DOI: 10.24412/2075-7913-2026-2(102)-39-49

УДК 343.3/.7

Волкова А. В.

ОБЪЕКТИВНАЯ СТОРОНА СОСТАВА ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТАТЬЁЙ 272[1] УК РФ: ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ

Аннотация. *Настоящая статья представляет собой исследование объективной стороны состава преступления, предусмотренного ст. 272[1] УК РФ. Автор осуществляет детальное изучение элементов объективной стороны состава. Исследуются альтернативные формы преступного деяния: использование, передача (распространение, предоставление, доступ), сбор, хранение компьютерной информации, содержащей персональные данные, а также создание и обеспечение функционирования информационных ресурсов, предназначенных для незаконного оборота такой информации. Критическому изучению подвергается законодательная конструкция состава преступления. Детально исследуются способы получения персональной информации: неправомерный доступ к средствам обработки и хранения, иное вмешательство в функционирование средств, иной незаконный путь получения. Особое внимание уделяется квалифицирующим признакам состава преступления. Выявляются проблемы правоприменения, связанные с определением момента окончания преступления, установлением причинной связи в условиях цифровой среды, квалификацией продолжаемых и длящихся преступлений. Формулируются практические рекомендации по установлению признаков объективной стороны в процессе расследования и судебного рассмотрения.*

Ключевые слова: *объективная сторона преступления, ст. 272[1] УК РФ, общественно опасное деяние, персональные данные, компьютерная информация, неправомерный доступ, трансграничная передача данных*

Для цитирования: Волкова А. В. Объективная сторона состава преступления, предусмотренного статьёй 272[1] УК РФ: проблемы теории и практики // Проблемы права. 2026. № 2 (102). С. 39–49. DOI: 10.24412/2075-7913-2026-2(102)-39-49

Volkova A. V.

THE OBJECTIVE SIDE OF THE CRIME PROVIDED FOR BY ARTICLE 272[1] OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION: PROBLEMS OF THEORY AND PRACTICE

Abstract. *This article is a study of the objective side of the corpus delicti provided for in art. 272[1] of the Criminal Code of the Russian Federation. The author carries out a detailed study of the elements of the objective side of the composition. Alternative forms of a criminal act are investigated: the use, transfer (dissemination, provision, access), collection, storage of computer information containing personal data, as well as the creation and maintenance of information resources intended for the illicit trafficking of such information. The legislative structure of the corpus delicti is being critically studied. The methods of obtaining personal information are studied in detail: unauthorized access to the means of processing and storing, other interference in the functioning of the means, another illegal way of obtaining. Special attention is paid to the qualifying elements of the crime. The problems of law enforcement related to determining the moment of the end of a crime, establishing a causal*

relationship in the digital environment, and qualifying ongoing and ongoing crimes are identified. Practical recommendations are formulated for the identification of signs of an objective party in the process of investigation and judicial review.

Keywords: *objective side of the crime, Article 2721 of the Criminal Code of the Russian Federation, socially dangerous act, personal data, computer information, unauthorized access, cross-border data transfer*

For citation: Volkova A. V. The Objective Side of the Crime Provided for by Article 272[1] of the Criminal Code of the Russian Federation: Problems of Theory and Practice. *Problemy prava (Issues of Law)*. 2026. No. 2 (102). P. 39–49. DOI: 10.24412/2075-7913-2026-2(102)-39-49

Объективная сторона состава преступления представляет собой внешнюю, объективно выраженную сторону общественно опасного посягательства, характеризующуюся совокупностью признаков, описывающих процесс причинения вреда охраняемым уголовным законом общественным отношениям. В доктрине специалистами выделяются обязательные и факультативные признаки объективной стороны состава преступления [1, с.155–157].

Статья 272[1] УК РФ включает в себя шесть частей. Частями 1 и 2 ст. 272[1] УК РФ установлена ответственность за четыре альтернативные формы деяния: использование, передачу (с расшифровкой в виде распространения, предоставления, обеспечения доступа), сбор, хранение компьютерной информации, содержащей персональные данные, полученной незаконным путем. Части 3–5 ст. 272[1] УК РФ вводят квалифицирующие и особо квалифицирующие признаки, некоторые из которых относятся к объективной стороне: причинение крупного ущерба, трансграничная передача информации, причинение тяжких последствий. Часть 6 ст. 272[1] УК РФ устанавливает ответственность за создание и обеспечение функционирования информационного ресурса, предназначенного для незаконного оборота персональных данных.

Актуальность исследования объективной стороны состава преступления, предусмотренного ст. 272[1] УК РФ, обусловлена несколькими факторами. Во-первых, специфика преступлений в сфере компьютерной информации, характеризующихся нематериальным предметом посягательства, использованием информационных технологий, возможностью дистанционного совершения преступлений, создает уникальные проблемы установления признаков объективной стороны, определения момента окончания преступления, выявления причинной связи [2–5]. Во-вторых, отсутствие разъяснений Пленума Верховного Суда Российской Федерации обусловливает необходимость формирования теоретической правил по квалификации содеянного. Именно поэтому многими специалистами исследуются проблемы юридического конструирования состава преступления, предусмотренного ст. 272[1] УК РФ, и практики его применения [6–9].

