



Научная статья

УДК 343

<https://doi.org/10.33874/2072-9936-2025-0-2-166-182>

НОВЫЕ ПОДХОДЫ К УГОЛОВНО-ПРАВОВОЙ ОХРАНЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Анастасия Васильевна Малешина¹

Анна Сергеевна Озерова²

^{1,2} МГУ им. М. В. Ломоносова, 119991, Россия, г. Москва, Ленинские горы, д. 1

¹ anastasia.gololobova@gmail.com

² annaozerova55@mail.ru

Аннотация

Цель исследования – анализ новеллы уголовного закона в части установления уголовной ответственности за незаконные использование и (или) передачу, сбор и (или) хранение компьютерной информации, содержащей персональные данные. В результате проведенного исследования авторы приходят к выводу об ошибочном определении объекта новых составов преступления и, соответственно, их места в системе УК РФ. Видовым объектом рассматриваемых преступлений, по мысли законодателя, выступают общественные отношения, гарантирующие безопасность компьютерной информации. В статье обосновывается, что уголовно-правовыми мерами защищать необходимо не информацию саму по себе в отрыве от контекста ее функционирования, а непосредственно те общественные отношения, которые претерпевают негативные изменения, причиняемые преступлением. Наряду с этим в статье поднимаются и иные проблемы, решение которых позволит более эффективно защищать уголовно-правовыми средствами безопасность персональных данных субъектов. Так, рассматриваются следующие вопросы: терминологические недостатки нового состава преступления, разграничение состава преступления, предлагаемого в законопроекте, с иными смежными составами преступлений, а также с правонарушениями.

Ключевые слова: персональные данные; неприкосновенность частной жизни; компьютерная информация; информационные технологии; информационная безопасность; личная тайна; незаконный доступ к компьютерной информации.

Для цитирования: Малешина А. В., Озерова А. С. Новые подходы к уголовно-правовой охране персональных данных // Вестник Российской правовой академии. 2025. № 2. С. 166–182. <https://doi.org/10.33874/2072-9936-2025-0-2-166-182>

Research Article

THE NEW APPROACHES TOWARD CRIMINAL LAW PROTECTION OF PERSONAL DATA

Anastasia V. Maleshina¹

Anna S. Ozerova²

^{1,2} Lomonosov Moscow State University, 1 Leninskie Gory, Moscow, 119991, Russia

¹ anastasia.gololobova@gmail.com

² annaozerova55@mail.ru

Abstract

The purpose of the study is conducting analysis of the new law, which provides for amendments to the Criminal Code of the Russian Federation in terms of establishing liability for the illegal use and transfer, collection and storage of computer information containing personal data. The conducted research shows that the corpus delict of the new offence is misplaced in the system of the Criminal Code of the Russian Federation. According to the legislator, the specific object of the crime is public relations that guarantee the security of computer information. Apparently, the information should be criminally protected not in itself but in a broader social context and the concept of social harm caused by the crime. Along with this, the article raises other problems, the solution of which, in the authors' opinion, will make it possible to more effectively protect the security of personal data of subjects by criminal legal means. Thus, the following issues are considered: terminological shortcomings of the new offence, the differentiation of the offence proposed with the related offences, as well as with the torts.

Keywords: personal data; privacy; computer information; information technologies; information security; personal secrets; illegal access to computer information.

For citation: *Maleshina A.V., Ozerova A. S. The New Approaches Toward Criminal Law Protection of Personal Data. Herald of the Russian Law Academy, 2025, no. 2, pp. 166–182. (In Russ.)* <https://doi.org/10.33874/2072-9936-2025-0-2-166-182>

Введение

К моменту принятия рассматриваемой новеллы в научных кругах сложилось устойчивое понимание необходимости уголовно-правовой охраны информационной безопасности личности, правоприменительная практика в свою очередь выработала подходы как к определению категории персональных данных, так и к реализации уголовно-правовой охраны. Несмотря на очевидный вывод о неоднородности судебной практики, ее анализ позволяет выделить ряд составов преступных посягательств (ст. 137, 138, 173.2, 183, 272, 320 Уголовного кодекса РФ (далее – УК РФ)), которые до введения новой ст. 272.1 УК РФ чаще всего вменялись в случае совершения посягательств на персональные данные. Зачастую при этом имело место расширительное толкование признаков, характеризующих предмет преступления. В частности, по ст. 137 УК РФ суды квалифицировали в качестве посягательства на личную тайну случаи незаконного использования следующих категорий персональных данных, не подпадающих под правовой режим «тайны»:

