотраслевую правовую категорию, охватывающую любые сведения, способные идентифицировать личность либо раскрыть элементы ее частной жизни. Вместе с тем, определяющим критерием признания информации персональными данными, выступает не источник их получения и не форма фиксации, а потенциальная возможность установления конкретного субъекта и причинения вреда его правам и законным интересам. Данный вывод подтверждает тенденцию к функциональному толкованию персональных данных в судебной практике.

Следовательно, проблематика уголовно-правовой охраны персональных данных и, вместе с тем, актуальность выбранной темы, во многом обусловлены неопределенностью и многообразием содержания данной категории, а также объективной необходимостью идентификации личности в большинстве сфер общественной жизни. Современные социальные и цифровые процессы предполагают постоянное раскрытие и использование сведений и позволяют установить личность субъекта, что существенно расширяет круг информации, подпадающей под режим персональных данных. В результате границы данного правового объекта приобретают размытый характер и затрудняют его нормативное закрепление.

Тематика признания персональных данных объектом уголовно-правовой охраны в доктрине остается дискуссионной, поскольку сама категория объекта уголовно-правовой охраны традиционно раскрывается через призму охраняемых уголовным законом общественных отношений, которым в результате совершения преступления причиняется либо может быть причинен вред. Позиция является устоявшейся в теории уголовного права и приводит к сближению понятий объекта уголовно-правовой охраны и объекта преступления [2, с. 29, 31].

В рамках упомянутого понимания нередко утверждается, что между указанными категориями отсутствуют принципиальные различия. Е.К. Каиржанов исходил из совпадения объекта уголовно-правовой охраны и объекта преступления по своему объему, поскольку в обоих случаях речь идет об одних и тех же общественных отношениях, поставленных под защиту уголовного закона [3, с. 22].

Иной точки зрения придерживался Н.И. Коржанский, который усматривал различие между объектом уголовно-правовой охраны и объектом преступления в факте наличия либо отсутствия преступного посяательства. По его мнению, объект уголовно-правовой охраны представляет собой общественное отношение, находящееся под защитой уголовного закона, но еще не подвергшееся противоправному воздействию, тогда как объект преступления – это уже нарушенное или измененное в результате преступного деяния общественное отношение [4, с. 116]. Разграничение носит дина-

¹ Решение Центрального районного суда г. Читы от 23 июня 2025 г. по делу № 2А-3254/2025. URL: sudact.ru/regular/doc/ovzfsqnQmcm0/ (дата обращения: 18.01.2026).

² Приговор Советского городского суда от 10 июня 2025 г. по делу № 1-37/2025. URL: sudact.ru/regular/doc/BD5yJL9B3cLJ/ (дата обращения: 18.01.2026).

³ Постановление Городецкого городского суда от 27 марта 2025 г. по делу № 1-66/2025. URL: sudact.ru/regular/doc/12W126SYCxdn/ (дата обращения: 17.01.2026).

⁴ Приговор Перовского районного суда г. Москвы от 17 марта 2025 г. по делу № 01-0170/2025. URL: sudact.ru/regular/doc/Bd7cxJEe3xoR/ (дата обращения: 17.01.2026).

мический характер и связано со стадией реализации уголовно-правового запрета.

В то же время в современной уголовно-правовой доктрине сформировались и противоположные концепции, согласно которым объект уголовно-правовой охраны и объект преступления не являются тождественными категориями. Так, Л.Д. Гаухман отмечал, что «понятие «объект уголовно-правовой охраны» и «объект преступления» – понятия неодинаковые по своему значению, даже несмотря на то, что в основе их обоих лежит категория «общественные отношения. Первое дает лишь общее представление о круге общественных отношений, защищаемых уголовным законом, имеет общесоциальное значение. Второе имеет уголовно-правовое значение, так как характеризует элемент состава преступления» [5, с. 64].

Видится, что деяние не может признаваться преступным в случае, если оно посягает на сферу общественных отношений, не поставленных под защиту уголовного закона. В связи с этим объект уголовно-правовой охраны существует автономно, независимо от факта совершения конкретного преступного посягательства, тогда как объект преступления возникает исключительно в результате реализации общественно опасного деяния, запрещенного уголовным законом.

