УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА.
СЕРИЯ ГУМАНИТАРНЫЕ НАУКИ

2024, Т. 166, кн. 6
С. 122–134

ISSN 2541-7738 (Print)
ISSN 2500-2171 (Online)

УГОЛОВНО-ПРАВОВЫЕ НАУКИ

ОРИГИНАЛЬНАЯ СТАТЬЯ

УДК 343.3/.7

doi: 10.26907/2541-7738.2024.6.122-134

НОВЕЛЛЫ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА ОБ ОТВЕТСТВЕННОСТИ ЗА НЕЗАКОННЫЙ ОБОРОТ ПЕРСОНАЛЬНЫХ ДАННЫХ

А.А. Шутова

Казанский инновационный университет имени В. Г. Тимирясова, г. Казань, 420111, Россия

Аннотация

В настоящем исследовании впервые проведен критический юридический анализ новой нормы об ответственности за незаконные использование и (или) передачу, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконного хранения и (или) распространения. Выявлены недостатки и противоречия в конструировании ст. 272[1] Уголовного кодекса Российской Федерации, предложены пути решения отдельных проблем, связанных с правоприменением данной нормы. Разработаны теоретические предложения и рекомендации по совершенствованию законодательства и практики применения в сфере незаконного оборота компьютерной информации, содержащей персональные данные несовершеннолетних лиц, специальные категории персональных данных и (или) биометрические персональные данные. Выявлены проблемы, которые могут возникнуть в процессе квалификации деяний, сопряженных с трансграничной передачей компьютерной информации, содержащей персональные данные, и (или) трансграничным перемещением носителей информации, содержащих персональные данные. Основные предложения в публикации могут быть использованы для модернизации уголовно-правовой охраны персональных данных, дальнейшего развития отечественной доктрины уголовного права об ответственности за преступления в сфере компьютерной информации.

Ключевые слова: биометрические персональные данные, персональные данные несовершеннолетних, преступления в сфере компьютерной информации, трансграничная передача персональных данных, утечка персональных данных, цифровые преступления

1. Введение

Новеллой уголовного законодательства являются изменения, обусловленные принятием Федерального закона от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» (ФЗ № 421), вступающего в силу 11 декабря 2024 г. Уголовный кодекс Российской Федерации

(УК РФ) дополнен новой ст. 272[1] УК РФ, устанавливающей ответственность за незаконный оборот компьютерной информации, содержащей персональные данные, путем осуществления компьютерной атаки, а также внесены соответствующие изменения в ст. 137 и 272 УК РФ, связанные с принятием нового уголовно-правового запрета.

Начнем с небольшого экскурса, позволяющего определить обусловленность принятия подобных изменений. Так, 4 декабря 2023 г. проект федерального закона (законопроект № 502113-8[1]) о внесении изменений в УК РФ был внесен в Государственную думу Российской Федерации сенаторами А.А. Турчаком, А.А. Клишасом, И.В. Руковишниковым и депутатами Государственной думы А.Е. Хинштейном, И.А. Панькиной, Д.Ф. Вяткиным и А.И. Немкиным, являющимися субъектами законотворческой инициативы. Несомненно, указанные должностные лица активно лоббируют принятие законов в свете форсированной цифровизации и применяемых цифровых технологий, в том числе в противоправных целях. На законопроект поступили официальные отзывы о недостатках от Правительства Российской Федерации и Верховного Суда Российской Федерации.

В пояснительной записке указывается, что особо значимыми являются проблемы защиты персональных данных вследствие участившихся случаев неправомерного доступа к ним, распространения и использования в преступных целях, в том числе мошенничеств, что повлияло в совокупности на криминализацию. Приведены сведения об случаях утечки персональных данных и их последствиях. Уточняется, что чаще «утекают» базы данных, содержащие записи о конкретных людях и являющиеся компьютерной информацией.

По результатам проведенной существенной доработки новая редакция ст. 272[1] УК РФ представлена в ином виде, отличном от ее первоначальной редакции, на что поступил официальный отзыв Правительства Российской Федерации о поддержке проекта закона.

Однако, как представляется, с учетом новизны представленного уголовно-правового запрета, наличия в нем множества оценочных категорий, отсутствия разъяснений о квалификации подобных уголовно наказуемых деяний, исследование состава преступления в целях облегчения процесса правоприменения и совершенствования является весьма перспективным и важным направлением.

