Научная статья С. 174–182
УДК 343.3/.7
DOI: 10.47475/2311-696X-2026-50-3-174-182

ОБЪЕКТ И ПРЕДМЕТ СОСТАВА ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТАТЬЕЙ 272.1 УК РФ

Анна Валерьевна Волкова

Казанский инновационный университет имени В. Г. Тимирясова, г. Казань, Россия
avmail555@gmail.com

Аннотация. Настоящая статья посвящена исследованию объекта и предмета преступления, предусмотренного ст. 272[1] УК РФ. Автор предпринимает попытку концептуального осмысления природы охраняемых общественных отношений в условиях дуалистической конструкции объекта, одновременно охватывающего безопасность компьютерной информации и конституционное право на неприкосновенность частной жизни. Критическому исследованию подвергается размещение нормы в главе о преступлениях в сфере компьютерной информации, выявляются теоретические противоречия между формальной локализацией и материальным содержанием охраняемых правовых благ. Детальному изучению подвергается предмет преступления как интегративная правовая категория, синтезирующая признаки компьютерной информации и персональных данных. Внимание уделяется анализу специальных видов предмета, закрепленных в ч. 2 ст. 272[1] УК РФ.

Ключевые слова: объект преступления, предмет преступления, статья 272.1 УК РФ, персональные данные, компьютерная информация, неприкосновенность частной жизни, информационная безопасность, биометрические данные, специальные категории персональных данных

Для цитирования: Волкова А. В. Объект и предмет состава преступления, предусмотренного статьей 272.1 УК РФ // Правопорядок: история, теория, практика. 2026. № 3 (50). С. 174–182. DOI: 10.47475/2311-696X-2026-50-3-174-182

Research article

THE OBJECT AND SUBJECT OF THE CORPUS DELICTI PROVIDED FOR IN ARTICLE 272.1 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION

Anna V. Volkova

Kazan Innovative University named after V. G. Timiryasov, Kazan, Russia
avmail555@gmail.com

Abstract. This article is devoted to the study of the object and subject of the crime provided for in Article 272[1] of the Criminal Code of the Russian Federation. The author attempts to conceptualize the nature of protected public relations in terms of a dualistic object design that simultaneously encompasses the security of computer information and the constitutional right to privacy. The placement of the norm in the chapter on crimes in the field of computer information is critically examined, and theoretical contradictions between the formal localization and the material content of protected legal goods are revealed. The subject of crime is subjected to a detailed study as an integrative legal category synthesizing the features of computer information and personal data. Attention is paid to the analysis of special types of the subject fixed in part 2 of art. 272[1] of the Criminal Code of the Russian Federation.

Keywords: object of crime, subject of crime, Article 272.1 of the Criminal Code of the Russian Federation, personal data, computer information, privacy, information security, biometric data, special categories of personal data

For citation: Volkova AV. The Object and Subject of the Corpus Delicti Provided for in Article 272.1 of the Criminal Code of the Russian Federation. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2026;(3):174-182. (In Russ.). DOI: 10.47475/2311-696X-2026-50-3-174-182

© Волкова А. В.

Введение

Федеральным законом от 30 ноября 2024 года № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»[1] установлена ответственность за незаконный оборот персональных данных (ст. 272[1] УК РФ). Новеллы ознаменовали новый этап развития уголовно-правовой охраны персональных данных, что актуализирует необходимость фундаментального переосмысления категорий объекта и предмета данного состава преступления в контексте существенного расширения диапазона криминализированных деяний и усложнения их квалифицирующих признаков [7]. Законодательная новелла представляет собой конструкцию с градуированной системой санкций, охватывающих диапазон от штрафа до десяти лет лишения свободы, что отражает признание законодателем критической значимости защиты персональных данных в условиях цифровизации, экспоненциального роста объемов обрабатываемой персональной информации, множественных инцидентов несанкционированного доступа к базам данных, содержащим чувствительную информацию о миллионах граждан.

Многообъектная природа преступления: теоретическая реконструкция охраняемых общественных отношений

Проблематика определения объекта преступления, предусмотренного ст. 272[1] УК РФ, характеризуется исключительной сложностью, обусловленной дуалистической, а по мнению некоторых исследователей [23], даже множественной природой охраняемых общественных отношений, не позволяющей однозначно определить непосредственный объект преступного посягательства. Расположение статьи в главе 28 УК РФ «Преступления в сфере компьютерной информации» указывает на родовой объект в виде общественной безопасности и видовой объект в виде безопасности компьютерной информации, однако содержательное исследование охраняемых общественных отношений, интересов и благ, которые непосредственно страдают в результате совершения указанного преступления свидетельствует о том, что центральным элементом защиты выступает конституционное право граждан на неприкосновенность частной жизни, информационное самоопределение, контроль над персональной информацией. Персональные данные представляют собой не просто информацию в техническом смысле, но информационную проекцию личности, ее цифровую идентичность, совокупность сведений, определяющих индивида в информационном обществе. Незаконные действия с персональными данными посягают на фундаментальные права человека, гарантированные не только национальным конституционным правом, но и международными актами о правах человека: Всеобщей декларацией прав человека[2], Международным пактом о гражданских и политических правах[3], Конвенцией о защите физических лиц при автоматизированной обработке персональных данных[4].