1) паспортные данные, сведения о месте регистрации, дата рождения, фамилия, имя и отчество [1; 2; 3]; фамилия, имя, отчество, номер мобильного телефона, место работы, адрес проживания, фотография потерпевшего, позволяющие персонализировать его личность [4];

2) номера абонентов, с которыми у потерпевшего были соединения, ставшие известными виновному в связи с исполнением им служебных обязанностей (по совокупности со ст. 138 УК РФ) [5];

3) фотография лица, анкетные данные, адрес регистрации, сведения о судимости. Так, виновный имел доступ к информационной базе данных ГУ МВД России по Новосибирской области, который был предоставлен на основании занимаемой им должности оперуполномоченного. Указанные сведения были предоставлены виновным его приятелю по просьбе последнего [6];

4) личный абонентский номер потерпевшего, фотография с его изображением, а также фотография его водительского удостоверения и паспорта гражданина РФ [7];

5) сведения о жителях, содержащиеся в электронной базе данных органа муниципального образования (администрации города N), а именно: фамилия, имя, отчество, год и место рождения, регистрация, паспортные данные, семейное положение, данные о коммунальных платежах. Доступ к указанной информации виновный имел в силу своего служебного положения, распространяя ее в систематизированном виде за денежное вознаграждение третьим лицам [8];

6) информация об адресе местожительства потерпевшего [9; 10].

Даже на примере анализа судебной практики по одной приведенной статье очевидно, что такая квалификация небесспорна и требует переосмысления. Безусловно, личная или семейная тайна, составляющие предмет преступления ст. 137 УК РФ, могут быть представлены персональными данными лица, в том числе биометрически-

ми, но отождествлять рассматриваемые категории представляется неверным. Вместе с тем, несмотря на очевидное расширение судебного толкования термина «личная и семейная тайна», подобный подход объясним преимущественной направленностью таких посягательств на неприкосновенность частной жизни лица. Именно по этой причине одним из возможных путей реформирования ответственности за незаконный оборот персональных данных выступало уточнение предмета ч. 1 ст. 137 УК РФ, с тем чтобы он включал в себя, в том числе, и персональные данные.

1. Анализ законодательной новеллы. Определение объекта состава преступления

Несмотря на то, что в литературе зачастую поддерживался сложившийся *de lege lata* подход к квалификации деяний, нарушающих Федеральный закон «О персональных данных», ряд правоведов [11, с. 21; 12, с. 107–116; 13, с. 29] указывали в своих работах на необходимость самостоятельной уголовно-правовой охраны персональных данных. Впервые в отечественном законодательстве Федеральным законом от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» криминализованы незаконные действия в отношении персональных данных. Согласно указанному закону, УК РФ дополнен ст. 272.1, которой устанавливается ответственность 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» [14].

Следует сказать, что в научной литературе [15, с. 93–103] положения новеллы уголовного закона в период его рассмотрения в Государственной Думе уже подвергались критике, которая во многом представляется обоснованной. Выскажем и мы свои соображения, проанализировав объективные и субъективные признаки нового состава преступления.

В пояснительной записке данного закона отмечается: «для целей уголовного законодательства конкретизирован объект преступного посягательства (компьютерная информация), который содержит персональные данные, полученные незаконным путем» [14].

Не вызывает сомнений, что ошибочно считать компьютерную информацию, а именно *персональные данные в форме компьютерной информации* объектом преступления. Посредством компьютерной информации, содержащей персональные данные, как предмета преступления преступник главным образом причиняет ущерб информационной приватности личности. В противном случае нарушается фундаментальное правило разграничения объекта преступления и его факультативного признака предмета.

Переходя к вопросу определения объекта, отметим, что место рассматриваемого состава преступления в системе УК РФ определено в разд. IX «Преступления против общественной безопасности и общественного порядка», а именно в гл. 28 «Преступления в сфере компьютерной информации». Отсюда родовым объектом указанного преступления, по мысли законодателя, выступает общественная безопасность, а видовым объектом – общественные отношения, гарантирующие безо-

пасность компьютерной информации. Представляется спорным решение о месте нового состава преступления в системе уголовного законодательства.