В части 1 ст. 272[1] УК РФ установлена ответственность за четыре альтернативные формы общественно опасного деяния, образующие объективную сторону преступления: использование, передачу (конкретизируемую через синонимический ряд: распространение, предоставление, доступ), сбор и хранение компьютерной информации, содержащей персональные данные, полученной незаконным путем. Альтернативность деяний означает, что для наличия состава преступления достаточно совершения любого из указанных действий; совершение нескольких действий не образует множественности преступлений. Данная законодательная конструкция отражает стремление законодателя охватить все возможные формы незаконного оборота персональных данных, создать комплексную систему уголовно-правовых запретов на всех стадиях жизненного цикла оборота персональной информации: от первоначального сбора через хранение и использование до передачи третьим лицам.

Использование компьютерной информации, содержащей персональные данные, представляет собой применение информации в какой-либо деятельности, извлечение полезных свойств информации для достижения определенных целей субъекта, эксплуатацию информационного ресурса. Понятие использования является наиболее широким и абстрактным из всех форм деяния, охватывающим любые способы применения информации. Статья 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — Федеральный закон № 152-ФЗ

«О персональных данных») определяет использование персональных данных как действия (операции) оператора с персональными данными. Использование персональных данных может включать: применение информации для принятия решений в отношении субъекта персональных данных (например, использование незаконно полученной информации о кредитной истории для отказа в предоставлении услуг); использование персональных данных для совершения иных преступлений (например, использование данных банковских карт для хищения денежных средств, использование адресов и телефонов для совершения мошенничества); применение персональных данных в маркетинговых целях (рассылка рекламы, таргетирование); использование информации для шантажа, вымогательства, принуждения; любое иное применение информации, извлечение из нее пользы.

Важно разграничивать использование персональных данных как самостоятельное деяние и их использование в качестве средства совершения другого преступления. Если использование персональных данных выступает способом совершения иного преступления (например, мошенничества, вымогательства, незаконного предпринимательства), возникает вопрос о конкуренции норм или совокупности преступлений. Представляется, что в случае, когда использование незаконно полученных персональных данных образует объективную сторону другого состава преступления, содеянное квалифицируется по совокупности преступлений, предусмотренных ст. 272[1] УК РФ и соответствующей статьей о преступлении, совершенном с использованием персональных данных. Такой подход основывается на том, что ст. 272[1] УК РФ защищает право на безопасность персональных данных в цифровой форме, тогда как другие составы защищают иные объекты (собственность при мошенничестве, экономические интересы при незаконном предпринимательстве), что исключает поглощение одной нормой другой.

Передача компьютерной информации, содержащей персональные данные, конкретизируется законодателем через синонимический ряд: распространение, предоставление, доступ. Данная законодательная техника направлена на полный охват всех возможных форм передачи информации третьим лицам с учетом специфики цифровой среды. Передача в широком смысле означает действия, направленные на то, чтобы персональные данные стали доступны другим лицам, не имеющим законного права на доступ к ним. Так, *по данным следствия, в период с 31 января 2025 года помощник нотариуса, осуществляя деятельность на территории Индустриального района г. Ижевска, используя своё служебное положение, незаконно использовала и передавала компьютерную информацию, содержащую персональные данные граждан Российской Федерации. Эта информация была получена путём неправомерного доступа к средствам её обработки и хранения и передавалась третьим лицам посредством мессенджеров. В отношении нее было возбуждено уголовное дело по факту совершения преступления, предусмотренного п. «г» ч. 3 ст. 272.1 УК РФ*. Статья 3 Федерального закона № 152-ФЗ «О персональных данных» определяет распространение персональных данных как «действия, направленные на раскрытие персональных данных неопределенному кругу лиц». Распространение характеризуется публичностью, открытостью, доступностью информации для широкого круга субъектов: размещение персональных данных на общедоступных интернет-ресурсах; публикация в социальных сетях без ограничения доступа; рассылка по спискам адресов электронной почты неопределенному кругу лиц; публикация в средствах массовой информации; размещение в публичных базах данных, доступных без регистрации и аутентификации.

Предоставление персональных данных в отличие от распространения характеризуется передачей информации определенному лицу или ограниченному кругу лиц: передача базы данных клиентов конкурирующей организации; продажа персональных данных маркетинговым компаниям; передача информации частным детективам, коллекторам; предоставление доступа к информационным системам, содержащим персональные данные, конкретным лицам.

Обеспечение доступа к персональным данным означает создание технической возможности для третьих лиц получить персональные данные без непосредственной их передачи: предоставление учетных данных (логинов и паролей) для входа в информационные системы; размещение персональных данных на защищенных паролем ресурсах с предоставлением пароля доступа; настройка прав доступа

в информационных системах, позволяющая неуполномоченным лицам получать персональные данные; создание каналов утечки информации (бэкдоров, скрытых интерфейсов).