Конституционный Суд Российской Федерации в ряде решений сформулировал правовую позицию о праве на защиту персональных данных как элементе конституционного права на неприкосновенность частной жизни, имеющем самостоятельное значение в системе прав человека. В постановлении от 25 мая 2021 г. № 22-П[5] Конституционный Суд указал, что право на защиту персональных данных, являясь элементом права на неприкосновенность частной жизни, обеспечивает индивидуальную автономию и человеческое достоинство, предоставляет возможность контролировать информационные потоки персональных данных и тем самым осуществлять информационное самоопределение. Европейский Суд по правам человека в решениях по ст. 8 Конвенции о защите прав человека и основных свобод[6] (право на уважение частной и семейной жизни) неоднократно подчеркивал, что сбор, хранение, использование и распространение персональных данных подпадают под действие гарантий частной жизни, государство обязано обеспечивать эффективную защиту от злоупотреблений с персональными данными. Данные правовые позиции свидетельствуют о том, что защита персональных данных выходит за пределы исключительно технической безопасности компьютерной информации, охватывая фундаментальные права личности.

Предмет преступления, дефинируемый законодателем через комплексную формулу «компьютерная информация, содержащая персональные данные», представляет собой интегративную правовую конструкцию, требующую одновременного установления двух

[1] Федеральный закон от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // Собрание законодательства Российской Федерации. 2024. № 49 (ч. IV). Ст. 7412.

[2] Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 A (III) от 10 декабря 1948 г.) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/ (дата обращения: 18.03.2026).

[3] Международный пакт о гражданских и политических правах (Нью-Йорк, 16 декабря 1966 г.) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/ (дата обращения: 18.03.2026).

[4] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ N 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // Собрание законодательства Российской Федерации. 2005. № 52 (ч. I). Ст. 5573.

[5] Постановление Конституционного Суда Российской Федерации от 25 мая 2021 г. № 22-П «По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона «О персональных данных» в связи с жалобой общества с ограниченной ответственностью «МедРейтинг»» // Конституционный суд Российской Федерации. URL: http://publication.pravo.gov.ru/document/0001202105280003 (дата обращения: 18.03.2026).

[6] Конвенция о защите прав человека и основных свобод ETS N 005 (Рим, 4 ноября 1950 г.) (с изм. и доп. от 21 сентября 1970 г., 20 декабря 1971 г., 1 января 1990 г., 6 ноября 1990 г., 11 мая 1994 г.) // Собрание законодательства Российской Федерации. 2001. № 2. Ст. 163.

© Волкова А. В.

групп признаков: характеризующих информацию как компьютерную (форма представления, способ обработки, место нахождения) и характеризующих информацию как персональные данные (содержание, связь с конкретным индивидом, идентифицирующая способность). Нематериальная природа информации как предмета преступления обусловливает ее специфические свойства, кардинально отличающие от традиционных материальных предметов: способность к неограниченному копированию без утраты оригинала, мгновенное перемещение в пространстве посредством информационно-телекоммуникационных сетей, неисчерпаемость при использовании, невозможность уничтожения всех копий после распространения. Эти свойства создают уникальные проблемы правоприменения и определения юридической судьбы предмета преступления после его изъятия: в отличие от материальных предметов, изъятие компьютерной информации не лишает виновного возможности сохранения копий, распространение информации приводит к ее неконтролируемому размножению, делая невозможным устранение последствий преступления.

Часть 2 ст. 272[1] УК РФ устанавливает уголовную ответственность в зависимости от категории персональных данных (персональные данные несовершеннолетних лиц, специальные категории персональных данных, биометрические персональные данные). Данная дифференциация основывается на признании законодателем различной степени чувствительности персональной информации, различных рисков причинения вреда субъектам персональных данных в зависимости от категории информации, различной степени общественной опасности незаконных действий с различными категориями данных. Повышенная санкция части второй отражает особую уязвимость несовершеннолетних, особую чувствительность специальных категорий персональных данных (информации о расовой, национальной принадлежности, политических взглядах, религиозных убеждениях, состоянии здоровья, интимной жизни), повышенные риски злоупотреблений с биометрическими данными, способными обеспечивать однозначную идентификацию личности.

Определение объекта преступления, предусмотренного ст. 272[1] УК РФ, требует последовательного применения классификации объектов по вертикали и по горизонтали, разработанной российской уголовно-правовой доктриной. Родовой объект в виде общественной безопасности и общественного порядка является предельно абстрактным, охватывающим разнородные общественные отношения, объединенные общим признаком связи с безопасными условиями существования общества, стабильностью социального порядка, защищенностью жизненно важных интересов личности, общества и государства от различных угроз. Раздел IX «Преступления против общественной безопасности и общественного порядка» УК РФ включает в себя разнообразные главы: преступления против основ конституционного строя и безопасности государства, уголовно наказуемые деяния против здоровья населения и общественной нравственности, экологические преступления, уголовно наказуемые деяния против безопасности движения и эксплуатации транспорта и в сфере компьютерной информации. Включение в раздел противоправных деяний в сфере компьютерной информации отражает признание законодателем того, что информационная безопасность является элементом безопасности.