2. Объект преступного посягательства

Законодатель, расположив названную норму в главе 28 УК РФ, определяет родовым объектом преступления общественные отношения, охраняющие общественный порядок и общественную безопасность. По мнению Е.С. Смольянинова, определение родовым объектом преступлений в сфере компьютерной информации отношений общественной безопасности спорно [1, с. 118–119]. Полагаем, что 28 глава УК РФ, содержащая уголовно-правовые запреты совершения уголовно наказуемых деяний в сфере компьютерной информации,

[1] Законопроект № 502113-8. URL: https://sozd.duma.gov.ru/bill/502113-8, свободный.

в целом должна быть выделена в самостоятельные раздел и главу уголовного закона России [2, с. 662–663].

Включение ст. 272–274[2] УК РФ в раздел IX Особенной части УК РФ позволяет определить объект рассматриваемых преступлений. При этом непосредственный объект является частью родового объекта, в связи с чем возникает вопрос о том, как в случае причинения вреда конституционным правам конкретной личности будет страдать (или поставлена под угрозу) общественная безопасность. Так, достаточно нередки случаи неправомерного доступа к компьютерной информации для дальнейшего распространения порнографических материалов[2], которые квалифицируются по совокупности составов преступлений, предусмотренных ч. 1 ст. 272 и ст. 242 УК РФ. В другом аналогичном случае, как установило следствие, обвиняемый в период с мая по август 2021 г. в процессе общения в одной из социальных сетей с 14-летней и 15-летней жительницами Сарапульского района предложил им направить свои фотоизображения в обнаженном виде. Получив фотоизображения, он распространил их в информационно-телекоммуникационной сети Интернет своим знакомым. Кроме того, обвиняемый направил 31-летней местной жительнице изображение порнографического характера, полученное в сети Интернет[3]. Приведенные примеры свидетельствуют о том, что своими действиями виновные посягают на общественную безопасность и на неприкосновенность частной жизни лица. Поэтому злоумышленника обвиняют в совершении двух эпизодов преступления, предусмотренного ч. 1 ст. 137 УК РФ и п. «г» ч. 2 ст. 242[1] УК РФ.

Поэтому уголовно наказуемые деяния, перечисленные в 28 главе УК РФ, необходимо выделить в самостоятельный раздел и главу Особенной части УК РФ, сформулировав название как «Преступления против цифровой безопасности».

Интересно и вызывает дискуссию законодательное решение о расположении нормы об ответственности за «незаконный оборот» персональных данных именно в 28 главе, а не в 19 главе УК РФ. Случаи утечки персональных данных, в частности баз данных, причиняют вред предприятиям и компаниям, конкурентоспособность которых зависит от деловой репутации организации (частные предприятия), страдают и сами граждане, которые могут стать жертвами мошенничества, лишиться денежных средств или испортить, к примеру, кредитную историю. Поэтому совершение уголовно наказуемого деяния, предусмотренного ст. 272[1] УК РФ, не всегда непосредственно посягает на общественную безопасность, а может затрагивать и личные интересы, и непосредственно безопасность самого человека, а также отношения в сфере экономической деятельности, когда может быть, к примеру, подорвана деловая репутация юридических лиц, что также, как мы полагаем, подтверждает нашу позицию о выделении 28 главы УК РФ в самостоятельный раздел и главу Особенной части УК РФ.

---

[2] По факту показа порно в Москве возбуждено уголовное дело. URL: https://www.rbc.ru/society/20/01/2010/5703d8f19a7947733180ddd6, свободный.

[3] В г. Сарапуле завершено расследование уголовных дел по обвинению 18-летнего местного жителя в нарушении неприкосновенности частной жизни и распространении порнографических материалов. URL: https://udm.sledcom.ru/news/item/1705838/, свободный.

2.1. Предмет преступного посягательства. Однако исследование объекта преступления невозможно без определения предмета преступного посягательства, являющегося обязательным признаком состава. Предмет преступления – не просто охраняемая законом компьютерная информация, а информация, содержащая персональные данные.

