

Уголовно-правовая новелла за нарушение законодательства о персональных данных (ст. 272¹ УК РФ): особенности конструирования состава и вопросы квалификации

Аннотация. В статье рассматриваются различные аспекты технико-юридического совершенствования ст. 272¹, внесенной в уголовное законодательство Федеральным законом от 30.11.2024 № 421-ФЗ. Представляется, что достаточных криминологических оснований для расширения криминализации главы о компьютерных преступлениях путем конструирования самостоятельного состава преступления не имелось. С появлением ст. 272¹ УК РФ возникает конкуренция со ст. 137 УК РФ и ст. 13.11 КоАП РФ. Самостоятельная криминализация хранения персональных данных в электронной форме в качестве деяния средней тяжести не соответствует характеру и степени общественной опасности деяния. Отсутствие нормативно-правового регулирования в сфере противодействия незаконному обороту программ, предназначенных для незаконного оборота компьютерной информации, содержащей персональные данные, затрудняет возможность эффективного правоприменения, для чего необходимо внесение изменений в действующее законодательство криминального цикла и об оперативно-разыскной деятельности. Методологическая база исследования построена на диалектическом методе познания, общенаучных и частнонаучных методах исследования. Автор использует системный подход к анализу проблемы, что позволяет рассмотреть ее в комплексе.

Ключевые слова: персональные данные, компьютерная информация, биометрические персональные данные, трансграничная передача информации, телеграм-боты



**Александр Александрович
КНЯЗЬКОВ,**

доцент кафедры
уголовного права
Университета имени
О.Е. Кутафина (МГЮА),
кандидат юридических наук
aaknyazkov@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2025.129.5.065-073

Alexander A. KNYAZKOV,

Associate Professor, Department of Criminal Law
of the Kutafin Moscow State Law University (MSAL),
Cand. Sci. (Law)

aaknyazkov@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

**Criminal law novel for violation of the legislation
on personal data (Art. 272¹ of the Criminal Code of Russia):
design features of the composition and qualification issues**

Abstract. *The article examines various aspects of the technical and legal perfection of the novel of Article 272¹ of the Criminal Code, introduced into criminal law by Federal Law No. 421-FZ dated 11/30/2024. It seems that there were no sufficient criminological grounds for expanding the criminalization of the chapter on computer crimes by constructing an independent corpus delicti. With the advent of Article 272¹ of the Criminal Code, competition arose with Article 137 of the Criminal Code and Article 13.11 of the Administrative Code of the Russian Federation. The independent criminalization of storing personal data in electronic form as an act of moderate severity does not correspond to the nature and degree of public danger of the act. The lack of regulatory and legal regulation in the field of countering the illicit trafficking of programs designed for the illicit trafficking of computer information containing personal data makes it difficult to effectively enforce law enforcement, which requires amendments to the current legislation on the criminal cycle and operational investigative activities.*

Keywords: *personal data, computer information, biometric personal data, cross-border information transfer, telegram bots*

В России Интернетом пользуются в настоящее время не менее 130 млн человек, включая более 106 млн пользователей социальных сетей¹, куда они, в том числе по требованию соответствующих платформ, загружают свои различные персональные данные. Кроме того, по состоянию на ноябрь 2024 г. порядка 84 % граждан пользуются услугами маркетплейсов (Ozon, Wildberries и др.)², что также предполагает введение и сохранение персональных данных пользователей в электронном виде.

Фактически без персональных данных в настоящее время полноценное пользование сетью Интернет значительно ограничивается в своем функционале — персональные данные требуются для верификации пользователя, дающей дополнительные возможности проверки его платежеспособности и т.д. В этой связи все более актуальными становятся проблемы надлежащего обеспечения

¹ URL: <https://blog.manufact.pro/2024/07/01/digital-russia-2024/> (дата обращения: 23.03.2025).

² URL: <https://1prime.ru/20241112/marketpleys-852766679.html> (дата обращения: 23.03.2025).

уголовно-правовой защиты таких данных, недопустимости их несанкционированного распространения и использования в криминальных целях.

В последние годы на федеральном уровне предпринимаются определенные шаги по нормативному решению указанной проблемы. Так, в конце 2023 г. ужесточена ответственность за утечку персональных данных путем повышения размера административного штрафа для должностных и юридических лиц (ч. 1 ст. 13.11 КоАП РФ). В октябре 2024 г. в Совет Федерации Всероссийским союзом страховщиков направлен проект концепции добровольного страхования рисков неправомерной утечки персональных данных, предусматривающий возможность получения компенсации морального ущерба, вреда имуществу и здоровью³.