Видовым объектом преступлений является безопасность компьютерной информации, понимаемая как защищенность информации в электронно-цифровой форме от неправомерных действий, способных нарушить ее конфиденциальность, целостность или доступность [1].

Вместе с тем сведение объекта преступления, предусмотренного ст. 272[1] УК РФ, исключительно к безопасности компьютерной информации представляется явно недостаточным, игнорирующим специфику персональных данных как информации о личности, непосредственно связанной с конституционными правами человека. Персональные данные — это не просто информация в техническом смысле, не просто данные, подлежащие обработке средствами вычислительной техники, но информационная проекция личности, ее цифровая идентичность, совокупность сведений, определяющих индивида в информационном обществе. В эпоху цифровизации персональные данные приобрели фундаментальное значение для реализации практически всех сфер жизнедеятельности человека: социальных коммуникаций (профили в социальных сетях) [16], экономических отношений (банковские аккаунты, электронные кошельки) [13; 22], доступа к государственным услугам (порталы госуслуг) [12], медицинского обслуживания (электронные медицинские карты) [11], образования (электронные дневники, образовательные платформы) [5], трудовых отношений (кадровые информационные системы) [10]. Компрометация персональных данных способна причинить индивиду многообразный вред: имущественный (мошенническое использование банковских данных), моральный (распространение компрометирующих сведений), репутационный (публикация порочащей информации), психологический (чувство незащищенности, утраты контроля над информацией о себе) [3; 14; 20].

Конституция Российской Федерации[7], закрепляя систему гарантий защиты персональных данных, устанавливает право каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, а также право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, ограничение которого допускается только на основании судебного решения. Статьей 24 Конституции Российской Федерации установлен запрет сбора, хранения, использования и распространения

[7] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07. 2020), ст. 3. М., 2020. 63 с.

© Волкова А. В.

информации о частной жизни лица без его согласия. В свою очередь ч. 2 ст. 24 Конституции Российской Федерации обязывает органы государственной власти и местного самоуправления, их должностных лиц обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Данные конституционные нормы образуют правовую основу защиты персональных данных, которые представляют собой информацию о частной жизни лица в широком смысле.

Признание того, что незаконные действия с персональными данными посягают не только на техническую безопасность компьютерной информации, но прежде всего на конституционное право граждан на неприкосновенность частной жизни и информационное самоопределение, обусловливает необходимость отнесения преступления, предусмотренного ст. 272[1] УК РФ, к многообъектному. В уголовно-правовой доктрине многообъектное преступление характеризуется тем, что одно преступное деяние причиняет вред или создает угрозу причинения вреда двум или более объектам [21, с. 141].

Применительно к преступлению, предусмотренному ст. 272[1] УК РФ, возникает дискуссионный вопрос о том, какой из объектов является основным, а какой — дополнительным: безопасность компьютерной информации или право на неприкосновенность частной жизни и защиту персональных данных. Формальный критерий размещения нормы в главе о преступлениях в сфере компьютерной информации указывает на безопасность компьютерной информации как основной объект. Вместе с тем материальный критерий, основанный на телеологическом толковании, учитывающем цели законодателя при установлении уголовной ответственности, свидетельствует о приоритете защиты прав личности. Законодатель криминализировал не любые действия с компьютерной информацией, а только действия с компьютерной информацией, содержащей персональные данные, что указывает на специфику предмета как квалифицирующего признака. Если бы целью было исключительно обеспечение безопасности компьютерной информации, предмет не ограничивался бы персональными данными, а охватывал бы любую компьютерную информацию. Ограничение предмета персональными данными свидетельствует о том, что целью является защита прав субъектов персональных данных, а не абстрактная информационная безопасность.

Основным непосредственным объектом преступления, предусмотренного ст. 272[1] УК РФ, являются конституционное право граждан на неприкосновенность частной жизни и информационное самоопределение, реализуемое через контроль над персональными данными, тогда как дополнительным обязательным объектом выступают общественные отношения по обеспечению безопасности компьютерной информации. Данный подход ставит под вопрос обоснованность размещения ст. 272[1] УК РФ в главе 28 УК РФ. Альтернативным решением могло бы быть включение нормы в главу 19 «Преступления против конституционных прав и свобод человека и гражданина» УК РФ. Законодатель, однако, обоснованно исходил из специфики способа совершения преступления и формы представления информации: ст. 272[1] УК РФ охватывает только действия с компьютерной информацией, то есть информацией в электронно-цифровой форме, обрабатываемой с использованием информационных технологий, что определяет ее принадлежность к преступлениям в сфере компьютерной информации как к специальной группе составов, характеризующихся специфическим предметом и способом совершения.