Сбор компьютерной информации, содержащей персональные данные, представляет собой действия, направленные на получение и аккумулирование персональной информации. Статья 3 Федерального закона № 152-ФЗ «О персональных данных» определяет сбор персональных данных как действия, направленные на получение персональных данных. Сбор предполагает активные действия по формированию массива персональных данных, созданию баз данных, агрегированию информации из различных источников. Сбор может осуществляться различными способами: копирование персональных данных из информационных систем, к которым осуществлен неправомерный доступ; парсинг (автоматизированный сбор) персональных данных с веб-сайтов, социальных сетей, публичных источников с использованием специализированных программ; агрегирование персональных данных из различных источников, сопоставление и объединение разрозненных данных для создания детальных профилей личности; получение персональных данных от третьих лиц, располагающих незаконно полученной информацией; извлечение персональных данных из перехваченного трафика, взломанных систем, утечек данных.

Важно различать законный и незаконный сбор персональных данных. Ст. 272[1] УК РФ криминализирует не любой сбор, а только сбор персональных данных, полученных незаконным путем, что выступает обязательным признаком объективной стороны. Если персональные данные собираются из общедоступных источников (официальные реестры, публичные профили в социальных сетях с открытым доступом, опубликованные контакты), при условии, что информация размещена самими субъектами персональных данных или с их согласия [10. С. 21], такой сбор не образует состава преступления, предусмотренного ст. 272[1] УК РФ. Вместе с тем, если общедоступная информация используется в целях, противоречащих законодательству о персональных данных, возможна административная ответственность по ст. 13.11 КоАП РФ (при отсутствии признака незаконного получения информации) [11]. По мнению Г. А. Есакова, в ситуации неправомерного оборота персональных данных, когда как минимум неправомерный доступ к ним получают сотрудники оператора, последние будут нести уголовную ответственность по ст. 272.1 УК РФ, а сам оператор — по указанным частям ст. 13.11 КоАП РФ [12. С. 10].

Хранение компьютерной информации, содержащей персональные данные, полученной незаконным путем, представляет собой фактическое обладание информацией, ее сохранение на носителях информации, в информационных системах в течение определенного времени. Статья 3 Федерального закона № 152-ФЗ «О персональных данных» определяет хранение персональных данных как действия, направленные на обеспечение сохранности персональных данных. Хранение может осуществляться на различных носителях и в различных формах: на жестких дисках компьютеров, серверов, съемных накопителях (флэш-накопителях, внешних жестких дисках); в облачных хранилищах, на удаленных серверах; в информационных системах, базах данных; в зашифрованном виде в специализированных хранилищах; в архивах, резервных копиях. Криминализация хранения незаконно полученных персональных данных отражает признание законодателем того, что само по себе обладание такой информацией создает угрозу правам и законным интересам субъектов персональных данных, поскольку потенциально может привести к ее использованию или распространению.

Хранение как форма преступного деяния создает специфические проблемы квалификации, связанные с определением момента окончания преступления и его продолжительности [13; 14]. Хранение по своей природе является длящимся преступлением: оно начинается с момента начала хранения (сохранения информации на носителе) и продолжается в течение всего времени, пока информация находится во владении виновного. Окончание хранения происходит в результате действий самого виновного (уничтожение информации, передача ее другим лицам) либо помимо его воли (изъятие информации правоохранительными органами, утрата носителей). Длящийся характер хранения имеет значение для исчисления сроков давности привлечения к уголовной ответственности: согласно п. 2 ст. 78 УК РФ сроки давности исчисляются с момента окончания преступления, а в отношении длящихся преступлений — с момента их прекращения. Следовательно, хранение неза-

конно полученных персональных данных будет считаться оконченным не в момент начала хранения, а в момент его прекращения, что может значительно продлевать срок давности.

Ключевым элементом объективной стороны состава преступления, предусмотренного ст. 272[1] УК РФ (за исключением части 6), выступает способ получения компьютерной информации, содержащей персональные данные. Криминализируются действия с персональными данными, «полученной путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование либо иным незаконным путем». Данная формулировка означает, что не любые действия с персональными данными образуют состав преступления, а только те, которые совершаются с информацией, полученной незаконным путем. Если персональные данные получены законным путем (с согласия субъекта, на основании договора, в силу закона), но затем используются с нарушением целей обработки или условий согласия, состав преступления, предусмотренный ст. 272[1] УК РФ, отсутствует.

Законодатель выделяет три альтернативные формы незаконного получения персональных данных, образующие способ совершения преступления. Первая форма — получение путем неправомерного доступа к средствам обработки или хранения персональных данных. За неправомерный доступ к компьютерной информации ст. 272 УК РФ установлена ответственность. Применительно к ст. 272[1] УК РФ неправомерный доступ означает получение персональных данных путем несанкционированного проникновения в информационные системы, содержащие такие данные, преодоления средств защиты информации (систем аутентификации, шифрования, контроля доступа), использования уязвимостей программного обеспечения, применения специализированных программных средств для взлома. Типичные способы неправомерного доступа включают: использование украденных, подобранных или полученных путем социальной инженерии учетных данных (логинов и паролей); эксплуатацию уязвимостей веб-приложений (SQL-инъекции, межсайтовый скриптинг, подделка межсайтовых запросов); применение вредоносных программ (троянских программ, кейлоггеров, программ удаленного администрирования); атаки на протоколы аутентификации и передачи данных; физический доступ к компьютерным системам с последующим копированием информации [15–17].