По нашему мнению, уголовно-правовая охрана должна предоставляться не информации как таковой, в отрыве от ее содержания, а общественным отношениям, претерпевающим негативные изменения в результате совершения преступления. Например, при разглашении сведений о мерах безопасности, применяемых в отношении должностного лица, страдает нормальная деятельность государственных органов; при незаконном сборении личной тайны или персональных данных – неприкосновенность частной жизни и т.д. Данное представление основано и на тексте Федерального закона «О персональных данных», в ст. 2 которого определена цель обеспечения прав и свобод человека и гражданина, помимо прочего, посредством обеспечения неприкосновенности частной жизни, личной и семейной тайны.

На связь персональных данных и неприкосновенности личной жизни неоднократно указывал и Конституционный Суд РФ (далее – КС РФ). Так, в определении КС РФ от 26 марта 2019 г. № 849-О [16] право на защиту персональных данных было выведено из прав, гарантированных ст. 23 и ч. 1 ст. 24 Конституции РФ. В других определениях КС РФ персональные данные представлены как разновидность [17] информации о частной жизни лица, а природа персональных данных обусловлена конституционными требованиями уважения частной жизни лица [18]. К сведениям о частной жизни лица КС РФ относит и персональные данные медицинского работника, «публикуемые на интернет-сайте, а равно отзывы о его профессиональной деятельности, размещаемые на сайте пользователями» [19].

В правовой доктрине институт персональных данных рассматривается как результат исторического развития права на неприкосновенность частной жизни [20, с. 669–672; 21; 22, с. 26; 23, с. 43–82]. Главной целью рассматриваемого института является, прежде всего, недопущение манипулирования любой информацией, относящейся к физическому лицу. Преступные посяательства на персональные данные приводят к нарушению права лица контролировать сбор, распространение и использование персональных данных, а также вступать в различные общественные отношения от своего имени. Именно по этой причине ряд авторов исключает возможность исчерпывающего определения категории «частная жизнь» [24, с. 103–118].

Кроме того, представляется, что предлагаемое законодателем место нового состава преступления в системе УК РФ оставляет вне уголовно-правовой защиты большой массив персональных данных, которые хранятся на бумажных носителях, а не в форме компьютерной информации.

Например, можно переписать от руки или сфотографировать персональные данные, которые используются в служебных целях и хранятся на бумажных носителях (например, анкета при поступлении на работу, личный листок по учету кадров, трудовая книжка, паспорт, свидетельство о рождении, налоговые справки (2-НДФЛ, 3-НДФЛ и иные), диплом о высшем образовании, ИНН, СНИЛС, ОМС, аттестат, свидетельство о заключении брака, свидетельство о расторжении брака, гражданско-правовые и трудовые договоры, расписки, служебные удостоверения, временная регистрация и иные материальные (бумажные) носители персональных данных).

Таким образом, выходит, что в ряде случаев компьютерная информация не только не является объектом, но и не выступает предметом подобного преступления.

Представляется, что специфика совершения посягательств на персональные данные в виде «неправомерного доступа к компьютерной информации» или «использования информационных технологий» может быть отражена при описании способа совершения преступления, например, путем указания на соответствующий квалифицирующий признак.

Следует отметить и тот факт, что исторически, до внесения рассматриваемого законопроекта в Государственную Думу, высказывались иные идеи относительно правовой сути категории «персональные данные».

Так, в 2021 г. в верхней палате российского парламента прошли парламентские слушания на тему «Неприкосновенность частной жизни в условиях цифровизации и ответственность за ее нарушение» [25], где обсуждались вопросы защиты прав субъектов персональных данных в свете защиты неприкосновенности частной жизни.

Один из докладчиков совершенно справедливо отметил: «частные данные принадлежат тому лицу, которое, собственно говоря, является носителем этих данных, – это прежде всего. И это право, право неприкосновенности частной жизни, и право на защиту этих данных – это права конкретного индивидуального лица» [25].

Кроме того, на указанных слушаниях приводились результаты социологического опроса, согласно которому люди в большей степени обеспокоены возможностью совершения мошеннических и иных преступных действий с использованием персональных данных. «Другими словами, речь идет о том, насколько распространение и использование цифровых технологий обеспечивает соблюдение конституционных прав каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени» [25].

В связи с вышеуказанным сложно согласиться с законодателем относительно определения объекта нового состава преступления. Полагаем, что *de lege ferenda* видо-вым объектом посягательств на персональные данные должны выступать *общественные отношения в сфере реализации конституционных прав и свобод личности*.

Непосредственным объектом посягательств на персональную информацию, по нашему мнению, выступают общественные отношения по охране неприкосновенности частной жизни.