Предмет преступления: диалектика компьютерной информации и персональных данных

Предметом преступления является «компьютерная информация, содержащая персональные данные». Он представляет собой правовую конструкцию, требующую последовательного анализа двух понятий с последующим установлением их взаимосвязи и синтеза в единое понятие предмета преступления [6]. Компьютерная информация определяется в прим. 1 к ст. 272 УК РФ. Данное определение основывается на сочетании двух критериев: формы представления информации (в форме электрических сигналов) и места нахождения информации (независимо от средств их хранения, обработки и передачи).

Ключевым признаком компьютерной информации является форма ее представления: информация должна быть представлена в электронно-цифровой форме, закодирована в виде последовательности битов (двоичных единиц информации — 0 и 1) [2], доступна для обработки с помощью средств вычислительной техники путем применения алгоритмов преобразования данных. Электронно-цифровая форма отличает компьютерную информацию от информации на иных носителях: печатных документах, где информация представлена в виде графических символов на бумаге; аналоговых аудиозаписях, где информация представлена в виде непрерывных изменений физических параметров сигнала на магнитной ленте; аналоговых видеозаписях; устной информации. Вместе с тем развитие технологий приводит к конвергенции различных форм представления информации: печатные документы сканируются и преобразуются в электронную форму (форматы PDF, JPEG, TIFF), аналоговые аудиозаписи оцифровываются (форматы MP3, WAV, FLAC), аналоговые видеозаписи преобразуются в цифровой формат (AVI, MP4, MKV), устная речь преобразуется в текст с помощью систем автоматического распознавания речи. Для квалификации по ст. 272[1] УК РФ значение имеет то, в какой форме находилась информация в момент совершения преступных действий с ней: если персональные данные находились в форме компьютерной информации, применяется ст. 272[1] УК РФ; если в иной форме (например, в рукописном документе, в устном сообщении) — применяются

© Волкова А. В.

иные нормы (прежде всего ст. 137 УК РФ о нарушении неприкосновенности частной жизни) [18, с. 30].

Е. А. Русскевич поднимает важную проблему о квалификации содеянного, когда лицо часть сведений предоставило посредством отправки фотографий монитора компьютера (скриншотов), а часть по причине значительного объема данных передало на бумаге [17]. Нужна ли дополнительная квалификация содеянного? Мы поддерживаем мнение специалиста о том, что с учетом единства умысла квалифицировать содеянное необходимо только по норме, которая предусматривает более тяжкий состав преступления, то есть по ст. 272[1] УК РФ.

Нематериальная природа компьютерной информации обусловливает ее специфические свойства, кардинально отличающие от традиционных материальных предметов преступления, что создает уникальные проблемы уголовно-правовой квалификации и определения юридической судьбы предмета преступления. Во-первых, информация не подчиняется законам сохранения материи: она может быть скопирована неограниченное число раз без утраты оригинала, при копировании создается полностью идентичный экземпляр информации, обладающий теми же свойствами и ценностью, что и источник. Материальные предметы при изъятии у владельца утрачиваются им; информация при копировании остается у источника и одновременно появляется у получателя. Во-вторых, информация может мгновенно перемещаться в пространстве посредством информационно-телекоммуникационных сетей, преодолевая любые географические расстояния за доли секунды, что делает территориальный принцип действия уголовного закона проблематичным. В-третьих, информация не утрачивается при передаче: лицо, передавшее информацию другому субъекту, сохраняет ее копию и возможность дальнейшего использования и распространения. В-четвертых, информация может существовать одновременно во множестве экземпляров в различных местах, что делает практически невозможным ее полное изъятие или уничтожение.

Эти свойства создают специфические проблемы правоприменения при квалификации деяний по ст. 272[1] УК РФ. Изъятие компьютерной информации, содержащей персональные данные, из незаконного владения не лишает виновного возможности сохранения копий на иных носителях, в облачных хранилищах, на удаленных серверах. Распространение персональных данных в сети Интернет приводит к их неконтролируемому размножению, копированию пользователями, индексации поисковыми системами, архивированию специализированными сервисами, что делает практически невозможным полное удаление информации и устранение последствий преступления. Специфика информации как предмета преступления обусловливает особенности определения момента окончания преступления: в отличие от материальных предметов, изъятие которых образует момент окончания хищения, при незаконных действиях с информацией момент окончания связывается с совершением действий по использованию, передаче, сбору, хранению информации независимо от последующей возможности изъятия или уничтожения информации.