Вторая форма незаконного получения персональных данных –вмешательство в функционирование средств обработки или хранения. Данная формулировка охватывает способы получения информации, не связанные с неправомерным доступом в техническом смысле, но предполагающие воздействие на информационные системы, нарушающее нормальное функционирование средств обработки и защиты информации (отключение или нейтрализация средств защиты информации (систем обнаружения вторжений, антивирусного программного обеспечения, средств аудита); модификация настроек информационных систем для получения несанкционированного доступа к персональным данным; создание скрытых каналов утечки информации; перехват информации в процессе ее передачи по каналам связи; эксплуатация побочных каналов утечки информации (электромагнитное излучение, акустические каналы, анализ времени выполнения операций) [18;19].

Третья форма — получение персональных данных иным незаконным путем — представляет собой оценочную категорию, охватывающую все иные способы незаконного получения информации, не относящиеся к неправомерному доступу или иному вмешательству в функционирование средств обработки. Обеспечивает универсальность нормы, ее применимость к новым способам незаконного получения информации, появление которых обусловлено развитием информационных технологий. К получению персональных данных иным незаконным путем могут относиться: получение персональных данных от третьих лиц, которые получили их незаконным путем (приобретение баз данных на черном рынке, получение информации от инсайдеров); получение информации в результате утечек данных, вызванных действиями третьих лиц; получение персональных данных путем обмана субъекта персональных данных относительно целей обработки, идентичности получателя (фишинг, социальная инженерия); получение информации с использованием служебного положения вопреки установленным ограничениям; получение персональных данных из открытых источников, если размещение информации в открытом доступе само по себе было результатом незаконных действий третьих лиц.

Важно установление причинно-следственной связи между незаконным получением информации и последующими действиями с ней. Статья 272[1] УК РФ криминализирует не сам процесс незаконного получения информации (который может образовывать состав по ст. 272 УК РФ), а последующие действия с незаконно полученной информацией: использование, передачу, сбор, хранение. Следовательно, для квалификации по ст. 272[1] УК РФ необходимо установить, что лицо совершает указанные действия именно с той информацией, которая была получена незаконным путем. Если неправомерный доступ к информационной системе осуществлен одним лицом, а последующее использование или распространение персональных данных — другим лицом, действия первого квалифицируются по ст. 272 УК РФ, действия второго — по ст. 272[1] УК РФ, при наличии предварительного сговора — по ч. 3 ст. 272[1] УК РФ по признаку совершения группой лиц по предварительному сговору.

Определение конструкции состава преступления имеет важное значение для установления момента окончания преступления, квалификации приготовления и покушения, разграничения оконченного и неоконченного преступления. Части 1 и 2 ст. 272[1] УК РФ сконструированы по типу формального состава: диспозиция описывает только деяние (использование, передачу, сбор, хранение персональных данных), не указывая на необходимость наступления общественно опасных последствий в качестве обязательного признака объективной стороны. Формальная конструкция состава означает, что преступление считается оконченным с момента совершения деяния независимо от наступления последствий [20]. Фактически действия с персональными данными влекут негативные последствия для субъектов персональных данных (нарушение права на неприкосновенность частной жизни, риски причинения имущественного, морального, репутационного вреда), однако законодатель не включает эти последствия в конструкцию основного состава, что упрощает доказывание и обеспечивает более раннюю момент криминализации поведения.

Момент окончания преступления определяется в зависимости от формы деяния. При использовании персональных данных преступление считается оконченным с момента начала использования информации: применения ее для принятия решений, совершения на ее основе каких-либо действий, извлечения пользы из информации. Единичный акт использования образует оконченное преступление; последующее продолжение использования не образует новых преступлений, может учитываться при назначении наказания. При передаче (распространении, предоставлении, обеспечении доступа) персональных данных преступление считается оконченным с момента, когда информация стала доступна третьим лицам. Для распространения это момент размещения информации в открытом доступе, независимо от того, ознакомились ли с ней конкретные лица. Для предоставления — момент фактической передачи информации определенному лицу. Для обеспечения доступа — момент создания технической возможности получения информации третьими лицами, независимо от фактического использования этой возможности.