Дополнительным объектом преступлений, предметом которых выступает персональная информация, *de lege ferenda* выступает психическая неприкосновенность личности. Факультативным объектом рассматриваемых преступлений могут выступать честь и достоинство личности. Одной из распространенных преступных целей совершения преступных посягательств в отношении общедоступной персональной информации является желание виновного унижить, оскорбить и умалить репутацию потерпевшего [26; 27]. Стремление представить лицо в невыгодном свете в настоящее время реализуется злоумышленниками не посредством раскрытия личных тайн потерпевшего, а путем, например, распространения той или иной дискредитирующей информации от его имени в интернете с использованием персональных данных.

Предметом рассматриваемого преступления является полученная незаконным путем компьютерная информация, содержащая как общие (ФИО, дата и место рождения, адрес, контактные данные, профессиональная деятельность, место работы и т.д.), так и специальные (касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, а также биометрические персональные данные) персональные данные [14].

Следует отметить, что в первой редакции законопроект не выделял каких-либо специальных категорий потерпевших. Однако при подготовке редакции законопроекта ко второму чтению в ч. 2 ст. 272.1 УК РФ была закреплена ответственность за незаконные действия в отношении компьютерной информации, содержащей персональные данные несовершеннолетних лиц. С таким шагом законодателя следует согласиться, поскольку посягательства на персональную информацию о несовершеннолетнем характеризуются повышенной общественной опасностью в силу психофизиологических особенностей [28; 29, с. 3–4; 30, с. 165–169] такой группы потерпевших, а также в связи с интенсивным развитием цифровых технологий и социальных сетей. В частности, в Концепции информационной безопасности детей в Российской Федерации [31] защищенность персональных данных несовершеннолетних, размещенных в сети Интернет, отнесена к приоритетным задачам государства. В Концепции также указывается на риски размещения несовершеннолетними личной информации в силу открытости и доступности такого рода информации для использования злоумышленниками в противоправных целях [31]. Кроме того, несовершеннолетние в меньшей степени осознают риски, последствия, соответствующие гарантии и права при обработке данных [32].

2. Объективная сторона состава преступления

Если обратиться к анализу объективной стороны нового состава преступления, то следует отметить, что в законе действия, посягающие на персональные данные, описаны как «использование и (или) передача (распространение, предоставление, доступ), сбор и (или) хранение компьютерной информации, содержащей персональные данные» [14]. Если сопоставить данный текст со ст. 3 Федерального закона «О персональных данных», которая определяет действия, направленные на обработку персональных данных, то можно прийти к выводу, что в тексте закона не нашли отражения такие действия, как запись, систематизация, накопление, уточнение (обновление, изменение), извлечение, обезличивание, блокирование, удаление, уничтожение персональных данных.

Если подробно характеризовать каждый из способов совершаемого преступления, то следует отметить, что «незаконное собирание» (в редакции закона «сбор») охватывает и такие способы обработки, как *накопление* и *запись*.

Каждый из перечисленных терминов имеет свою специфику согласно Федеральному закону «О персональных данных», которая не является существенной в уголовно-правовом значении, а потому не требуется их перечисление в норме закона.

Полагаем, что термин «*использование*» персональных данных в уголовно-правовом смысле включает в себя *систематизацию, уточнение (обновление, измене-*

ние), а также *извлечение*. Например, к *систематизации* данных следует относить любой вид обработки таковых по качественным критериям. В процессе *уточнения персональных данных* могут быть устранены какие-либо неточности или внесены дополнения, конкретизирующие данные по какому-либо критерию. *Извлечение* в свою очередь – это «совокупность алгоритмов и компьютерных методов обработки информации, используемых для выборки данных из специальных хранилищ или баз данных» [21].

В связи с этим следует согласиться с отсутствием выделения в ст. 272.1 УК РФ в качестве альтернативных признаков объективной стороны вышеназванных действий, установленных в отраслевом законодательстве, содержание которых полностью охватывается термином «использование» и «собираение».

В то же время *незаконные обезличивание, блокирование, удаление и уничтожение персональных данных*, определенные в Законе, по нашему мнению, причиняют вред не информационной автономии личности, а компьютерной безопасности. В связи с этим в случае совершения таких действий возможна квалификация по ст. 272 УК РФ, объективная сторона которой включает в себя такие преступные последствия, как *уничтожение и блокирование компьютерной информации*. Например, в ситуации обезличивания персональных данных без дополнительной информации невозможно определить ее принадлежность конкретному субъекту и, соответственно, причинить вред личным правам. Сказанное справедливо и в отношении *блокирования, удаления и уничтожения персональных данных*.