Объект уголовно-правовой охраны соотносится с категорией объекта особой охраны, поскольку именно через его закрепление в уголовном законодательстве обеспечивается возможность реагирования государства на наиболее опасные формы нарушения общественных отношений.

Персональные данные как специфический вид информации во многих случаях выступают необходимым условием реализации субъектом своих прав и свобод, поскольку участие в правоотношениях предполагает обязательную идентификацию личности и ее индивидуализацию по отношению к иным участникам. Общественные отношения в сфере установленного законом оборота персональных данных подвержены повышенным рискам противоправного воздействия, в связи с чем возникает необходимость их признания объектом уголовно-правовой охраны.

В тех случаях, когда личность выступает объектом преступного посягательства, обеспечение неприкосновенности ее персональных данных приобретает особую значимость, а наличие в уголовном законе норм, устанавливающих ответственность за соответствующие деяния, свидетельствует о формировании обособленного и усиленного режима правовой охраны сведений. В то же время сами персональные данные в ряде ситуаций могут рассматриваться и как объект охраны, и как предмет преступления, поскольку именно посредством их незаконного получения, использования или распространения совершаются многие противоправные деяния.

Анализ современного состояния уголовно-правовой защиты персональных данных показывает, что с момента введения в действие Федерального закона «О персональных данных» правоприменительная практика пошла по пути квалификации соответствующих посягательств по различным статьям Особенной части Уголовного кодекса РФ (далее – УК РФ). Вместе с тем, данные нормы носят преимущественно бланкетный характер и не содержат в самом уголовном законе конкретизации категорий персональных данных, подлежащих охране. Учитывая межотраслевой характер правового режима персональных данных и разнообразие требований к их защите, вопрос о применимости уголовно-правовых средств в каждом конкретном случае решается с учетом вида персональных данных, их содержания, установленных законодательством запретов и ограничений. Это обуславливает сложность и оценочный характер соответствующей правоприменительной деятельности.

Персональные данные, выступающие в качестве предмета либо средства совершения преступления, служат информацией о физическом лице, зафиксированной на материальном носителе или существующей в нематериальной форме. Существенным признаком информации является ее конфиденциальный характер и ограниченный доступ, поскольку именно совокупность соответствующих сведений позволяет осуществить однозначную идентификацию субъекта персональных данных и тем самым затрагивает сферу его частной жизни и законных интересов [6, с. 14].

На основе анализа международного права, российского законодательства и отечественной доктрины Е.В. Хохлова выделяет следующие признаки персональных данных. Во-первых, это сведения о физическом лице, независимо от того, как они воспринимаются и используются. Во-вторых, информация должна иметь связь с конкретным субъектом, прямо или косвенно идентифицируемым. В-третьих, сведения соотносятся с определенным или потенциально определяемым человеком, это отличает их от иных категорий информации. В-четвертых, персональные данные обладают конфиденциальным характером, охрана распространяется лишь на сведения, использование которых может причинить вред публичным или частным интересам. В-пятых, эти данные являются обособленной информацией, фиксированной в какой-либо форме. И, наконец, в-шестых, их содержание может отражать и объективные факты, и слухи или домыслы, находящиеся в ограниченном доступе, расширяя понимание предмета правовой защиты [6, с. 77].

Несмотря на отсутствие в уголовном законодательстве исчерпывающего и четко структурированного понятия, представляется возможным выделить круг преступлений, в рамках которых персональные данные либо непосредственно составляют предмет преступного посягательства, либо исполь-