При сборе персональных данных преступление считается оконченным с момента получения информации виновным, ее фиксации на носителях информации, находящихся в его владении. Процесс сбора может быть продолжительным, растянутым во времени (например, длительный парсинг данных с множества источников), однако каждый акт получения информации образует продолжение единого преступления, а не самостоятельные преступления. При хранении персональных данных возникает специфическая ситуация, связанная с длящимся характером данного деяния. Преступление считается оконченным с момента начала хранения — сохранения информации на носителях, в информационных системах, находящихся во владении виновного. Однако в отличие от использования или передачи, где деяние имеет одномоментный характер, хранение продолжается во времени, образуя длящееся преступление. Юридическое окончание длящегося преступления происходит в момент его прекращения: уничтожения информации самим виновным, передачи ее другим лицам, изъятия правоохранительными органами.

Пункт «б» части 3 ст. 272[1] УК РФ связывает момент окончания с причинением крупного ущерба, которое должно находиться в причинной связи с действиями виновного по использованию, передаче, сбору или хранению персональных данных. В ст. 272[1] УК РФ законодатель не определяет количественный критерий крупного ущерба. Однако в примечании 2 к ст. 272

УК РФ отмечается, что «крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей». Представляется, что необходимы дальнейшие исследования для определения достаточности указанного ущерба в денежном выражении, ведь отмеченное положение появилось за долго до установления ответственности за незаконный оборот персональных данных. К примеру, следует ли включать в установление ущерба прямые имущественные потери субъектов персональных данных (хищение денежных средств с использованием персональных данных, имущественный вред от мошеннических действий), упущенную выгоду, а также расходы на устранение последствий компрометации персональных данных (замена документов, смена реквизитов, юридические расходы) и т. д.

В свою очередь ч. 5 ст. 272[1] УК РФ устанавливает ответственность за деяния, повлекшие тяжкие последствия, что также образует материальный состав. Тяжкие последствия представляют собой оценочную категорию, содержание которой определяется судом в каждом конкретном случае с учетом всех обстоятельств дела. Согласно пункту 14 постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» под тяжкими последствиями как квалифицирующим признаком в статьях 272–274[1] УК РФ следует понимать, в частности, «длительную приостановку или нарушение работы предприятия, учреждения или организации, получение доступа к информации, составляющей охраняемую законом тайну, предоставление к ней доступа неограниченному кругу лиц, причинение по неосторожности смерти, тяжкого вреда здоровью хотя бы одному человеку и т. п.».

Установление причинной связи в преступлениях, связанных с персональными данными, может представлять значительную сложность в силу опосредованного характера причинения вреда. Например, виновный распространяет в сети Интернет персональные данные граждан (адреса, номера телефонов, данные банковских карт); третьи лица, неустановленные или находящиеся за пределами юрисдикции России, используют эти данные для совершения мошенничества, в результате чего потерпевшим причинен имущественный ущерб. Можно ли вменить этот ущерб лицу, распространившему персональные данные? С точки зрения теории причинной связи, распространение персональных данных создало условия для совершения мошенничества третьими лицами, однако не было единственной и достаточной причиной наступления ущерба — требовались дополнительные действия третьих лиц. Представляется, что распространение персональных данных создает реальную и предвидимую возможность их использования для совершения преступлений против потерпевших, что обосновывает вменение причинения крупного ущерба.

Часть 4 ст. 272[1] УК РФ устанавливает особо квалифицирующий признак, относящийся к объективной стороне: совершение деяний, сопряженных с трансграничной передачей компьютерной информации, содержащей персональные данные, и (или) трансграничным перемещением носителей информации, содержащих персональные данные. Данный признак отражает повышенную общественную опасность деяний, связанных с выводом персональных данных граждан Российской Федерации за пределы юрисдикции российского государства, что создает риски утраты контроля над информацией, невозможности ее защиты правовыми средствами, использования в целях, противоречащих интересам национальной безопасности. Примечание 2 к ст. 272[1] УК РФ определяет трансграничное перемещение носителей информации как совершение действий по ввозу на территорию Российской Федерации и (или) вывозу с территории Российской Федерации машиночитаемого носителя информации, на который осуществлены запись и хранение персональных данных.

Трансграничная передача компьютерной информации, содержащей персональные данные, представляет собой передачу информации в электронной форме через государственную границу Российской Федерации посредством информационно-телекоммуникационных сетей. Типичные формы трансграничной передачи включают: размещение персональных данных на серверах, физически находящихся за пределами территории Российской Федерации (иностранные хостинг-провайдеры, облачные хранилища); передачу персональных данных иностранным

компаниям, организациям, физическим лицам; направление персональных данных по электронной почте, через мессенджеры получателям, находящимся за границей; загрузку персональных данных в иностранные информационные системы, сервисы, социальные сети с серверами за пределами Российской Федерации. Трансграничное перемещение носителей информации означает физическое перемещение через границу Российской Федерации материальных объектов, содержащих персональные данные в машиночитаемой форме: жестких дисков, твердотельных накопителей, флэш-накопителей, оптических дисков, мобильных устройств (ноутбуков, смартфонов, планшетов) с записанными на них персональными данными.