Однако согласно ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ФЗ № 152) обработка персональных данных может осуществляться без использования «средств вычислительной техники». Следовательно, законодатель выделяет в специальный предмет только персональные данные, обрабатываемые с помощью цифровых технологий, и именно они подлежат уголовно-правовой охране. В свою очередь, документарные данные не подлежат уголовно-правовой охране по данной статье, или же должен применяться иной состав преступления. Уголовно-правовой охране подлежит своеобразная «цифровая база данных», которая представляет собой разновидность охраняемой законом компьютерной информации, хотя это всего лишь форма их предоставления (цифровой или документированный вид), а ценностью является именно специфический предмет – персональные данные. К примеру, коммерческая тайна, вызывающая определенный интерес у злоумышленника, также может быть представлена в виде базы данных, однако законодатель посчитал, что ее неправомерное собирание, распространение и использование в первую очередь посягают на общественные отношения в сфере нормальной экономической деятельности субъектов (ст. 183 УК РФ).

Несомненно, действие уголовно-правовой нормы направлено в первую очередь на злоумышленников – хакеров, которые совершают компьютерные атаки на информационные системы персональных данных с целью «неправомерной передачи (предоставления, распространения, доступа) персональных данных» (ч. 12 ст. 19 Федерального закона № 152-ФЗ).

Таким образом, исследование объекта и предмета преступления, предусмотренного ст. 272^1 УК РФ, позволяет сделать выводы о том, что:

1) имеется потребность в выделении преступлений в сфере компьютерной информации в самостоятельный раздел УК РФ;

2) персональные данные граждан, обрабатываемые с помощью цифровых технологий (в законе – средств вычислительной техники), представляют собой информационную систему (базу персональных данных), поэтому можно допустить (исходя из формы ее предоставления) расположение данного уголовно-правового запрета именно в 28 главе УК РФ;

3) необходимо продумать и установить режим уголовно-правовой охраны персональных данных, не обрабатываемых с использованием цифровых технологий («документированных»), если имеется социальная потребность в этом.

2.2. «Документированные» персональные данные как предмет преступлений. Говоря о «документированных персональных данных», стоит уточнить, что их неправомерное собирание или распространение можно квалифицировать по ст. 137 УК РФ. Однако на данный момент остается недостаточно ясным следующее: являются ли сведения о частной жизни лица, составляющие его личную или семейную тайну, персональными данными, по каким критериям их следует

между собой разграничивать [3, с. 11–12]. Критикой представленной легальной позиции занимается И.Г. Ильин [4, с. 126].

Указанная проблема обусловлена тем, что законодательное определение понятия «персональные данные» является чрезмерно абстрактным, позволяющее относить к таковым «любые сведения» (по мнению субъекта). Кроме того, конкретного перечня сведений, относимых к персональным, в законе не выделено [5, с. 333]. Согласно ст. 3 Федерального закона № 152-ФЗ, «сведения, составляющие личную и семейную тайну, могут быть отнесены к персональным данным лица». В разъяснении Верховного Суда Российской Федерации не определено, какой перечень сведений следует относить к личной и семейной тайне, не сформулировано их отличие от персональных данных, а следовательно, отсутствуют и критерии отграничения уголовной ответственности от административной.

В связи с уязвимостью персональных данных необходимо установить уголовную ответственность за незаконную обработку иных персональных данных, причинившую существенный вред правам и законным интересам лица, внеся соответствующие изменения в ст. 137 УК РФ. Соответственно, предмет преступления, предусмотренный ст. 137 УК РФ, расширится. При этом следует закрепить более строгий вид и размер наказания за незаконное распространение подобных сведений по сравнению с их незаконным сбором и обработкой.

3. Объективная сторона состава преступления

Далее перейдем к рассмотрению объективной стороны состава преступления, которую образуют деяния в виде незаконного использования и (или) передачи (распространения, предоставления, доступа), сбора и (или) хранения компьютерной информации, содержащей персональные данные.

Возникают вопросы по поводу юридической техники конструирования уголовно-правового запрета, требуется несколько раз внимательно прочитать норму, чтоб понять ее смысл и состав по законодательной конструкции; к тому же статья так перегружена оценочными категориями, что это, безусловно, делает ее сложной для процесса правоприменения. Скорее всего, уголовно-правовая норма вызовет проблемы квалификации в судебно-следственной практике.

Для начала остановимся более подробно на рассмотрении альтернативных действий, совершение каждого из которых достаточно для привлечения к уголовной ответственности. Учитывая то, что диспозиция представленной нормы является бланкетной, неизбежно возникнет необходимость изучения ее во взаимосвязи с Федеральным законом № 152-ФЗ.