зуются как инструмент реализации противоправного умысла. В ряде составов преступлений персональные данные фактически выступают предметом преступления, поскольку именно на них направлено противоправное воздействие, что характерно, в частности, для преступлений, посягающих на неприкосновенность частной жизни (ст. 137 УК РФ), тайну переписки и иных сообщений (ст. 138 УК РФ), отказ в предоставлении информации (ст. 140 УК РФ), а также для деяний, связанных с незаконным получением, разглашением или утратой сведений, охраняемых различными режимами тайны – личной, семейной (ст. 155 УК РФ), коммерческой (ст. 183 УК РФ) и государственной (ст. 275, 283, 284 УК РФ). Аналогичным образом персональные данные становятся предметом посягательства при неправомерном доступе к компьютерной информации (ст. 272 УК РФ). Наряду с этим в отдельных составах преступлений персональные данные не являются непосредственным объектом посягательства, но используются в качестве средства совершения преступления. К примеру, при фальсификации избирательной документации (ст. 142 УК РФ), совершении мошенничества в сфере кредитных правоотношений (ст. 159.1 УК РФ), незаконном использовании документов при создании или реорганизации.

С точки зрения В.А. Чукреева УК РФ не содержит специальных составов преступлений, прямо направленных на защиту персональных данных, ответственность за незаконные действия с личной информацией обеспечивается через нормы, регулирующие нарушение неприкосновенности частной жизни, тайны переписки и коммерческой или банковской информации, неправомерный доступ к компьютерной информации [7, с. 109]. Н.Е. Рязанова разделяет эту позицию, отмечая, что в России уголовно-правовая охрана персональных данных носит опосредованный характер и направлена на защиту конституционных прав и свобод человека и гражданина, экономических интересов и информационной безопасности. Персональные данные могут выступать и как предмет преступления, и как средство его совершения [8, с. 119]. Учитывая ограниченные профилактические возможности действующих норм и рост новых угроз в сфере информации, авторы признают необходимость формирования специальной уголовно-правовой охраны персональных данных.

Сравнительный анализ статей 137 и 183 УК РФ позволяет выявить ряд общих характеристик объекта преступного посягательства, несмотря на различие охраняемых сфер общественных отношений. Прежде всего, в обеих нормах объект преступления связан с **общественными отношениями по обеспечению конфиденциальности охраняемой законом информации**. В ст. 137 УК РФ сведениями выступают данные, составляющие личную и семейную тайну, тогда как в ст. 183 УК РФ – сведения, отнесенные к коммерческой, налоговой или банковской тайне.

Общность объекта проявляется и в том, что в обоих случаях преступление посягает на **нематериальные блага**, выраженные в установленном законом порядке обращения с информацией. Объект преступления ст. 137 УК РФ не сводится к отдельным сведениям, а представляет собой общественные отношения, обеспечивающие реализацию конституционного права на неприкосновенность частной жизни [9, с. 40].

Неприкосновенность частной жизни является социальной потребностью, лежащей за пределами права, но получающей юридическое закрепление и защиту посредством правовых механизмов. В свою очередь, охрана коммерческой, налоговой и банковской тайны направлена на обеспечение стабильности экономических отношений и безопасности гражданского оборота, в связи с чем имеет конституционно значимый характер [10, с. 283].

Первостепенной отличительной чертой объекта преступного посягательства является **характер защищаемого интереса**. В ст. 137 УК РФ непосредственным объектом выступают общественные отношения, складывающиеся по поводу реализации личных неимущественных прав человека. Как указывается в комментарии к УК РФ под редакцией В.Т. Томина и В.В. Сверчкова, основным объектом является неприкосновенность частной жизни, личная и семейная тайна, тогда как честь, достоинство и доброе имя могут выступать факультативными объектами преступления [11, с. 225]. Объект преступного посягательства ст. 183 УК РФ носит **экономико-правовой характер**, следовательно, личность как носитель индивидуальных нематериальных благ не является центральным элементом объекта преступления по ст. 183 УК РФ. Изучение материалов уголовных дел, в которых деяния квалифицировались по статье 183 УК РФ и в качестве предмета преступления фигурировали персональные данные, позволяет сделать вывод о типовых направлениях нарушения режима коммерческой тайны. Судебная практика свидетельствует о том, что наиболее уязвимыми оказываются сведения о лицах, находящихся в устойчивых либо эпизодических договорных отношениях с коммерческими организациями и использующих предоставляемые ими товары, работы или услуги. Наряду с этим существенное место занимают случаи незаконного получения или разглашения персональных данных физических лиц, взаимодействующих с организацией в качестве партнеров на равноправной либо иной основе, поскольку сведения нередко обладают самостоятельной экономической ценностью. В ряде уголовных дел объектом посягательства также становились персональные данные иных лиц, формально не связанных с организацией, однако способных прямо либо опосредованно влиять на ее положение в конкурентной среде и результаты участия в торговом обороте, что характеризует сведения как коммерчески значимую информацию [12, с. 130].