Персональные данные определяются статьей 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[8] (далее — Федеральный закон № 152-ФЗ) как «любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)». Юридическая конструкция данного определения основывается на критерии связи информации с конкретным индивидом, при этом характер информации, ее содержание, способ получения не имеют значения — любая информация, позволяющая идентифицировать лицо или связанная с идентифицированным лицом, является персональными данными. Определение является чрезвычайно широким, охватывая практически безграничный спектр информационных объектов [4; 8]. Информация относится к определенному физическому лицу прямо, если она сама по себе идентифицирует это лицо, позволяет однозначно установить его личность без привлечения дополнительных сведений: фамилия, имя, отчество в сочетании с датой рождения и местом жительства; паспортные данные (серия и номер паспорта); СНИЛС (страховой номер индивидуального лицевого счета); ИНН (идентификационный номер налогоплательщика); номер водительского удостоверения; номер полиса обязательного медицинского страхования; уникальные идентификаторы пользователей в информационных системах при наличии связи с реальной личностью.

Информация относится к определяемому физическому лицу косвенно, если она сама по себе не идентифицирует лицо непосредственно, но при наличии дополнительных сведений, доступных или потенциально доступных оператору или иным лицам, позволяет установить личность. К косвенно идентифицирующей информации можно отнести: IP-адрес интернет-соединения (при наличии у провайдера информации о привязке IP-адреса к конкретному абоненту); MAC-адрес сетевого оборудования или устройства (при возможности сопоставления с регистрационными данными); геолокационные данные (при систематическом отслеживании перемещений, позволяющем идентифицировать лицо по местам постоянного нахождения — место жительства, место работы); cookies и иные уникальные идентификаторы устройств и браузеров (при сопоставлении с данными аутентификации); идентификаторы абонентов мобильной связи IMEI, IMSI (при наличии у операторов связи информации о привязке к абонентам); адреса электронной почты (при возможности установления владельца); никнеймы в социальных сетях и на форумах (при наличии технической возможности деанонимизации).

[8] Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31 (ч. I). Ст. 3451.

© Волкова А. В.

Следует отметить, что критерием отнесения информации к персональным данным является не фактическая идентификация конкретного лица в момент обработки информации, а принципиальная возможность такой идентификации при наличии технических средств, дополнительной информации, специальных методов анализа данных, доступных или потенциально доступных для реализации.

Объем понятия персональных данных включает чрезвычайно широкий спектр информационных категорий: идентификационные данные (ФИО, дата и место рождения, пол, фотография, паспортные данные, реквизиты иных документов, удостоверяющих личность); контактные данные (адрес места жительства или пребывания, номера телефонов стационарных и мобильных, адреса электронной почты, идентификаторы в мессенджерах); социально-демографические данные (гражданство, семейное положение, наличие детей, образование, профессия, должность); экономические данные (сведения о доходах, имуществе, налогах, кредитах, банковских счетах, финансовых операциях); биографическая информация (сведения о трудовой деятельности, местах работы, карьерном пути, образовательной траектории); данные о состоянии здоровья (медицинские диагнозы, результаты анализов и обследований, назначенное лечение, обращения за медицинской помощью, группа инвалидности); информация о частной жизни (фотографии и видеозаписи личного характера, информация о круге общения, интересах, хобби, убеждениях, мировоззрении); поведенческие данные (информация о перемещениях, геолокационные треки, история посещений мест, история покупок, потребительские предпочтения); психологические характеристики и профили (результаты тестирования, оценки личностных качеств, прогнозы поведения) [24].

Предмет преступления, предусмотренный ст. 272^1 УК РФ, определяется через пересечение двух множеств: компьютерной информации и персональных данных. К предмету преступления относится только та информация, которая одновременно удовлетворяет двум критериям: (1) является персональными данными по содержанию (относится прямо или косвенно к определенному или определяемому физическому лицу); (2) представлена в форме компьютерной информации (находится в форме электрических сигналов, независимо от средств их хранения, обработки и передачи). Информация, удовлетворяющая только одному из критериев, не является предметом преступления по ст. 272^1 УК РФ. Персональные данные в нецифровой форме (рукописные документы с персональными данными, печатные фотографии, устная информация о лице) не являются предметом преступления, предусмотренного ст. 272^1 УК РФ; незаконные действия с такой информацией могут квалифицироваться по ст. 137 УК РФ о нарушении неприкосновенности частной жизни или по иным статьям в зависимости от характера действий [17]. Компьютерная информация, не содержащая персональных данных (информация о юридических лицах, обезличенные статистические данные, научная информация, программное обеспечение, иной цифровой контент, не связанный с конкретными физическими лицами), также не является предметом данного преступления; незаконные действия с ней могут образовывать иные составы преступлений в сфере компьютерной информации или иные составы в зависимости от характера информации и действий.