Несмотря на усилия федерального законодателя и правоохранительных органов, черный рынок оборота персональных данных процветает, чему способствуют и сами недобросовестные работники организаций, предоставляющие персональные данные клиентов на безвозмездной или возмездной основе для последующего неправомерного использования.

Длительное время применение уголовной ответственности за преступления, связанные с незаконным использованием персональных данных, являлось малоэффективным. Имеющиеся составы уголовно-наказуемых деяний (ст. 137, 183, 272 УК РФ) не позволяли добиваться неотвратимости ответственности и соразмерного наказания.

Как следствие, Федеральным законом от 30.11.2024 № 421-ФЗ криминализирован незаконный оборот персональных данных⁴. С 11.12.2024 в российском уголовном законе появилась ст. 272¹, предусматривающая два самостоятельных состава преступления, представленных в шести частях с различными квалифицирующими признаками.

Не оспаривая необходимость ужесточения уголовно-правового противодействия соответствующему виду общественно опасного посягательства, отметим ряд технико-юридических недостатков при конструировании нового состава в тексте уголовного закона.

1. Законодатель при проектировании рассматриваемой новеллы допустил существенную ошибку, выразившуюся в подмене объекта и предмета преступления ст. 272¹, что следует из текста пояснительной записки к законопроекту о внесении изменений в УК РФ. Так авторы-разработчики безосновательно определили компьютерную информацию, содержащую персональные данные, как объект преступления⁵. Речь в данном случае не идет о какой-то незначительной оплошности; по нашему убеждению, именно указанный сбой законодательной техники свидетельствует об ошибочности введения в гл. 28 УК нового состава преступления, что вряд ли будет отвечать потребностям правоприменительной практики и криминологическим реалиям.

³ Страховщики запустят возмещения от утечек данных до конца 2025 года // URL: <https://www.rbc.ru/finances/12/11/2024/6731fa139a79475b4427e441> (дата обращения: 23.03.2025).

⁴ Российская газета. 06.12.2024.

⁵ Пояснительная записка к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации» // URL: <https://sozd.duma.gov.ru/download/e55ce1c8-6725-497a-af16-e20265a80eed> (дата обращения: 23.03.2025).



Анализ изменений гл. 28 УК РФ свидетельствует, что отечественный законодатель своими точечными и не до конца проработанными поправками продолжил политику экспериментирования с нормами о компьютерных преступлениях. Так, несмотря на относительную устойчивость гл. 28 УК к нормотворческим реформам, законодатель сначала криминализировал неправомерное воздействие на критическую информационную инфраструктуру в 2017 г. (ст. 274¹ УК), что встретило преимущественно неодобрительную оценку в доктрине уголовного права по причине значительного количества технико-юридических дефектов данной нормы⁶. Следом законодатель добавил в гл. 28 УК в 2022 г. новый состав с административной преюдицией с весьма громоздкой диспозицией, перенасыщенной узкоспециализированной терминологией, по непонятным причинам снабженный дублирующим определением понятия должностного лица (в примечании к ст. 274² УК). Оценить эффективность ст. 274¹ УК пока не представляется возможным, поскольку новый состав преступления еще не применялся в правоприменительной практике.

Анализируемую нами ст. 272¹ УК РФ, введенную в конце 2024 г., также вряд ли обоснованно характеризовать в качестве необходимой правотворческой меры, поскольку данное преступление существенно не отличается по степени общественной опасности от основных составов преступлений в сфере компьютерной информации (ст. 272, 273), что могло бы оправдать конструирование специальной нормы⁷. В данном конкретном случае мы такого не наблюдаем, так как законодатель мог бы пойти по пути углубления дифференциации уголовной ответственности за указанные выше «компьютерные» преступления, добавив в соответствующие составы гл. 28 УК квалифицирующий признак «в отношении компьютерной информации, составляющей персональные данные», что не требовало бы включения в уголовный закон нового состава преступления.

2. Законодатель описывает диспозицию ст. 272¹ посредством указания на три способа совершения преступления путем (1) неправомерного доступа к средствам обработки компьютерной информации с персональными данными, (2) хранения или иного вмешательства в их функционирование либо (3) иным незаконным путем.