Квалификация деяния по ч. 4 ст. 272[1] УК РФ требует установления умышленного характера трансграничной передачи или перемещения: виновный должен осознавать, что осуществляет передачу информации за пределы Российской Федерации или перемещает носители через границу. Если лицо, распространяя персональные данные в сети Интернет, не осознавало и не должно было осознавать, что информация размещается на серверах, находящихся за пределами Российской Федерации, признак трансграничной передачи не вменяется. Вместе с тем в современных условиях, когда большинство глобальных интернет-сервисов используют распределенные системы хранения данных с серверами в различных юрисдикциях, осведомленность о трансграничном характере передачи может презюмироваться при использовании иностранных платформ.

Часть 6 ст. 272[1] УК РФ криминализирует качественно иное деяние, не связанное непосредственно с действиями над персональными данными, — создание и (или) обеспечение функционирования информационного ресурса, заведомо предназначенного для незаконных хранения, передачи персональных данных. Объективная сторона данного состава включает два альтернативных действия: создание информационного ресурса и обеспечение его функционирования.

Создание означает разработку, программирование, развертывание информационного ресурса: сайта в сети Интернет, страницы сайта, информационной системы, компьютерной программы.

Обеспечение функционирования означает поддержание работоспособности информационного ресурса: хостинг, техническое обслуживание, администрирование, обновление, обеспечение доступности.

Важным признаком объективной стороны выступает предназначенность информационного ресурса для незаконных действий с персональными данными. Предназначенность означает, что ресурс создан и функционирует специально для хранения, передачи, распространения незаконно полученных персональных данных; это главная функция ресурса. Примерами таких ресурсов являются: специализированные сайты (так называемые «даркнет-рынки»), где продаются базы персональных данных; форумы, предназначенные для обмена персональными данными; файлообменники, специализирующиеся на распространении скомпрометированных баз данных; информационные системы, агрегирующие персональные данные из утечек. Если ресурс имеет законное назначение, но используется отдельными пользователями для незаконных действий с персональными данными, состав преступления по ч. 6 ст. 272[1] УК РФ отсутствует для разработчика, однако нельзя исключать возможность привлечения третьих лиц к ответственности за обеспечение функционирования информационного ресурса.

Итак, объективная сторона характеризуется полиморфной структурой, включающей множественные альтернативные формы общественно опасного деяния: использование, передачу (распространение, предоставление, доступ), сбор, хранение компьютерной информации, содержащей персональные данные. Данная законодательная конструкция обеспечивает комплексный охват всех стадий незаконного оборота персональных данных, создает правовые механизмы противодействия различным формам посягательств на информационное самоопределение личности.

Обязательным криминообразующим признаком объективной стороны выступает способ получения информации: неправомерный доступ к средствам обработки и хранения, иное вмешательство в функционирование средств, иной незаконный путь получения. Данный признак дифференцирует преступное и непреступное поведение: криминализируются только действия с персональными данными, полученными незаконным путем, тогда как нарушения законодательства о персональных данных при обработке законно полученной

информации образуют административные правонарушения.

Момент окончания преступления дифференцируется в зависимости от формы деяния: при использовании и передаче — момент начала использования или фактической передачи информации; при сборе — момент получения информации; при хранении — момент начала хранения с признанием длящегося характера преступления. Квалифицированные признаки объективной стороны включают причинение крупного ущерба, трансграничную передачу информации или перемещение носителей, причинение тяжких последствий. Специфическая форма деяния, предусмотренная ч. 6 ст. 272[1] УК РФ, представляет собой создание инфраструктуры для незаконного оборота персональных данных, что отражает криминализацию не только непосредственных действий с персональными данными, но и создания условий для таких действий.