Существенным отличием является и **основание возникновения режима тайны**. В отношении личной и семейной тайны, охраняемой ст. 137 УК

РФ, конфиденциальность вытекает из самой природы частной жизни и не требует специального юридического оформления. Напротив, для квалификации по ст. 183 УК РФ необходимо наличие установленного в соответствии с законом режима коммерческой, налоговой или банковской тайны.

Видится возможным сформулировать методику разграничения объекта преступного посягательства при квалификации деяний, связанных с незаконным получением или распространением информации.

1. **Определение характера информации.** Устанавливается, имеет ли разглашенная или использованная информация личный характер (личная или семейная тайна) либо относится к сфере предпринимательства (коммерческая, налоговая, банковская тайна).

2. **Проверка правовой охраны информации.** Уточняется, существует ли специальный режим конфиденциальности. Для квалификации по ст. 137 УК РФ достаточно установления факта личного характера данных. Для применения ст. 183 информация должна быть официально признана коммерческой, налоговой или банковской тайной.

3. **Идентификация объекта и субъекта правоотношений.** Оценивается, чьи интересы затронуты: частного лица или юридического/физического лица как хозяйствующего субъекта.

4. **Анализ сущности посягательства.** Устанавливается, имело ли место посягательство на конституционное право (в неприкосновенности частной жизни) или на право собственности и деловой репутации (коммерческая тайна).

5. **Учет иных обстоятельств.** При необходимости рассматривается наличие иных признаков состава: отнесенность сведений к категории коммерческой (налоговой, банковской) тайны подтверждается режимом доступа и потенциальным экономическим ущербом. Для любого преступления необходим несанкционированный характер посягательства.

Проблемой квалификации деяния, объектом посягательства которого выступают персональные данные, является разграничение уголовной и административной ответственности. Особую сложность вызывает соотнесение состава административного правонарушения, предусмотренного ст. 13.11 КоАП РФ, и преступления, предусмотренного ст. 272.1 УК РФ, поскольку обе нормы направлены на охрану однородных общественных отношений и допускают пересечение по фактическим обстоятельствам совершенного деяния.

Конструкция части первой статьи 272.1 УК РФ не содержит достаточного набора признаков, позволяющих однозначно провести границу между уголовно наказуемым деянием и административным проступком, предусмотренным статьей 13.11 КоАП РФ [13].

Анализ действующего законодательства и научных позиций изложенных в работе, позволяет утверждать, что конкуренция между ст. 13.11 КоАП РФ и ст. 272.1 УК РФ обусловлена внешним

сходством охраняемых общественных отношений, однако при более тщательном рассмотрении данные нормы имеют принципиальные различия по ряду признаков.

Прежде всего, различие проявляется по предмету правового воздействия. Административная норма направлена на охрану порядка обработки персональных данных в широком смысле и распространяется на любые персональные данные независимо от формы их существования и способа получения. Напротив, уголовно-правовая норма сужает предмет посягательства, ограничивая его компьютерной информацией, содержащей персональные данные, при этом обязательным признаком является незаконный способ получения информации.

Вторым отличительным признаком является характеристика данных. В ст. 13.11 КоАП РФ речь идет о нарушении установленных законодательством требований обработки персональных данных, в том числе, сбора, хранения, использования и передачи, независимо от того, каким образом данные были получены. В норме ст. 272.1 УК РФ ответственность предусмотрена в случае, если указанные действия совершаются в отношении информации, изначально полученной незаконным путем [14].