Если первые два описанных в законе способа не встречают существенных нареканий, то последний из них обоснованно вызывает вопросы. Пока в отсутствие какой-либо судебной практики складывается предположение, что указанный законодателем «иной незаконный путь» будет приравняться правоприменителем к не установленному (не доказанному) органами следствия пути, чем будет неизбежно допускаться расширительное толкование закона с

⁶ См., например: Бражник С. Д. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (статья 274.1 УК РФ): о некоторых проблемах дифференциации ответственности // Актуальные проблемы уголовного права на современном этапе (вопросы дифференциации ответственности и законодательной техники). 2020. № 9. С. 92—101.

⁷ Князьков А. А. Освобождение от уголовной ответственности по делам об экономических преступлениях (гл. 22 УК РФ): вопросы дифференциации и законодательной техники : дис. ... канд. юрид. наук. 2015. С. 27.

упрощением процесса доказывания и квалификации содеянного, что, в свою очередь, будет являться нарушением права обвиняемого на защиту от такого неконкретизированного обвинения в совершении преступления средней тяжести (ч. 1, 2 и 6) или тяжкого (ч. 3, 4 и 5 ст. 272¹ УК РФ) преступления.

Думается, что практика может сложиться иным путем, отличающимся от устоявшейся позиции Пленума Верховного Суда РФ применительно к ст. 272 УК РФ. Так, высшая судебная инстанция указала, что по уголовным делам о преступлениях, предусмотренных ст. 272 УК, неправомерным доступом к компьютерной информации является получение или использование такой информации в нарушение установленного нормативными правовыми актами порядка независимо от формы такого доступа⁸.

И если в целях применения ст. 272 УК Пленум Верховного Суда РФ раскрыл неправомерный доступ посредством бланкетного приема, то по ст. 272¹ УК имеются разумные основания прогнозировать практику упрощения квалификации содеянного, исходя из того, что если лицо изначально не могло получить доступ к персональным данным законным путем, следовательно, презюмируется уголовная противоправность по ст. 272¹ УК, т.е. получение субъектом доступа к информации с персональными данными незаконным путем.

При этом такой подход может быть удобен правоприменителю и избавит его от обязанности доказывать криминообразующий признак состава преступления, что не будет законным и не соответствует криминологическим реалиям⁹, поскольку по новой статье наказуемым является уже сам по себе факт хранения компьютерной информации, содержащей персональные данные, а не ее хранение в целях, например, последующего сбыта либо иного использования, что было бы допустимым.

Так, содеянное по ч. 1 рассматриваемой статьи образует состав преступления средней тяжести с санкцией в виде лишения свободы до 4 лет, что сопоставимо с хранением особо ценных диких животных и водных биологических ресурсов, занесенных в Красную книгу России (ч. 1 ст. 258¹ УК), и даже строже по наказанию, чем хранение наркотиков (ч. 1 ст. 228 УК), либо психотропных веществ (ч. 1 ст. 228³ УК), что вряд ли оправданно с точки зрения характера и степени общественной опасности сопоставляемых деяний. В этой связи мы не можем

⁸ Постановление Пленума Верховного Суда РФ от 15.12.2022 № 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». П. 15 // СПС «КонсультантПлюс».

⁹ Вместе с тем подобная порочная практика встречается по другим категориям дел, в частности о незаконном обороте наркотиков. Так, например, суд указал, что «вывод суда первой инстанции о бланкетном характере диспозиции инкриминируемого ФИО1 преступления противоречит тексту уголовного закона, поскольку часть 1 статьи 228 УК РФ не содержит ссылки на нарушение или несоблюдение норм и правил, утверждаемых иными нормативными актами» (апелляционное постановление Ленинградского областного суда от 10.01.2025 № 22-146/2025 // СПС «КонсультантПлюс»). С данным подходом суда согласиться не представляется возможным.



согласиться с авторами — разработчиками законопроекта о введении ст. 272¹ УК¹⁰, которые, по нашему мнению, не обосновали необходимость конструирования основного состава преступления в виде преступления средней тяжести. Ссылки на увеличение сроков давности уголовного преследования и погашения судимости не являются гарантией эффективного уголовно-правового противодействия криминальному обороту персональных данных.

3. Характеризуя норму ст. 272¹ УК, нам приходится затронуть проблематику установления содержания понятия «персональные данные» и его соотношения с предметом преступления, предусмотренного ст. 137 УК.