Начнем с того, что компьютерная информация, содержащая персональные данные, должна быть получена ***незаконным путем*** (путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование либо иным способом). Указанные действия схожи с деянием, образующим объективную сторону преступления, предусмотренного ч. 1 ст. 272 УК РФ. Так, согласно п. 5 постановления Пленума Верховного Суда Российской Федерации 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 инфор-

мационно-телекоммуникационных сетей, включая сеть “Интернет”» (далее – постановление Пленума), под неправомерным доступом понимается «получение или использование такой информации без согласия обладателя информации» (Пост. № 37). «Неправомерный доступ» составляют деяния в виде получения или использования информации. На наш взгляд, проблемным вопросом является такое понятие, как «использование», в контексте неправомерного доступа, предусмотренного ст. 272 УК РФ. Состав преступления требует наступления негативных общественно опасных последствий в виде блокирования, копирования, модификации и уничтожения этих сведений. В контексте неправомерного доступа говорить об использовании сведений уже не совсем корректно. Использование – это следующий этап после завладения информацией (получения информации), то есть необходимо вначале завладеть ею, а потом использовать ее, иначе нарушается последовательность технологических этапов жизненного цикла цифровой (в контексте действующей редакции УК РФ – компьютерной) информации. Полагаем, что наличие приведенной законодательной неточности подтверждается и разъяснением суда, в п. 5 которого приведены примеры «получения» сведений, а не «использования». Поэтому нам представляется, что словосочетание «или использование» нужно исключить из постановления Пленума.

Также стоит уточнить, что упомянутый акт толкования применяется только для ст. 272 УК РФ, несмотря на использование в ст. 272^1 и 274^1 УК РФ категории «неправомерный доступ». Кроме того, в ч. 2 ст. 274^1 УК РФ в отличие от ст. 272 УК РФ указываются способы осуществления неправомерного доступа. Законодатель в конструкции нормы использует фразу «в том числе», оставляя перечень действий, образующих «неправомерный доступ» открытым.

В свою очередь, в ч. 1 ст. 272^1 УК РФ указывается, что информация может быть получена «путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование либо иным незаконным путем». Словосочетание «незаконным путем» оставляет перечень действий по неправомерному доступу к информации открытым. Возникает вопрос, можно ли расширительно толковать норму и, к примеру, относить сюда подкуп лиц, которые могут предоставить указанные данные? Представляется, что все-таки с учетом расположения представленной нормы в 28 главе УК РФ законодатель полагал, что любая форма неправомерного доступа будет связана с посягательством на общественные отношения, охраняющие компьютерную безопасность, поэтому фраза «иным незаконным способом», которая позволяет расширительно толковать упомянутые действия, видится нам в контексте представленной статьи несколько неуместной.

Полагаем, что указание на характер неправомерного получения подобных сведений и описание его способов усложняет процесс квалификации. Для упрощения понимания нормы права и ее использования вполне достаточно фразы «неправомерный доступ», который можно раскрыть в разъяснении высшей судебной инстанции применительно к ст. 272 и 272^1 УК РФ, исключив из него словосочетание «или использование».

Далее рассмотрим, что следует понимать под деяниями в виде незаконного использования и (или) передачи (распространения, предоставления, доступа), сбора и (или) хранения.

Естественно, Федеральный закон № 152-ФЗ регламентирует только законную деятельность по обработке персональных данных, которая подразумевает такие действия, как использование, сбор, передача, хранение персональных данных. Понятие «передача» раскрывается через три действия, которые также имеют разное легальное наполнение. Если распространение связано с раскрытием персональных данных неопределенному кругу лиц, то предоставление – это раскрытие персональных данных определенному лицу или кругу лиц. Определение понятия «доступ» отсутствует, однако системное толкование закона позволяет говорить, что он имеется в виду тогда, когда мы рассматриваем действия оператора, на которого в связи с получением доступа к информации возлагаются определенные обязанности (к примеру, не распространять персональные данные без согласия субъекта персональных данных). Понятие «хранение» также не содержится в законе, однако опять же из системного толкования понимаем, что есть требования к хранению (форма хранения), а также срок хранения, который может быть установлен законом, договором. Сбор персональных данных также связан с действиями оператора (ст. 18 Федерального закона). Однако возникает вопрос – насколько корректно использовать терминологию, применяемую в целях регулирования общественных отношений, связанных с обработкой персональных данных (то есть осуществлением законной деятельности субъектов), для конструирования уголовно-правовых запретов (то есть по отношению к незаконной деятельности)? Разве злоумышленники осуществляют сбор персональных данных, как операторы? Кроме того, мы уже упоминали, что необходимо вначале завладеть информацией, а потом ее использовать, это уже следующий этап жизни цифровой информации, который, как представляется, должен быть выражен в последствиях, к примеру, вместе с теми, которые указаны в ч. 1 ст. 272 УК РФ или иным образом.