Следует согласиться с предлагаемым в новой ст. 272.1 УК РФ разграничением *незаконного распространения персональных данных* и их *незаконного использования*.

Незаконное использование персональных данных может быть выражено в следующих действиях:

- 1) создание фэйковой страницы потерпевшего в социальных сетях и дальнейшая переписка от его имени;
- 2) использование персональных данных в целях получения гражданско-правовых услуг от имени потерпевшего (например, каршеринга или медицинских услуг);
- 3) создание с использованием технологии *deepfake* недействительного видео- или фотоизображения потерпевшего посредством компиляции различных фотографий лица из интернета и иных источников (например, лицо потерпевшего используется в неприличном видео в целях причинения ему репутационного ущерба);
- 4) продажа персональных данных на черном рынке;
- 5) подмена личности в цифровом пространстве и иное.

Под *распространением информации*, толкуя указанный термин строго и нерасширительно, необходимо понимать исключительно процесс передачи определенных сведений от одного лица другому. Ошибочно включать в понятие распространения персональных данных различные способы их незаконного использования, а именно: применение указанных сведений в процессе противозаконной деятельности и иное распоряжение таковой злоумышленником.

Наряду с названными действиями, согласно положениям ст. 272.1 УК РФ, уголовная ответственность альтернативно установлена и за *передачу* персональных

данных. Вряд ли можно согласиться с использованием термина «передача» данных, избыточным видится и указание в уголовном законе на её формы – распространение, предоставление, доступ. Отраслевое законодательство [34] различает такие формы передачи персональных данных в зависимости от категории адресата. В случае распространения речь идет о неопределенном круге адресатов, а при предоставлении всегда можно указать таковых. В уголовно-правовой доктрине, а также судебной практике [35] под распространением сведений понимается их *сообщение (разглашение) даже одному лицу*. В связи с этим, с нашей точки зрения, указанные незаконные действия обоснованно в рамках предлагаемой криминализации определять как незаконное распространение.

Кроме того, применительно к информации как нематериальному благу в иных составах преступлений используется термин «распространение» (ст. 128.1, 163 УК РФ и иные). В целях терминологического единства уголовного закона более обоснованным будет именование указанного преступного действия как «распространение», в содержание которого входят передача, предоставление и доступ. Как уже было указано выше, обоснован такой вывод и в отношении термина «сбор». В УК РФ устоявшимся термином, который используется для обозначения указанного действия, выступает «собираание» информации (например, ст. 137, 183, 276 УК РФ).

В соответствии со ст. 272.1 УК РФ последним альтернативным признаком объективной стороны преступления выступает «хранение» персональных данных.

Представляется, что с учетом стремительного развития информационных технологий решение о криминализации незаконного хранения персональных данных является обоснованным. Так, если незаконная деятельность в отношении персональных данных осуществляется, например, организованной группой, то один из членов такой группы может осуществлять исключительно хранение незаконно собираемых данных. Указанная позиция поддерживается также и в уголовно-правовой доктрине [36, с. 135; 37, с. 110].

Обращаясь к понятию «неправомерный доступ» к средствам обработки компьютерной информации, ее хранения или иного вмешательства в их функционирование, следует упомянуть об отсутствии единообразного подхода к его сущностному определению в уголовно-правовой доктрине. В частности, ряд правоведов [38, с. 12; 39; 40, с. 8.] называет в качестве ключевого признака рассматриваемого термина отсутствие у лица, получившего доступ, законного права на него.

Вместе с тем в научной литературе сформулирован и широкий подход к определению неправомерного доступа, согласно которому «доступ будет являться неправомерным, если лицо не имеет права на доступ к данной информации, либо лицо имеет право на доступ к данной информации, однако осуществляет его помимо установленного порядка, с нарушением правил ее защиты» [41, с. 251].

Соглашаясь с широким подходом к пониманию «неправомерного доступа», отметим, что иное толкование термина будет оставлять за рамками уголовно-правового запрета последующие незаконные действия в отношении данных, полученных лицом без нарушения закона или, другими словами, имеющим законное право на доступ к ним.

3. Разграничение смежных составов преступлений и правонарушений

Прежде всего необходимо определить соотношение ст. 272.1 и 272 УК РФ.

На первый взгляд может показаться, что рассматриваемые нормы соотносятся как общая и специальная по признаку предмета преступления. Так, если предметом преступления, предусмотренного ст. 272 УК РФ, выступает любая охраняемая законом компьютерная информация, то, согласно ст. 272.1 УК РФ, предмет сужается до «компьютерной информации, содержащей персональные данные» [14].