В связи с введением в УК ст. 272¹ криминализация незаконного оборота персональных данных в компьютерной (электронной) форме охватывается гл. 28 УК; в том же случае, если субъект совершает противоправные действия (собирает или распространение) сведений, образующих личную тайну гражданина в «бумажной» форме, то уголовная ответственность будет наступать по ст. 137 УК. Во избежание возможной конкуренции составов указанных преступлений одновременно с внесением поправок в гл. 28 УК законодатель поправил диспозицию ст. 137 УК.

Согласно судебной статистике за 2023 г., по ч. 1 ст. 137 УК было осуждено 224 человека¹¹. С учетом внесенных законодателем вышеуказанных изменений в гл. 28 УК можно прогнозировать, что дальнейшее применение ст. 137 УК будет неуклонно снижаться. До введения в УК ст. 272.1 уголовные дела в отношении посягательств на персональные данные, как правило, возбуждались по ст. 137 УК. Однако частная жизнь по смыслу ст. 137 УК не охватывает всего объема персональных данных.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Закон № 152-ФЗ) определяет персональные данные как любую информацию, которая относится к прямо или косвенно определенному или определяемому физическому лицу¹². Несмотря на то что данное определение было изначально сформулировано законодателем и не менялось на протяжении всего периода применения Закона № 152-ФЗ, в доктрине и на практике толкование содержания понятия персональных данных всегда сопровождалось дискуссиями.

Следует заметить, что статьей 13.11 КоАП РФ, предусматривающей административную ответственность за нарушения требований законодательства в области персональных данных, в том числе связанных с обработкой таких данных, охватываются незаконные сбор, хранение, использование и передача как самих персональных данных, так и баз, включающих такие данные.

В то же время в диспозиции ч. 1 ст. 272¹ УК отсутствуют конститутивные признаки, позволяющие четко отграничивать преступление от административного правонарушения по ст. 13.11 КоАП, что неизбежно приведет к конкуренции указанных норм и рассогласованию практики их применения.

¹⁰ Пояснительная записка к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации».

¹¹ URL: <https://stat.ani-пресс.рф/stats/ug/t/14/s/17> (дата обращения: 23.03.2025).

¹² СПС «КонсультантПлюс».

4. Квалифицированный вид преступления, установленный ч. 2 ст. 272¹ УК, предусматривает ответственность за деяние, совершенное в отношении компьютерной информации, содержащей персональные данные несовершеннолетних лиц, специальные категории персональных данных или биометрические персональные данные.

Повышенная общественная опасность незаконного оборота указанных видов персональных данных очевидна и не вызывает сомнений, поскольку презюмируется наступление негативных последствий для лица при их несанкционированном использовании. Так, к специальной категории персональных данных относятся данные о расе, национальности, состоянии здоровья, об интимной жизни, о политических взглядах, религиозных или философских убеждениях (ч. 1 ст. 10 Закона № 152-ФЗ).

Перечень типов персональных данных, отнесенных к категории специальных, является в силу закона закрытым. Однако отнесение той или иной информации к данной категории персональных данных может быть сопряжено с рядом квалификационных сложностей. Например, фотография индивида может выявлять его расовую или этническую принадлежность, а в некоторых случаях — и политические убеждения при наличии соответствующего контекста¹³.

К числу биометрических персональных данных, указанных в ч. 2 ст. 272¹ УК, закон относит сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (ч. 1 ст. 11 Закона № 152-ФЗ), например, фотографическое изображение и иные сведения, используемые для обеспечения однократного и (или) многократного прохода на охраняемую территорию и установления личности гражданина¹⁴.

5. Квалифицированные составы ст. 272¹ УК влекут повышенную уголовную ответственность, в частности, за деяния, сопряженные с трансграничной передачей компьютерной информации, содержащей персональные данные, или трансграничным перемещением носителей информации, содержащих персональные данные (ч. 4). Очевидно, что конструирование данного особо квалифицирующего признака рассчитано на применение в отношении облачных сервисов и серверов на территории иностранных (так называемых недружественных) государств.

Также предусмотрена уголовная ответственность за создание или обеспечение функционирования информационного ресурса, заведомо предназначенного для незаконных хранения, передачи (распространения, предоставления, доступа) компьютерной информации, содержащей персональные данные, полученной незаконным путем (ч. 6).