Кроме того, представляется некорректным в тексте уголовно-правовой нормы проводить отличие между такими деяниями, как «предоставление» и «распространение». Для правоприменителя, вероятно, нет особой разницы в том, распространяет злоумышленник указанные сведения определенному кругу лиц или неопределенному, а важен факт их передачи. В деяниях, связанных с распространением (разглашением) охраняемой законом информации, важна их передача хотя бы одному человеку. Так, согласно п. 3 постановления Пленума Верховного Суда РФ от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (ст. 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» под распространением сведений о частной жизни лица понимается «сообщение (разглашении) их одному или нескольким лицам…» (Пост. № 46). В связи с этим нам представляется возможным использовать в контексте данной нормы вместо словосочетания «передача (распространение, предоставление, доступ)» термин «распространение».

Также хотелось бы рассмотреть одно из альтернативных действий, характеризующих объективную сторону состава преступления, – сбор. Использовать данное слово в конструкции нормы также некорректно в связи с тем, что под неправомерным доступом к компьютерной информации понимается ее получение.

Тогда непонятно отличие сбора от получения. Неверно применительно к «духу» уголовно-правовой нормы отождествлять указанные понятия. Именно поэтому ее «получение» включает в себя «сбор». Кроме того, есть и так называемый жизненный цикл оборота цифровой информации, первым этапом которой является ее получение, что по содержанию аналогично «сбору».

Возникает вопрос о том, насколько общественно опасным считается «хранение компьютерной информации, содержащей персональные данные», если при этом нет цели их распространить или, к примеру, продать.

В результате исследования представляется, что к деяниям, представляющим общественную опасность, в контексте представленного уголовно-правового запрета относятся распространение и использование подобных сведений. Однако также необходимо оценить, не будет ли использование указанных сведений являться в большей степени общественно опасным по сравнению с их распространением.

Полагаем, что одним из аргументов, подтверждающих нашу точку зрения, являются положения, отраженные в ч. 12 ст. 19 Федерального закона № 152-ФЗ, о том, что в результате компьютерной атаки на информационные системы наступают последствия в виде неправомерной передачи данных.

Стоит отметить, что ранее противоправные действия в виде незаконного оборота персональных данных подлежали уголовно-правовой оценке; нельзя сказать, что был правовой пробел и лица не подлежали ответственности. До появления ст. 274^1 в УК РФ подобные действия подлежали квалификации по ч. 4 ст. 272 УК РФ, предусматривающей наказание в виде лишения свободы сроком до 7 лет. Согласно же новелле, обозначенные действия влекут за собой максимальное наказание в виде лишения свободы сроком до 4 лет. Однако уголовный закон был дополнен ст. 274^1 УК РФ в целях дифференциации ответственности, а также для усиления в связи с тем, что норма является специальной по отношению к общей (ст. 272 УК РФ). Представляется, что детальный анализ санкций проведен не был.

Кроме того, остановимся на фразе диспозиции ч. 1 ст. 274^1 УК РФ – «за исключением деяний, совершенных в отношении компьютерной информации, содержащей персональные данные, предусмотренные частью второй настоящей статьи». По нашему мнению, в ч. 2 указана фраза «те же деяния», которой достаточно для правильного применения и проведения дифференциации между ч. 1 и 2, содержащей указание на специальный предмет. Поэтому фраза в ч. 1 нам представляется лишней, утяжеляющей норму и усложняющей ее понимание и толкование, хотя такой законодательный прием используется в УК РФ.

Полагаем, что указанная фраза в целом использована в конструкции норм для облегчения работы правоприменителей. Однако при этом возникает вопрос о правилах, которые используют для разрешения конкуренции между составами преступлений. В уголовно-правовой доктрине общепризнанным является подход, согласно которому «при конкуренции основного и квалифицированного состава преступления квалификация производится по статье (части статьи) УК РФ, предусматривающей квалифицированный состав» [6]. Законодатель использует подобный подход, полагаем, что он в целом «загромождает» норму, и так являющуюся значительной по объему, а правоприменителю все равно нужно будет

ознакомиться с текстом уголовно-правовой нормы и ее примечаниями. В связи с вышеизложенным мы считаем, что наличие подобной фразы в тексте ч. 1 статьи является избыточным.