Представляется необходимым сформулировать методику разграничения составов ст. 13.11 КоАП РФ и ст. 272.1 УК РФ по критерию объекта посягательства.

1. **Определение объекта посягательства,** то есть какие сведения стали объектом действий: если это персональные данные в любой форме, деяние подпадает под административную ответственность по ст. 13.11 КоАП РФ; если же объектом является компьютерная информация, содержащая персональные данные, возможна квалификация по ст. 272.1 УК РФ.

2. **Проверка характеристики информации.** Необходимо соотнести действия с правовым режимом информации: сбор, хранение, использование или передача законно полученных данных образуют административное правонарушение, тогда как аналогичные действия с незаконно полученной компьютерной информацией подлежат уголовной оценке.

3. **Окончательная квалификация.** При отсутствии хотя бы одного признака уголовного состава (в первую очередь незаконного получения компьютерной информации) деяние квалифицируется по ст. 13.11 КоАП РФ; при наличии всех признаков (компьютерная информация, незаконное получение и действия с ней) применяется ст. 272.1 УК РФ.

Следовательно, положения административного и уголовного законодательства, регулирующие ответственность за противоправные действия в сфере персональных данных, имеют принципиально различные содержание и направленность. Нормы КоАП РФ ориентированы преимущественно на реагирование на несоблюдение установленных процедур и требований обработки персональных данных, тогда как нормы уголовного закона предназначены для защиты самой сферы конфиденци-

альности персональной информации, в отношении которой установлен особый правовой режим и нарушение которого затрагивает фундаментальные интересы охраняемых общественных отношений.

Таким образом, анализ судебной практики свидетельствует о тенденции к функциональному толкованию персональных данных, при котором определяющим критерием их признания выступает возможность идентификации личности и причинения вреда ее правам и законным интересам, независимо от формы фиксации и источника получения информации.

Разработанные в статье критерии и методики разграничения смежных составов преступлений

(ст. 137 и 183 УК РФ), уголовной и административной ответственности (ст. 272.1 УК РФ и ст. 13.11 КоАП РФ) позволят снизить риски ошибочной квалификации деяний.

Перспективными направлениями дальнейших исследований являются: разработка концепции системной уголовно-правовой защиты персональных данных, уточнение признаков объекта преступного посягательства в информационной сфере, анализ целесообразности закрепления в уголовном законодательстве специальных норм в сфере защиты персональных данных в цифровой среде.

Список источников

1. Бачило И.Л. Информационное право: основы практической информатики: учеб. пособие. Москва, 2001. 352 с.
2. Таганцев Н.С. Русское уголовное право. Лекции. Часть Общая: в 2 т. Т. 1. Москва, 1994.
3. Каиржанов Е.К. Интересы трудящихся и уголовный закон. Проблемы объекта преступлений. Алма-Ата, 1973. 160 с.
4. Коржанский Н.И. Основания и критерии выбора объектов уголовно-правовой охраны // Труды ВШ МВД СССР, 1976. Вып. 12. 191 с.
5. Гахуман Л.Д. Квалификация преступлений: закон, теория, практика. Москва: АО «Центр ЮрИнфоР», 2001. 316 с.
6. Хохлова Е.В. Незаконные действия с персональными данными: уголовно-правовое исследование: дис. ... канд. юрид. наук. Саратов, 2024. 255 с.
7. Чукреев В.А. Персональные данные, в том числе биометрические данные, как предметы уголовно-правовой охраны // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 3 (91). С. 107–116.
8. Рязанова Е.Н. Ответственность за распространение персональных данных как способ противодействия правонарушениям в сфере информационно-коммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. 2022. № 3 (95). С. 118–123.
9. Бунова И.И. О предмете нарушения неприкосновенности частной жизни (ст. 137 УК РФ) // Вестник Московского университета МВД России. 2023. № 5. С. 38–42.
10. Родивилин И.П. Информация как объект уголовно-правовой охраны: понятие, признаки, виды // Всероссийский криминологический журнал. 2024. Т 18, №3. С.278–285.
11. Комментарий к Уголовному кодексу Российской Федерации / под ред. В.Т. Томина и В.В. Сверчкова. Москва: Юрайт-Издат, 2010. 1312 с.
12. Гутник С.И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: дис. ... канд. юрид. наук. Красноярск, 2017. 241 с.
13. Князьков А.А. Уголовно-правовая новелла за нарушение законодательства о персональных данных (ст. 272.1 УК РФ): особенности конструирования состава и вопросы квалификации // Вестник Университета имени О.Е. Кутафина. 2025. №5. URL: <https://cyberleninka.ru/article/n/ugolovno-pravovaya-novella-za-narushenie-zakonodatelstva-o-personalnyh-dannyh-st-272-1-uk-rf-osobennosti-konstruirovaniya-sostava-i> (дата обращения: 19.01.2026).
14. Корешников Д.С. Конкуренция норм об охране персональных данных: разграничение статьи 272.1 УК РФ и ст.13.11 КоАП РФ // Правопорядок: история, теория, практика. 2025. №3. С. 49–54. URL: <https://cyberleninka.ru/article/n/konkurenciya-norm-ob-ohrane-personalnyh-dannyh-razgranichenie-stati-272-1-uk-rf-i-stati-13-11-koap-rf> (дата обращения: 19.01.2026).