К предмету преступления относятся следующие категории информационных объектов: электронные базы данных клиентов коммерческих организаций, содержащие персональные данные покупателей, заемщиков, страхователей, пользователей услуг (базы данных банков с информацией о счетах и операциях клиентов, базы данных интернет-магазинов с адресами и контактами покупателей, базы данных медицинских организаций с медицинскими картами пациентов); информационные системы персональных данных государственных органов и организаций (государственные реестры населения, базы данных налоговых органов, базы данных правоохранительных органов, базы данных учреждений образования и здравоохранения); персональные данные, размещенные на сайтах в сети Интернет (аккаунты пользователей социальных сетей с профилями, содержащими персональные данные; учетные записи на различных онлайн-платформах; объявления с контактными данными; резюме на сайтах поиска работы); персональные данные в электронной переписке и мессенджерах (сообщения электронной почты, содержащие информацию о лицах; переписка в мессенджерах; файлы, содержащие персональные данные, передаваемые в переписке); файлы на компьютерах, серверах и мобильных устройствах, содержащие персональные данные (фотографии и видеозаписи, идентифицирующие лиц; текстовые документы с персональными данными; электронные таблицы с базами данных; архивы файлов).

Отметим, что важным вопросом является определение того, относятся ли к предмету преступления, предусмотренного ст. 272^1 УК РФ, обезличенные персональные данные. Ст. 3 Федерального закона № 152-ФЗ «О персональных данных» определяет обезличивание персональных данных как действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. Из законодательного определения персональных данных следует, что обезличенная информация, не позволяющая идентифицировать лицо, не является персональными данными и, соответственно, не может быть предметом преступления, предусмотренного ст. 272^1 УК РФ. Вместе с тем на практике возникают вопросы определения степени обезличивания, достаточной для утраты информацией статуса персональных данных. Если обезличивание является обратимым, то есть существует техническая возможность реидентификации лиц путем использования дополнительной информации, находящейся у оператора или у третьих

© Волкова А. В.

лиц, либо путем применения специальных методов деанонимизации (сопоставление различных источников данных, статистический анализ, машинное обучение), информация сохраняет статус персональных данных. Так, например, практика применения GDPR[9] в Европейском Союзе исходит из того, что информация считается анонимизированной только при необратимом обезличивании, когда реидентификация невозможна даже при использовании всех разумно доступных средств.

Дифференциация персональных данных по категориям чувствительности

Часть 2 ст. 272[1] УК РФ устанавливает повышенную уголовную ответственность за деяния, совершенные в отношении компьютерной информации, содержащей три категории персональных данных: персональные данные несовершеннолетних лиц, специальные категории персональных данных, биометрические персональные данные. Данная дифференциация отражает признание законодателем различной степени чувствительности персональной информации, различных рисков причинения вреда субъектам в зависимости от категории данных.

Повышенная уголовно-правовая охрана персональных данных несовершеннолетних обусловлена особой уязвимостью данной категории субъектов, их неспособностью в полной мере осознавать риски раскрытия информации о себе, принимать взвешенные решения о предоставлении персональных данных, эффективно защищать свои права при нарушениях. Незаконные действия с персональными данными несовершеннолетних характеризуются повышенной общественной опасностью. Во-первых, распространение персональных данных несовершеннолетних создает повышенные риски их виктимизации: информация о местонахождении, образе жизни, маршрутах перемещения ребенка может быть использована для совершения преступлений против его половой неприкосновенности, похищения, вовлечения в противоправную деятельность. Во-вторых, несовершеннолетние особенно уязвимы к кибербуллингу — травле в цифровой среде [9], которая может осуществляться на основе распространенных персональных данных, включая фотографии, информацию о частной жизни. В-третьих, компрометация персональных данных несовершеннолетнего может оказать долгосрочное негативное влияние на его развитие, социализацию, психологическое состояние.

Специальные категории персональных данных определяются ч. 1 ст. 10 Федерального закона № 152-ФЗ «О персональных данных» как персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Запрет их обработки обусловлен их чувствительностью и затрагивает наиболее деликатные аспекты личности человека, ее незаконное использование способно причинить вред ее достоинству, привести к дискриминации, нарушению конституционного принципа равноправия граждан. Незаконное использование таких сведений создает риски расовой или национальной дискриминации, разжигания межнациональной розни, нарушения конституционного принципа равенства всех перед законом независимо от расы, национальности, языка. Незаконное распространение информации о политических убеждениях лица может привести к политическому преследованию, дискриминации по политическим мотивам, нарушению свободы мысли и слова. Незаконное использование сведений о религиозных или философских убеждениях создает риски религиозной дискриминации, нарушения свободы совести и вероисповедания.

Незаконное распространение сведений о состоянии здоровья может привести к дискриминации в трудовых отношениях (отказ в приеме на работу, увольнение), социальной стигматизации (в случае заболеваний, воспринимаемых обществом негативно: психических расстройств, ВИЧ-инфекции, инфекций, передающихся половым путем), психологическому дискомфорту, нарушению права на уважение частной жизни.

Сведения об интимной жизни включают информацию о сексуальной ориентации лица, половых связях, сексуальных предпочтениях — аспектах частной жизни. Незаконное распространение сведений об интимной жизни может привести к репутационному вреду, социальной дискриминации (особенно в отношении лиц нетрадиционной сексуальной ориентации), психологической травме, суицидальным попыткам.