В ч. 4 рассматриваемой статьи усилена ответственность за передачу баз данных с персональными данными иностранным гражданам, иностранным организациям или иностранным государственным структурам, а также злоумышленникам, которые вывозят такую компьютерную информацию из Российской Федерации на носителях. В прим. 2 к статье содержится определение понятия «трансграничное перемещение носителей информации», несмотря на то что в ч. 4 эта фраза имеет несколько иное звучание: «трансграничное перемещение носителей информации, содержащих персональные данные», и нам представляется не совсем верным использовать столь разный терминологический аппарат. В прим. 2 к статье употреблена конструкция «машиночитаемый носитель информации (в том числе магнитный и электронный), на который осуществлены запись и хранение такой информации». Полагаем, что в примечании нет смысла пояснять, что на указанный носитель информации осуществлены «запись и хранение информации», и указывать виды носителей (магнитный и электронный). Кроме того, и сформулированное определение видится не совсем удачным, так как категория «носитель информации» раскрывается через категорию «машиночитаемый носитель информации», что свидетельствует об неоправданной тавтологии, которая затрудняет ориентацию в нормативном материале, создавая сложности с пониманием смысла законодательных установлений [7]. Аналогичное умозаключение относится и к словосочетанию «в настоящей статье», дважды упоминаемое в определении. В законодательстве устоявшимся является термин «электронный носитель информации», используемый в ст. 164[1] Уголовно-процессуального кодекса Российской Федерации, под которым понимается «объект, предназначенный для записи, хранения и воспроизведения цифровой информации» (УПК РФ). Поэтому «запись» и «хранение» определяют его функциональное предназначение, в связи с чем нет необходимости в указании на них в примечании к статье.

Возникает также вопрос – в чем будет выражаться та самая трансграничная передача информации в связи с тем, что данные могут быть переданы с помощью сети Интернет и при этом используются иностранные сервисы почты или хранилища данных.

В ч. 6 содержится самостоятельный состав преступления, устанавливающий ответственность за так называемое создание и администрирование сайта в сети Интернет, предназначенного для незаконного оборота персональными данными.

Полагаем, что использование словосочетания «программы для электронно-вычислительных машин» уже давно устарело, и в том числе для уголовно-правового науки и законодательства. В 2011 г. законодатель исключил его из текста закона – это связано с тем, что в современном мире с развитием и появлением цифровых технологий используется и обращается уже цифровая, а не компьютерная информация. В этом же году в УК РФ появился термин «компьютерная информация» и его определение в прим. 1 к ст. 272 УК РФ. Однако в конце 2024 г.

в тексте уголовного закона России вновь упомянут термин «электронно-вычислительные машины», что представляется нам неудачным решением.

Помимо повышенной общественной опасности содеянного имеется и ее социальная обусловленность, выраженная в характере распространения подобных деяний. Действительно, существует необходимость в разработке самостоятельной запретительной нормы, однако мы считаем, что она должна быть выделена в отдельный состав преступления. Аргументом вышеназванной позиции является то, что указанные деяния являются новыми для уголовного закона, они не подлежали ранее уголовно-правовой оценке, создание подобных сайтов связано с новыми общественными отношениями и новыми субъектами, поэтому установление ответственности видится нам своевременным и отвечающим новым тенденциям.

4. Заключение

В результате исследования можно заключить, что введение уголовной ответственности за незаконный оборот персональных данных необходимо, однако выбранная и реализованная законодателем уголовно-правовая модель не будет обладать превентивным характером, а, скорее, наоборот, вызовет еще больше проблем в процессе правоприменения. В связи с изложенным предлагается следующее.

1. Ст. 272 УК РФ дополнить таким квалифицирующим признаком, как совершение тех же деяний в отношении персональных данных.

Обоснование предложения: в результате компьютерной атаки происходит завладение компьютерной информацией, содержащей персональные данные. При этом автоматически происходит и завладение иной цифровой информацией. В массиве обращающейся цифровой информации выбрать именно персональные данные злоумышленнику, вероятно, будет весьма проблематично, именно поэтому отнесение предмета преступления в новой норме к «охраняемой законом компьютерной информации», защищаемой ст. 272 УК РФ, представляется нам более уместным.