6. В силу прямого указания закона действие новой статьи УК РФ не распространяется на случаи обработки персональных данных физическими лицами исключительно для личных и семейных нужд.

¹³ Савельев А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М. : Статут, 2021. С. 300.

¹⁴ Письмо Минцифры России от 17.07.2020 № ОП-П24-070-19433 «О рассмотрении обращения» // СПС «КонсультантПлюс».



Очевидно, что это примечание к статье было обусловлено необходимостью избежать чрезмерно расширительного и произвольного толкования, как было, например, при оценке действий родителя, использующего мобильное приложение родительского контроля, позволяющего слышать происходящее в непосредственной близости от ребенка, для чего потребовалось вмешательство Конституционного Суда РФ с корректировкой сложившейся правоприменительной практики¹⁵, или же привлечение к уголовной ответственности фермеров по ст. 138¹ УК за использование технических средств контроля за домашними животными и скотом¹⁶.

Здесь возникает вопрос об уголовно-правовой оценке деяния в случае, если персональные данные требуются для иной, заведомо некриминальной цели, например, при необходимости установления идентификаторов истца или ответчика при подаче искового заявления в суд, перечисленных в п. 2—3 ч. 2 ст. 131 ГПК РФ.

На наш взгляд, по духу закона сбор таких сведений не должен квалифицироваться по ст. 137 УК РФ ввиду отсутствия субъективной стороны данного состава преступления, однако позиция судебной практики складывается иначе. Так, Пленум Верховного Суда РФ указывает, что не влечет уголовную ответственность собирание или распространение таких сведений лишь в государственных, общественных или иных публичных интересах¹⁷. Из этого разъяснения следует, что незаконный сбор идентификаторов участников судопроизводства не может сводиться к вышеперечисленным интересам, поскольку преследует личный интерес по судебной защите нарушенных прав и законных интересов.

7. Частью 6 ст. 272.1 УК РФ криминализировано создание и (или) обеспечение функционирования информационного ресурса, заведомо предназначенного для незаконных хранения, передачи (распространения, предоставления, доступа) компьютерной информации, содержащей персональные данные, полученной незаконным путем.

Фактически речь идет о введении уголовной ответственности за создание различных программ-роботов, телеграм-ботов и т.п., позволяющих получить всю необходимую персональную информацию преимущественно на возмездной основе путем автоматизированной обработки компьютерной информации в Интернете, не требующей человеческого участия, с существенной экономией времени на обработку информации, содержащей персональные данные.

Примеры следственно-судебной практики применения ст. 273 УК РФ в отношении вредоносного программного обеспечения показывают, что создателей таких

¹⁵ Постановление Конституционного Суда РФ от 18.01.2024 № 2-П «По делу о проверке конституционности части первой статьи 137 Уголовного кодекса Российской Федерации в связи с жалобой гражданина П. О. Вильке» // СПС «КонсультантПлюс».

¹⁶ Абдулин Р. С. Страсти по «Закону о сборе валежника»: от теории к практике // Уголовное судопроизводство. 2021. № 1. С. 31.

¹⁷ Постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145¹ Уголовного кодекса Российской Федерации)». Абз. 2 п. 2 // СПС «КонсультантПлюс».

роботов и программ-ботов будет сложно не только выявлять, но и привлекать к уголовной ответственности ввиду недостаточной регламентированности этой процедуры на законодательном уровне (в первую очередь в нормах Закона об оперативно-разыскной деятельности) и отсутствия организационных мероприятий, направленных на совершенствование системы выявления, раскрытия и противодействия преступлениям в сфере незаконного оборота персональных данных.

БИБЛИОГРАФИЯ

1. *Абдулин Р. С.* Страсти по «Закону о сборе валежника»: от теории к практике // Уголовное судопроизводство. — 2021. — № 1. — С. 27—31.
2. *Бражник С. Д.* Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (статья 274.1 УК РФ): о некоторых проблемах дифференциации ответственности // Актуальные проблемы уголовного права на современном этапе (вопросы дифференциации ответственности и законодательной техники). — 2020. — № 9. — С. 92—101.
3. *Князьков А. А.* Освобождение от уголовной ответственности по делам об экономических преступлениях (гл. 22 УК РФ): вопросы дифференциации и законодательной техники : дис. ... канд. юрид. наук. — 2015. — 219 с.
4. *Савельев А. И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». — М. : Статут, 2021. — 468 с.