Биометрические персональные данные определяются ч. 1 ст. 11 Федерального закона № 152-ФЗ «О персональных данных» как сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных. Биометрические данные используются для установления личности — для идентификации (установления, кто данное лицо) или аутентификации (подтверждения, что лицо является тем, за кого себя выдает). Не любые сведения о физиологических особенностях являются биометрическими персональными данными, а только те, которые используются в системах биометрической идентификации или аутентификации. Важно различать биометрические персональные данные и обычные изображения или иную информацию о физиологических особенностях. Обычные фотографии лица, видеозаписи, не используемые для биометрической идентификации (семейные фотографии, фотографии в социальных сетях, не обрабатываемые системами распознавания лиц), не являются биометрическими персональными данными, хотя остаются персональны-

[9] Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR) // СПС «Гарант». URL: https://base.garant.ru/ (дата обращения: 18.03.2026).

© Волкова А. В.

ми данными общей категории. Те же изображения лица, загруженные в системы распознавания лиц, используемые для биометрической идентификации, становятся биометрическими персональными данными. Запись голоса в обычном аудиофайле не является биометрическими данными; запись, обрабатываемая системой голосовой идентификации для создания голосового профиля, становится биометрическими данными. Данное различие имеет значение для квалификации по ч. 2 ст. 272^1 УК РФ: если изображения лиц или записи голоса не используются для биометрической идентификации, деяние квалифицируется по части первой; если используются — по части второй.

Квалификация деяния по ч. 2 ст. 272^1 УК РФ требует установления того, что виновный осознавал принадлежность персональных данных к специальным категориям. Субъективная сторона преступления должна охватывать сознанием виновного квалифицирующий признак предмета: если лицо не знало и не могло знать, что персональные данные относятся к несовершеннолетним, специальным категориям или биометрическим данным, квалификация по части второй исключается, деяние квалифицируется по ч. 1 ст. 272^1 УК РФ. Вместе с тем в большинстве случаев категория персональных данных очевидна из их содержания или контекста: информация о состоянии здоровья по своему характеру относится к специальным категориям; биометрические данные (отпечатки пальцев, данные систем распознавания лиц) легко идентифицируются как таковые; применительно к персональным данным несовершеннолетних критерием является осознание виновным того, что информация относится к лицам, не достигшим восемнадцати лет, что может устанавливаться через содержание данных (указание даты рождения, возраста) либо контекст их получения (базы данных образовательных или медицинских учреждений, школьные информационные системы, детские социальные сети).

Заключение

Объект преступления характеризуется многообъектной природой, синтезирующей элементы информационной безопасности и конституционных прав личности. Законодатель криминализировал действия не с любой компьютерной информацией, а исключительно с информацией, содержащей персональные данные, что свидетельствует о приоритете защиты прав субъектов персональных данных. Размещение статьи 272^1 УК РФ в главе 28 УК РФ требует осознания того, что охраняемые общественные отношения выходят за пределы исключительно компьютерной безопасности, охватывая фундаментальные права человека. Законодатель исходил из того, что специфика цифровой информации и использования цифровых технологий является определяющим фактором для расположения уголовно-правового запрета.

Предмет преступления представляет собой правовую конструкцию, объединяющую признаки компьютерной информации и персональных данных. Широта легального определения персональных данных обусловливает обширный круг информационных объектов, способных выступать предметом преступления, что требует от правоприменителя внимательного анализа каждого конкретного случая.

Квалифицированные виды предмета, закрепленные в ч. 2 ст. 272^1 УК РФ, отражают дифференцированный подход законодателя к различным категориям персональных данных в зависимости от их чувствительности и рисков причинения вреда. Персональные данные несовершеннолетних выделены в специальную категорию в силу особой уязвимости данных субъектов. Специальные категории персональных данных (информация о расовой, национальной принадлежности, политических взглядах, религиозных убеждениях, состоянии здоровья, интимной жизни) требуют усиленной защиты в силу их особой чувствительности и потенциала причинения вреда достоинству личности [15]. Биометрические персональные данные представляют повышенную опасность в силу их способности обеспечивать однозначную идентификацию личности и невозможности их изменения (в отличие от паролей).

Список источников

1. Батухтин М. Е. Киберпреступления: причины, виды, формы, последствия, направления противодействия // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе: материалы Междунар. науч. конференции адъюнктов, аспирантов, курсантов и студентов. Ч. 3. Самара, 2018. С. 28–31.

2. Бегишев И. Р. Цифровая информация: понятие и сущность как предмета преступления по российскому уголовному праву // Академический юридический журнал. 2011. № 2(44). С. 47–55.

3. Бегишев И. Р., Бикеев И. И. Преступления в сфере обращения цифровой информации. Казань, 2020. 300 с.

4. Бегишев И. Р., Кирпичников Д. В. Проблемные вопросы уголовно-правовой охраны персональных данных // Уголовная юстиция. 2020. № 15. С. 11–16. DOI: 10.17223/23088451/15/3.

5. Вифлеемский А. Б., Лозицкий И. Г. Обработка персональных данных в школе // Школьные технологии. 2012. № 1. С. 122–132.