Предмет преступления, предусмотренный ст. 272^1 УК РФ, в целом соответствует двум основным критериям:

во-первых, информация является охраняемой законом;

во-вторых, она должна быть представлена в виде цифровых данных.

Полагаем, что потенциала ст. 272 УК РФ более чем достаточно для уголовно-правовой охраны персональных данных в цифровой форме.

Персональные данные – такая же цифровая информация, что свидетельствует о том, что новые отношения не формируются при посягательстве на них и на опосредованные ими общественные отношения. Новые сущности не образуются, поэтому потенциала действующих уголовно-правовых запретов более чем достаточно.

2. В ст. 272^1 УК РФ:

а) изменить наименование на «Неправомерное распространение и использование компьютерной информации, содержащей персональные данные»;

б) сформулировать ч. 1 как «неправомерное распространение компьютерной информации, содержащей персональные данные»;

в) установить повышенную ответственность за неправомерное использование компьютерной информации, содержащей персональные данные.

3. Ответственность за запрет, установленный ч. 6 ст. 272^1 УК РФ, установить в отдельном уголовно-правовом запрете – в ст. 272^2 УК РФ.

Благодарности. Работа выполнена за счет гранта Академии наук Республики Татарстан, предоставленного молодым кандидатам наук (постдокторантам) с целью защиты докторской диссертации, выполнения научно-исследовательских работ, а также выполнения трудовых функций в научных и образовательных организациях Республики Татарстан в рамках Государственной программы Республики Татарстан «Научно-технологическое развитие Республики Татарстан».

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Источники

УК РФ – Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собр. законодательства Российской Федерации. 1996. № 25. Ст. 2954.

УПК РФ – Уголовно-процессуальный кодекс Российской Федерации от 18 дек. 2001 г. № 174-ФЗ // СЗ РФ. 2001. № 52 (часть I). Ст. 4921.

ФЗ № 152 – Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (часть I). Ст. 3451.

ФЗ № 421 – Федеральный закон от 30 нояб. 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // Рос. газета. 2024. № 278.

Пост. № 46 – Постановление Пленума Верховного Суда РФ от 25 дек. 2018 г. № 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, 145.1 Уголовного кодекса Российской Федерации)» // Рос. газета. 2019. № 1.

Пост. № 37 – Постановление Пленума Верховного Суда РФ от 15 дек. 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”» // Рос. газета. 2022. № 294.

Литература

1. *Ищук Я.Г., Пинкевич Т.В., Смольянинов Е.С.* Цифровая криминология. М.: Акад. управления МВД России, 2021. 242 с.
2. *Russkevich E.A.* Violating the rules of centralized management of technical means of counteracting the threats to information security // J. Digital Technol. Law. 2023. V. 1, No 3. P. 650–672. https://doi.org/10.21202/jdtl.2023.28.
3. *Бегишев И.Р., Кирпичников Д.В.* Проблемные вопросы уголовно-правовой охраны персональных данных // Уголовная юстиция. 2020. № 15. С. 11–16. https://doi.org/10.17223/23088451/15/3.
4. *Ильин И.Г.* Персональные данные в системах искусственного интеллекта: технология обработки естественного языка // J. Digital Technol. Law. 2024. Т. 2, № 1. С. 123–140. https://doi.org/10.21202/jdtl.2024.7.

5. *Шутова А.А.* Социальная обусловленность существования норм об уголовной ответственности за посягательства на персональные данные // Юридическая наука и практика: Вестн. Нижегород. акад. МВД России. 2015. № 4 (32). С. 332–335.

6. *Рясов А.И.* Некоторые особенности квалификации преступлений при конкуренции уголовно-правовых норм // Гуманитарные и юридические исследования. 2013. №. 2. С. 66–69.

7. *Кожокарь И.П.* Лингвистические дефекты нормативно-правового регулирования // Юридическая наука. 2019. № 8. С. 3–7.