Однако, обращаясь к анализу объективной стороны исследуемых составов преступлений, можно отметить отсутствие в диспозиции предлагаемой нормы последствий, указанных в ст. 272 УК РФ: «уничтожения, блокирования, модификации либо копирования компьютерной информации». В таком случае возникает закономерный вопрос: как следует квалифицировать содеянное в том случае, когда лицо осуществляет незаконное собирание персональных данных, а после этого уничтожает собранную информацию? Вменение совокупности преступлений в таком случае не видится справедливым решением вопроса.

Наряду с этим, остается открытым вопрос о квалификации незаконных действий в отношении той категории персональных данных, которые одновременно подпадают под режим охраняемой законом тайны. И если в отношении тех данных, посягательство на которые нарушает неприкосновенность частной жизни, проблема решена законодателем за счет внесения изменений в диспозицию ч. 1 ст. 137 УК РФ, то в отношении других видов охраняемой законом тайны, в частности коммерческой, налоговой или банковской (ст. 183 УК РФ), такого уточнения нет.

Кроме того, не представляется возможным разграничить рассматриваемый состав преступления и правонарушение, предусмотренное ст. 13.11 Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ). Если проанализировать названную норму, то можно прийти к заключению, что объективная сторона исследуемых норм частично совпадает, так как понятие «обработка данных», предусмотренное ст. 13.11 КоАП РФ, включает в себя все альтернативные признаки объективной стороны ст. 272.1 УК РФ. При этом отсутствует в диспозиции статьи и указание на преступные последствия, наличие которых позволило бы решить проблему разграничения норм. К аналогичному заключению пришел и Верховный Суд РФ в официальном отзыве на проект федерального закона [42].

До внесения соответствующих изменений в УК РФ разумным выглядело предложение, в соответствии с которым преступные посягательства в отношении персональных данных разграничивать с административными правонарушениями следует именно по признаку преступных последствий. Ввиду того, что такие последствия могут быть крайне разнообразными, обоснованным, с нашей точки зрения, было бы указание на *«причинение вреда правам и законным интересам граждан»*.

4. Субъективные признаки состава преступления

Субъектом рассматриваемого состава преступления по ч. 1 выступает физическое вменяемое лицо, которому ко времени совершения преступления исполнилось 16 лет. Вместе с тем определяется и возможность совершения указанного преступления специальным субъектом. Так, ст. 272.1 УК РФ предусматривает такой

квалифицирующий признак в ч. 3, как «использование своего служебного положения» субъектом преступления [14]. В практическом аспекте это означает, что уголовной ответственности будут подлежать как лица, которые выступают создателями или администраторами информационных ресурсов, предоставляющих доступ к незаконно полученным базам персональных данных, так и потребители подобных незаконных услуг, а равно другие лица, так или иначе вовлеченные в незаконный оборот персональных данных – пользователи персональных данных, распространяющие их или допускающие распространение, лица, осуществляющие сбор персональных данных для последующего распространения или иного незаконного использования, и т.д.

Формально-логический анализ признаков рассматриваемого преступления позволяет сделать вывод, что оно не может быть совершено с неосторожной формой вины или косвенным умыслом.

Отметим также, что новая норма уголовного закона содержит два примечания. Отдельное внимание обратим на примечание первое, согласно которому «действие настоящей статьи не распространяется на случаи обработки персональных данных физическими лицами исключительно для личных и семейных нужд» [14].

По нашему мнению, рассматриваемое примечание выступает вторым «ограничительным критерием» (как было рассмотрено выше, предмет преступления в виде компьютерной информации – первый критерий), который существенно сужает сферу применения рассматриваемого уголовно-правового запрета. Кроме того, считаем, что отсутствует правовая определенность в изложении указанного положения. Непонятно, что предлагается понимать под «обработкой персональных данных физическими лицами исключительно для личных и семейных нужд» для целей применения уголовного закона. Какие случаи в соответствии с предложенной логикой не будут подпадать под действие нормы? Например, повлекут ли уголовную ответственность действия ревливой женщины, которая целенаправленно собирает персональные данные коллеги своего супруга (или создает фейковую страницу в социальных сетях с целью общения от ее имени и получения конфиденциальной информации)?

Важно обратить внимание, что в ст. 1 Федерального закона «О персональных данных» указывается, что его действие не распространяется на отношения, возникающие при обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных. Соответственно, законодатель обращает внимание на то, что такая обработка может быть допустима только в том случае, если отсутствует нарушение прав субъектов персональных данных.