Литература

1. Уголовное право Российской Федерации. Общая часть: учебник / А. Я. Гришко, Е. А. Антонян, А. Ю. Беля-ков [и др.]. — Москва: Общество с ограниченной ответственностью «Научно-издательский центр ИНФРА-М», 2025. — 557 с. — ISBN 978-5-16-018447-0. — DOI 10.12737/2007669. — EDN NPYICM.
2. 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.
3. Винокуров В. Н. К вопросу о предмете преступления, предусмотренного статьей 272 УК РФ / В. Н. Винокуров, Е. А. Федорова // Законодательство. 2021. № 11. С. 73–80. EDN SYZUUT.
4. Гребенкин Ф. Б. Некоторые проблемные вопросы объективных признаков состава преступления, предусмотренного ст. 273 УК РФ / Ф. Б. Гребенкин, Л. А. Коврижных // Вестник гуманитарного образования. 2017. № 2. С. 71–77. EDN ZEUQRH.
5. Пелевина А. В. Общая характеристика преступлений в сфере компьютерной информации // Пробелы в российском законодательстве. 2015. № 4. С. 209–211. EDN UZFDSD.
6. 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. EDN LXPPWK.
7. Бегишев И. Р. Уголовно-правовая характеристика преступлений против безопасности персональных данных: анализ статьи 272[1] Уголовного кодекса Российской Федерации / И. Р. Бегишев, Н. Н. Рыбушкин // Вестник Дальневосточного юридического института МВД России имени И. Ф. Шилова. 2025. № 4(73). С. 19–23. EDN SGDXFX.
8. Денисович В.В., Кудряшов А. В., Перемолотова Л. Ю. Особенности применения современных цифровых технологий в сфере охраны персональных данных // Правопорядок: история, теория, практика. 2024. № 4 (43). С. 100–106. EDN: VZGALM.
9. 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 (129). С. 65–73. DOI:10.17803/2311-5998.2025.129.5.065-073.
10. Хохлова Е. В. Персональные данные в социальных сетях: теория и судебная практика толкования общедоступности // Научный вестник Омской академии МВД России. 2023. Т. 29, № 3 (90). С. 214–219. DOI:10.24412/1999-625X-2023-390-214-219.
11. Корешников Д. С. Конкуренция норм об охране персональных данных: разграничение статьи 272.1 УК РФ и статьи 13.11 КОАП РФ // Правопорядок: история, теория, практика. 2025. № . 3 (46). С. 49–54. DOI:10.47475/2311-696X-2025-46-3-49-54.
12. ЕЯсаков Г. А. Незаконный оборот персональных данных (ст. 272.1 УК РФ) // Уголовное право. 2025. № 11(183). С. 10–17. DOI 10.52390/20715870_2025_11_10. EDN VAZEMG.
13. Ектов А. С. Уголовно-правовые вопросы оценки длящихся преступлений // Проблемы правоохранительной деятельности. 2007. № 1. С. 33–36.
14. Ображиев К. В. Юридическая природа и признаки длящегося преступления // Всероссийский криминологический журнал. 2021. Т. 15, № 4. С. 442–455. DOI 10.17150/2500-4255.2021.15(4).442-455. EDN EGGTEP.
15. Защита информации от несанкционированного доступа в системах обработки данных при проектировании электронных средств / А. П. Галкин, Е. Г. Суслова, М. Аль Агбари, М. Аль Мураеш // Проектирование и технология электронных средств. 2007. № 2. С. 61–64. EDN KVWZLP.

16. Шодырова Б. Х. Актуальные технологии защиты от утечки конфиденциальной информации / Б. Х. Шодырова, Г. Т. Даненова, Б. С. Жекенова // Труды университета. 2011. № 3(44). С. 78–81. EDN TEMXFL.
17. Василькова, И. В. Классификация угроз информации / И. В. Василькова // Современные инновационные технологии и проблемы устойчивого развития общества: Материалы VIII международной научно-практической конференции, Минск, 14 мая 2015 года / Составители В. Н. Кривцов, Н. Н. Горбачев. Минск: ООО «Ковчег», 2015. С. 142–143. EDN YQTKPP.
18. Давыдов А. Е. Технические средства и методы защиты информации от утечки по техническим каналам на объектах информатизации / А. Е. Давыдов, Р. В. Максимов, О. К. Савицкий; А. Е. Давыдов, Р. В. Максимов, О. К. Савицкий; НИИ «Масштаб». Санкт-Петербург: Изд-во Политехнического ун-та, 2012. 192 с. ISBN 978-5-7422-3490-6. EDN QMXESB.
19. Защита информации при создании и эксплуатации сложных техниче-ских устройств и систем / В. В. Мухортов, И. Д. Королев, А. С. Мезенцев [и др.] // Информационная безопасность — актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности. 2017. № 1(8). С. 173–175. EDN LTXBWZ.
20. Ермакова О. В. Классификация формальных составов преступлений и ее значение // Вестник Восточно-Сибирского института МВД России. 2023. № . 4 (107). С. 126–133. DOI:10.55001/2312-3184.2023.38.28.011.