Поступила в редакцию 17.12.2024
Принята к публикации 21.12.2024

Шутова Альбина Александровна, кандидат юридических наук, старший научный сотрудник Научно-исследовательского института цифровых технологий и права, доцент кафедры уголовного права и процесса

Казанский инновационный университет имени В.Г. Тимирясова
ул. Московская д. 42, г. Казань, 420111, Россия
E-mail: *shutova1993@inbox.ru*

ISSN 2541-7738 (Print)
ISSN 2500-2171 (Online)

UCHENYE ZAPISKI KAZANSKOGO UNIVERSITETA. SERIYA GUMANITARNYE NAUKI
(Proceedings of Kazan University. Humanities Series)

2024, vol. 166, no. 6, pp. 122–134

ORIGINAL ARTICLE

doi: 10.26907/2541-7738.2024.6.122-134

Novelties in Russian Criminal Law on Liability for Personal Data Breaches

A.A. Shutova

Kazan Innovative University named after V.G. Timiryasov, Kazan, 420111 Russia

E-mail: *shutova1993@inbox.ru*

Received December 17, 2024; Accepted December 21, 2024

Abstract

This article presents the results of the first critical legal analysis of a novel provision in Russian criminal law that penalizes anyone who engages in the illegal use, transfer, collection, or storage of computer information containing personal data, as well as in the creation and management of information assets designed for the unauthorized storage and distribution of such data. The major flaws and contradictions in Article 272 of the Criminal Code of the Russian Federation were exposed, and potential solutions of certain problems associated with its enforcement were proposed. Theoretical recommendations were developed to strengthen the legislative measures targeting breaches of computer information containing personal data of minors, special categories of personal data, or biometric personal data. Some challenges that may arise when categorizing acts involving the cross-border transfer of computer information containing personal data and the cross-border flow of computer information carriers holding personal data were identified. The findings contribute to improving the criminal law framework for safeguarding personal data and advancing the Russian criminal law doctrine on liability for cybercrimes.

Keywords: biometric personal data, personal data of minors, crimes involving computer information, cross-border transfer of personal data, personal data breach, cybercrimes

Acknowledgments. This study was funded by the grant from the Tatarstan Academy of Sciences for early-career PhD holders (postdoctoral researchers) aimed to support them in writing doctoral dissertations, performing research work, and fulfilling professional responsibilities within scientific and educational organizations of the Republic of Tatarstan as part of the State Program of the Republic of Tatarstan "Scientific and technological development of the Republic of Tatarstan".

Conflicts of Interest. The author declares no conflicts of interest.

References

1. Ishchuk Ya.G., Pinkevich T.V., Smolyaninov E.S. *Tsifrovaya kriminologiya* [Digital Criminology] Moscow, Akad. Upr. MVD Ross., 2021. 242 p. (In Russian)
2. Russkevich E.A. Violation of the rules of centralized management of technical means of countering threats to information security. *Journal of Digital Technologies and Law*, 2023, vol. 1, no. 3, pp. 650–672. https://doi.org/10.21202/jdtl.2023.28.
3. Begishev I.R., Kirpichnikov D.V. Problems with protecting personal data in criminal law. *Ugolovnaya Yustitsiya*, 2020, no. 15, pp. 11–16. https://doi.org/10.17223/23088451/15/3. (In Russian)
4. Ilin I.G. Personal data in artificial intelligence systems: Natural language processing technology. *Journal of Digital Technologies and Law*, 2024, vol. 2, no. 1, pp. 123–140. https://doi.org/10.21202/jdtl.2024.7.
5. Shutova A.A. Social conditionality rules on the existence of criminal liability for the infringement of personal data. *Yuridicheskaya Nauka i Praktika: Vestnik Nizhegorodskoi Akademii MVD Rossii*, 2015, no. 4 (32), pp. 332–335. (In Russian)
6. Ryasov A.I. Some features of crime qualification in the case of competing criminal law norms. *Gumanitarnye i Yuridicheskie Issledovaniya*, 2013, no. 2, pp. 66–69. (In Russian)
7. Kozhokar' I.P. Linguistic defects of legal regulation. *Yuridicheskaya Nauka*, 2019, no. 8, pp. 3–7. (In Russian)

***Для цитирования*:** *Шутова А.А.* Новеллы уголовного законодательства об ответственности за незаконный оборот персональных данных // Учен. зап. Казан. ун-та. Сер. Гуманит. науки. 2024. Т. 166, кн. 6. С. 122–134. https://doi.org/10.26907/2541-7738.2024.6.122-134.

***For citation*:** Shutova A.A. Novelties in Russian criminal law on liability for personal data breaches. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Gumanitarnye Nauki*, 2024, vol. 166, no. 6, pp. 122–134. https://doi.org/10.26907/2541-7738.2024.6.122-134. (In Russian)