Заключение

Таким образом, анализ новых норм уголовного закона в части установления уголовной ответственности за «незаконное использование и передачу, сбор и хранение компьютерной информации, содержащей персональные данные» [14], позволяет сформулировать следующие выводы.

1. Определенный в законе объект состава преступления в виде общественных отношений, гарантирующих безопасность компьютерной информации, оставля-

ет вне уголовно-правовой защиты большой массив персональных данных, которые существуют не в форме компьютерной информации (на бумажном (материальном) носителе).

2. Нарушают терминологическое единство уголовного закона термины «передача» и «сбор», которые используются при описании альтернативных признаков объективной стороны преступления.

3. Следует положительно оценить выделение несовершеннолетних как специальной категории потерпевших, поскольку посягательства на их персональные данные характеризуются повышенной общественной опасностью в силу психофизиологических особенностей указанной группы.

4. Сформулированное в примечании первом к ст. 272.1 УК РФ условие об исключении уголовной ответственности в случае обработки персональных данных для личных и семейных нужд является неопределенным и повлечет трудности в применении нормы. Указанное примечание выступает «ограничительным критерием», который существенно сужает сферу применения рассматриваемого уголовно-правового запрета.

5. Неразрешенными остались вопросы разграничения нового состава преступления с правонарушением, предусмотренным ст. 13.11 КоАП РФ.

Анализируемая норма уголовного закона стала справедливым ответом на непрерывно возникающие угрозы незаконного оборота персональных данных, однако в рамках проведенного исследования было продемонстрировано, что существует потребность в поиске иных подходов к установлению уголовного запрета за совершение рассматриваемых деяний, способных качественно защитить неприкосновенность частной жизни потерпевших от посягательств на персональные данные.

Пристатейный библиографический список

1. Приговор Фрунзенского районного суда г. Владимира от 18 мая 2020 г. по делу № 1-77/2020 // СПС «КонсультантПлюс».
2. Приговор Ковровского городского суда Владимирской области от 6 августа 2020 г. № 1-257/2020 // СПС «КонсультантПлюс».
3. Постановление Центрального районного суда г. Челябинска от 27 января 2020 г. № 1-166/2020 // СПС «КонсультантПлюс».
4. Приговор мирового судьи судебного участка № 42 Узловского судебного района от 21 июня 2019 г. № 1-10/2019 // СПС «КонсультантПлюс».
5. Приговор Приморского районного суда г. Санкт-Петербурга от 15 апреля 2021 г. по делу № 1-482/2021// СПС «КонсультантПлюс».
6. Приговор Центрального районного суда г. Новосибирска от 1 февраля 2021 г. по делу № 1-13/2021// СПС «КонсультантПлюс».
7. Приговор Ново-Савиновского районного суда г. Казани от 1 июля 2019 г. № 1-198/2019// СПС «КонсультантПлюс».
8. Приговор Курганского городского суда Курганской области от 28 декабря 2018 г. по делу № 1-709/18// СПС «КонсультантПлюс».