References

1. Bachilo I.L. Informationsnoe pravo: osnovy prakticheskoi informatiki [Information law: fundamentals of practical computer science]: training manual. Moscow, 2001, 352 p. (In Russ.).
2. Tagantsev N.S. Russkoe ugovnoe pravo. Lektsii. Chast' Obshchaya [Russian criminal law. Lectures. The General Part]. In 2 volumes, vol. 1. Moscow, 1994. (In Russ.).
3. Kairzhanov E.K. Interesy trudyashchikhsya i ugovnyi zakon. Problemy ob"ekta prestuplenii [Interests of workers and criminal law. Problems of the crime object]. Alma-Ata, 1973, 160 p. (In Russ.).
4. Korzhansky N.I. Osnovaniya i kriterii vybora ob"ektov ugovno-pravovoi okhrany [Grounds and criteria for choosing objects of criminal law protection]. *Trudy VSSH MVD SSSR [Proceedings of the Higher School of the Ministry of Internal Affairs of the USSR]*, 1976, vol. 12, 191 p. (In Russ.).
5. Gakhuman L.D. Kvalifikatsiya prestuplenii: zakon, teoriya, praktika [Qualification of crimes: law, theory, practice]. Moscow: JSC "Center Yurinfo" Publ., 2001, 316 p. (In Russ.).

6. Khokhlova E.V. *Nezakonnnye deistviya s personal'nymi dannymi: ugovolno-pravovoe issledova-nie: dis. ... kand. yurid. nauk* [Illegal actions with personal data: criminal law research: Cand. Law Sci. Diss. Saratov, 2024, 255 p. (In Russ.).

7. Chukreev V.A. Personal'nye dannye, v tom chisle biometricheskie dannye, kak predmety ugovol-no-pravovoi okhrany [Personal biometric data as subjects of criminal law protection], *Vestnik Universiteta imeni O.E. Kutafina (MGYUA)* [Bulletin of the O.E. Kutafin University (MGUA)], 2022, no. 3 (91), pp. 107–116. (In Russ.).

8. Ryazanova E.N. Otvetstvennost' za rasprostranenie personal'nykh dannykh kak sposob protivodeistviya pravonarusheniyam v sfere informatsionno-kommunikatsionnykh tekhnologii [Responsibility for the dissemination of personal data as a way to counteract offenses in the field of information and communication technologies], *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii* [Vestnik of the St. Petersburg University of the Ministry of Internal Affairs of Russia], 2022, no. 3 (95), pp. 118–123. (In Russ.).

9. Bunova I.I. O predmete narusheniya neprikosновенности chastnoi zhizni (st. 137 UK RF) [On the subject of violation of privacy (Article 137 of the Criminal Code of the Russian Federation)], *Vestnik Moskovskogo universiteta MVD Rossii* [Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia], 2023, no. 5, pp. 38–42. (In Russ.).