References

1. Criminal law of the Russian Federation. General part: textbook / A. Ya. Grishko, E. A. Antonyan, A. Yu. Belyakov [and others]. — Moscow: Limited Liability Company “Scientific Publishing Center INFRA–M”, 2025. — 557 p. — ISBN 978-5-16-018447-0. — DOI 10.12737/2007669. — EDN NPYICM.
2. Ruskevich E. A. Digitalization of criminal legislation: difficult consequences of simple decisions // Bulletin of O. E. Kutafin University. 2025. No. 5 (129). pp. 26–33. DOI:10.17803/2311-5998.2025.129.5.026-033.
3. Vinokurov V. N. On the issue of the subject of the crime provided for in Article 272 of the Criminal Code of the Russian Federation / V. N. Vinokurov, E. A. Fedorova // Legislation. 2021. No. 11. pp. 73–80. EDN SYZUUT.
4. Grebenkin F. B. Some problematic issues of objective recognition of the corpus delicti provided for in Article 273 of the Criminal Code of the Russian Federation / F. B. Grebenkin, L. A. Kovrizhnykh // Bulletin of Humanitarian Education. 2017. No. 2. pp. 71–77. EDN ZEUQRH.
5. Pelevina A. V. General characteristics of crimes in the field of computer information // Gaps in Russian legislation. 2015. No. 4. pp. 209–211. EDN UZFDSD.
6. Shutova A. A. Novelties of criminal legislation on responsibility for illegal trafficking of personal data // Scientific notes of Kazan University. Series: Humanities. 2024. Vol. 166, No. 6. pp. 122–134. DOI 10.26907/2541–7738.2024.6.122–134. EDN LXPPWK.
7. Begishev I. R. Criminal and legal characteristics of crimes against personal data security: analysis of Article 2721 of the Criminal Code of the Russian Federation / I. R. Begishev, N. N. Rybushkin // Bulletin of the I. F. Shilov Far Eastern Law Institute of the Ministry of Internal Affairs of Russia. 2025. No. 4(73). pp. 19–23. EDN SGDXFX.
8. Denisovich V. V., Kudryashov A. V., Peremolotova L. Yu. Features of the use of modern digital technologies in the field of personal data protection // Law and order: history, theory, practice. 2024. No. 4 (43). pp. 100–106. EDN: VZGALM.
9. Knyazkov A. A. Criminal law novella for violation of legislation on personal data (art. 2721 of the Criminal Code of the Russian Federation): features of the structure design and qualification issues // Bulletin of the O. E. Kutafin University, 2025. № 5 (129). pp. 65–73. DOI:10.17803/2311-5998.2025.129.5.065-073.
10. Khokhlova E. V. Personal data in social networks: theory and judicial practice of interpretation of public accessibility // Scientific Bulletin of the Omsk Academy of the Ministry of Internal Affairs of Russia. 2023. Vol. 29, No. 3 (90). pp. 214–219. DOI:10.24412/1999-625X-2023-390-214-219.
11. Koreshnikov D. S. Competition of personal data protection standards: the distinction between Article 272.1 of the Criminal Code of the Russian Federation and Article 13.11 of the Administrative Code of the Russian Federation // Law and order: history, theory, practice. 2025. No. 3 (46). pp. 49–54. DOI:10.47475/2311-696X-2025-46-3-49-54.
12. Yesakov G. A. Illegal trafficking of personal data (art. 272.1 of the Criminal Code of the Russian Federation) // Criminal law. 2025. No. 11(183). pp. 10–17. DOI 10.52390/20715870_2025_11_10. EDN VAZEMG.
13. Ektov A. S. Criminal law issues of assessment of ongoing crimes // Problems of law enforcement activity. 2007. No. 1. pp. 33–36.
14. Obrazhiev K. V. The legal nature and signs of a continuing crime // All-Russian Journal of Criminology. 2021. Vol. 15, No. 4. pp. 442–455. DOI 10.17150/2500–4255.2021.15(4).442–455. EDN EGGTEP.

15. Protection of information from unauthorized access in data processing systems in the design of electronic tools / A. P. Galkin, E. G. Suslova, M. Al Agbari, M. Al Muraesh // Design and technology of electronic devices. 2007. No. 2. pp. 61–64. EDN KVWZLP.
16. Shodyrova B. H. Actual technologies of protection against confidential information leakage / B. H. Shodyrova, G. T. Danenova, B. S. Zhekenova // Proceedings of the University. 2011. No. 3(44). pp. 78–81. EDN TEMXFL.
17. Vasilkova, I. V. Classification of information threats / I. V. Vasilkova // Modern innovative technologies and problems of sustainable development of society: Proceedings of the VIII International Scientific and Practical Conference, Minsk, May 14, 2015 / Compiled by V. N. Krivtsov and N. N. Gorbachev. Minsk: Kovcheg LLC, 2015. pp. 142–143. EDN YQTKPP.
18. Davydov A. E. Technical means and methods of protecting information from leakage through technical channels at informatization facilities / A. E. Davydov, R. V. Maksimov, O. K. Savitsky; A. E. Davydov, R. V. Maksimov, O. K. Savitsky; Scientific Research Institute “Scale”. Saint Petersburg: Publishing House of the Polytechnic University, 2012. 192 p. ISBN 978-5-7422-3490-6. EDN QMXESB.
19. Information protection in the creation and operation of complex technical devices and systems / V. V. Mukhortov, I. D. Korolev, A. S. Mezentsev [et al.] // Information security is an urgent problem of our time. The improvement of educational technologies for training specialists in the field of information security. 2017. No. 1(8). pp. 173–175. EDN LTXBWZ.
20. Ermakova O. V. Classification of formal crimes and its significance // Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2023. No. 4 (107). pp. 126–133. DOI:10.55001/2312-3184.2023.38.28.011.

Информация об авторах

Волкова Анна Валерьевна — соискатель кафедры уголовного права и процесса Казанского инновационного университета имени В. Г. Тимирясова (г. Казань, Российская Федерация). E-mail: avmail555@gmail.com

Information about the author

Volkova Anna V. — Postgraduate Student, Department of Criminal Law and Procedure, Kazan Innovative University named after V. G. Timiryasov (Kazan, Russia). E-mail: avmail555@gmail.com

Конфликт интересов отсутствует.
There is no conflict of interest.

Дата поступления статьи / Received: 22.11.2026

Дата рецензирования / Received: 25.11.2026

Дата принятия к опубликованию / Accepted: 27.11.2026