6. Волкова А. В. Персональные данные как объект уголовно-правовой охраны // International Law Journal. 2025. Т. 8. № 8. С. 222–232.

7. Волкова А. В. Социальная обусловленность криминализации незаконных действий с компьютерной информацией, содержащей персональные данные // Проблемы права. 2025. № 4 (100). С. 86–95.

© Волкова А. В.

8. Волкова А. Ю. Персональные данные как объект уголовно-правовой охраны // Уголовное право: стратегия развития в XXI веке. 2023. № 3. С. 132–137.

9. Газизьянов Т. А., Мансурова З. Р. Психология кибербуллинга. виды и причины кибербуллинга // Общество, право, государственность: ретроспектива и перспектива. 2023. № . 4(16). С. 89–92.

10. Гильмуллина Д. А., Чикенёва И. В. О защите персональных данных в системе трудовых правоотношений // Известия Оренбургского государственного аграрного университета. 2014. № 3. С. 231–234.

11. Зингерман Б. В., Шкловский-Корди Н. Е. Электронная медицинская карта и принципы ее организации // Врач и информационные технологии. 2013. № 2. С. 37–58.

12. Игина К. А. Охрана персональных данных в контексте предоставления государственных и муниципальных услуг в РФ // Проблемы модернизации современного российского государства: сборник материалов IX Всероссийской научно-практической конференции, Стерлитамак, 24–25 июня 2020 года. Стерлитамак, 2020. С. 16–19.

13. Казаренкова Н. П., Звягинцева П. Ю., Бондарева А. А., Требухова И. А. Персональные данные как инновационный актив цифровой экономики // Естественно-гуманитарные исследования. 2024. № . 1(51). С. 323–327.

14. Кузьмин Ю. А. Кража персональных данных (криминологический аспект) // Oeconomia et Jus. 2020. № 3. С. 48–57. DOI: 10.47026/2499-9636-2020-3-48-57.

15. Новиков П. А. Совершенствования механизма защиты специальной категории персональных данных // Право и политика. 2025. № 2. С. 65–77. DOI: 10.7256/2454-0706.2025.2.73265

16. Ребязина В. А., Тункевичус Э. О. Цифровые профили пользователей сервисов совместного потребления в России: подход тематического моделирования // Вестник Московского университета. Серия 6. Экономика. 2021. Вып. 5. С. 183–206.

17. Русскевич Е. А. Об уголовной ответственности за незаконные действия с компьютерной информацией, содержащей персональные данные // Уголовный процесс. 2025. № 7(247). С. 53–59.

18. Русскевич Е. А. Цифровизация уголовного законодательства: непростые последствия простых решений // Вестник Университета имени О. Е. Кутафина. 2025. № 5(129). С. 26–33. DOI: 10.17803/2311-5998.2025.129.5.026-033.

19. Стяжкина С. А. Вопросы квалификации незаконного оборота персональных данных // Вестн. Удм. ун-та. Сер. Экономика и право. 2025. Т. 35, вып. 5. С. 945–952.

20. Талапина Э. В. Персональные данные: проблемы теории в судебных иллюстрациях // Российская юстиция. 2023. № 12. С. 57–65. DOI: 10.52433/01316761_2023_12_57.

21. Уголовное право Российской Федерации. Общая часть: учебник / А. Я. Гришко, Е. А. Антонян, А. Ю. Беляков [и др.]. Москва, 2025. 557 с. DOI: 10.12737/2007669.

22. Харуна И. О., Айдоноджи П. А., Бейда О. Д. Проблемы и перспективы нормативного регулирования системы электронных платежей в Нигерии // Journal of Digital Technologies and Law. 2024. № 2(2). С. 372–393. DOI: 10.21202/jdtl.2024.19.

23. Шутова А. А. Новеллы уголовного законодательства об ответственности за незаконный оборот персональных данных // Ученые записки Казанского университета. Серия: Гуманитарные науки. 2024. Т. 166, № 6. С. 122–134. DOI: 10.26907/2541-7738.2024.6.122-134.

24. Шутова А. А. Социальная обусловленность существования норм об уголовной ответственности за посягательства на персональные данные // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2015. № 4(32). С. 332–335.

СВЕДЕНИЯ ОБ АВТОРЕ

Волкова Анна Валерьевна

Соискатель кафедры уголовного права и процесса, Казанский инновационный университет имени В. Г. Тимирясова (ИЭУП) (г. Казань, Россия).

E-mail: avmail555@gmail.com

INFORMATION ABOUT THE AUTHOR

Anna V. Volkova

Postgraduate student in the Department of Criminal Law and Procedure, Kazan Innovative University named after V. G. Timiryasov (IEML) (Kazan, Russia).
E-mail: avmail555@gmail.com

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 26.05.2026.
Дата рецензирования статьи / Revised: 15.07.2026.
Дата принятия статьи к публикации / Accepted: 20.08.2026.

© Волкова А. В.