10. Rodivilin I.P. Informatsiya kak ob"ekt ugovolno-pravovoi okhrany: ponyatie, priznaki, vidy [Information as an object of criminal law protection: concept, features, types], *Vserossiiskii kriminologicheskii zhurnal* [All-Russian Journal of Criminology], 2024, vol. 18, no. 3, pp. 278–285. (In Russ.).

11. Kommentarii k Ugolovnomu kodeksu Rossiiskoi Federatsii [Commentary to the Criminal Code of the Russian Federation], edited by V.T. Tomin and V.V. Sverchkov. Moscow: Yurayt-Izdat Publ., 2010, 1312 p. (In Russ.).

12. Gutnik S.I. Ugolovno-pravovaya kharakteristika prestupnykh posyagatel'stv v otnoshenii perso-nal'nykh dannykh: dis. ... kand. yurid. nauk [Criminal and legal characteristics of criminal encroachments on personal data: Cand. Law Sci. Diss.]. Krasnoyarsk, 2017, 241 p. (In Russ.).

13. Knyazkov A.A. Ugolovno-pravovaya novella za narushenie zakonodatel'stva o personal'nykh dan-nykh (st. 2721 UK RF): osobennosti konstruirovaniya sostava i voprosy kvalifikatsii [Criminal law novell for violation of the legislation on personal data (art. 2721 of the Criminal Code of the Russian Federation): design features of the composition and qualification issues], *Vestnik Universiteta imeni O.E. Kutafina* [Bulletin of the O. E. Kutafin University], 2025, no.5. (In Russ.). Available at: <https://cyberleninka.ru/article/n/ugolovno-pravovaya-novella-za-narushenie-zakonodatelstva-o-personal'nykh-dannykh-st-2721-uk-rf-osobennosti-konstruirovaniya-sostava-i> (accessed 19.01.2026).

14. Koreshnikov D.S. Konkurentsia norm ob okhrane personal'nykh dannykh: razgranichenie stat'i 272.1 UK RF i st.13.11 KoAP RF [Competition of Personal Data Protection Standards: Differentiation of Article 272.1 of the Criminal Code of the Russian Federation and Article 13.11 of the Administrative Code of the Russian Federation], [Legal and Order: History, Theory, Practice], 2025, no. 3, pp. 49–54 (In Russ.). Available at: <https://cyberleninka.ru/article/n/konkurentsia-norm-ob-okhrane-personal'nykh-dannykh-razgranichenie-stati-272-1-uk-rf-i-stati-13-11-koap-rf> (accessed 19.01.2026).

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликтов интересов.

Authors' contribution: All authors have made an equivalent contribution to the preparation of the publication. The authors declare that there is no conflict of interest.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Алиева Диана Нурмагомедовна, кандидат юридических наук, доцент кафедры уголовного права и криминологии юридического института Дагестанского государственного университета, г. Махачкала, Российская Федерация. *E-mail:* kurbanova.diana2020@mail.ru

Сафаралиев Надир Маликович, аспирант кафедры уголовного права и криминологии юридического института Дагестанского государственного университета, г. Махачкала, Российская Федерация. *E-mail:* nadir-safaraliev@mail.ru

Поступила в редакцию 10.02.2026 г.; одобрена после рецензирования 25.03.2026 г.; принята к публикации 26.05.2026 г.

INFORMATION ABOUT THE AUTHORS

Aliyeva Diana Nurmagomedovna, Candidate of Law, Associate Professor of the Department of Criminal Law and Criminology of the Law Institute of Dagestan State University, Makhachkala, Russian Federation. *E-mail:* kurbanova.diana2020@mail.ru

Safaraliev Nadir Malikovich, Post-graduate Student of the Department of Criminal Law and Criminology of the Law Institute of Dagestan State University, Makhachkala, Russian Federation. *E-mail:* nadir-safaraliev@mail.ru

Received 10.02.2026; approved after reviewing 25.03.2026; accepted for publication 26.05.2026