9. Апелляционное постановление Верховного суда Республики Саха (Якутия) от 1 декабря 2020 г. по делу № 22-1827/2020 // СПС «КонсультантПлюс».
10. Приговор Мегино-Кангаласского районного суда Республики Саха (Якутия) от 29 сентября 2020 г. № 1-75/2020 // СПС «КонсультантПлюс».
11. *Кадников Б. Н.* Уголовно-правовая охрана неприкосновенности частной жизни : автореф. дис. ... канд. юрид. наук. М., 2008.
12. *Чукреев В. А.* Персональные данные, в том числе биометрические данные, как предметы уголовно-правовой охраны // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 3.
13. *Просветова О. Б.* Защита персональных данных : дис. ... канд. юрид. наук. Воронеж, 2005.
14. Система обеспечения законодательной деятельности: сайт. URL: <https://sozd.duma.gov.ru/bill/502113-8> (дата обращения: 01.03.2024).
15. *Хохлова Е. В.* Вопросы криминализации деяний в отношении персональных данных в контексте законопроекта № 502113-8 // Известия Юго-Западного государственного университета. Серия: История и право. 2024. Т. 14. № 1.
16. Определение Конституционного Суда РФ от 26 марта 2019 г. № 849-О // СПС «КонсультантПлюс».
17. Определение Конституционного Суда РФ от 28 июня 2012 г. № 1253-О // СПС «КонсультантПлюс».
18. Постановление Конституционного Суда РФ от 13 января 2020 г. № 1-П // СПС «КонсультантПлюс».
19. Постановление Конституционного Суда РФ от 25 мая 2021 г. № 22-П «По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона «О персональных данных» в связи с жалобой общества с ограниченной ответственностью «МедРейтинг» // СПС «КонсультантПлюс».
20. *Авакьян С. А.* Конституционное право России : учебное пособие : в 2 т. М., 2014.
21. *Савельев А. И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М., 2017.
22. *Бундин М. В.* Персональные данные в системе информации ограниченного доступа : дис. ... канд. юрид. наук. М., 2017.
23. *Дмитрик Н. А.* История, смысл и перспективы института персональных данных // Вестник гражданского права. 2020. № 3.
24. *Ромашов П. А.* К вопросу о праве на неприкосновенность частной жизни в цифровой век / под ред. О. А. Кузнецовой, В. Г. Голубцова, Г. Я. Борисевич, Л. В. Боровых, Ю. В. Васильевой, С. Г. Михайлова, С. Б. Полякова, А. С. Телегина, Т. В. Шершень // Пермский юридический альманах. Ежегодный научный журнал. 2019. № 1.
25. Комитет Совета Федерации по конституционному законодательству и государственному строительству : сайт. URL: <http://legislation.council.gov.ru/activity/activities/parliamentary/127610/> (дата обращения: 15.03.2024).
26. Приговор мирового судьи судебного участка № 1 Фрунзенского района г. Владимира от 15 марта 2021 г. по делу № 1-2/2021 // СПС «КонсультантПлюс».

27. Приговор мирового судьи судебного участка № 1 Ртищевского района от 8 мая 2018 г. по делу № 1-19/2018 // СПС «КонсультантПлюс».
28. Риски интернет-коммуникации детей и молодежи : учебное пособие / Т. Н. Владимирова и др. М., 2019.
29. Буданов С. А. Правовое обеспечение информационной безопасности несовершеннолетних : автореф. дис. ... канд. юрид. наук. Воронеж, 2006.
30. Буданов С. А., Гаврилов С. Т. Информационная безопасность несовершеннолетних: правовой аспект // Территория науки. 2015. № 2.
31. Распоряжение Правительства РФ от 28 апреля 2023 г. № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р» // СПС «КонсультантПлюс».
32. Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных) // СПС «Гарант».
33. Власенко М. С. Обеспечение информационной безопасности несовершеннолетних в сети Интернет: современное состояние и совершенствование правового регулирования // Вестник ВУиТ. 2019. № 3.
34. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс».
35. Постановление 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 (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» // СПС «КонсультантПлюс».
36. Калашникова Е. Е. Уголовно-правовое обеспечение неприкосновенности информации о частной жизни : дис. ... канд. юрид. наук. М., 2001.
37. Жеребкин В. П. Уголовно-правовая охрана частной жизни : дис. ... канд. юрид. наук. Саратов, 2003.
38. Доронин А. М. Уголовная ответственность за неправомерный доступ к компьютерной информации : автореф. дис. ... канд. юрид. наук. М., 2003.
39. Воробьев В. В. Преступления в сфере компьютерной информации: Юридическая характеристика составов и квалификация : автореф. дис. ... канд. юрид. наук. Н. Новгород, 2000.
40. Копырюлин А. Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты : автореф. дис. ... канд. юрид. наук. Тамбов, 2007.
41. Ефремова М. А. Уголовно-правовая охрана информационной безопасности. М., 2018.
42. Официальный отзыв Верховного Суда РФ от 11 января 2023 г. № 4-вс-79/23 // СПС «КонсультантПлюс».

References

1. Verdict of the Frunzensky District Court of the city of Vladimir of May 18, 2020 in case No. 1-77/2020 (SPS "ConsultantPlus"). (In Russ.)
2. Verdict of the Kovrov City Court of the Vladimir Region of June 8, 2020 No. 1-257/2020 (SPS "ConsultantPlus"). (In Russ.)
3. Resolution of the Central District Court of the City of Chelyabinsk of January 27, 2020 No. 1-166/2020 (SPS "ConsultantPlus"). (In Russ.)
4. Verdict of the Justice of the Peace of the Judicial District No. 42 of the Uzlovsky Judicial District of June 21, 2019 No. 1-10/2019 (SPS "ConsultantPlus"). (In Russ.)
5. Verdict of the Primorsky District Court of St. Petersburg of April 15, 2021 in case No. 1-482/2021 (SPS "ConsultantPlus"). (In Russ.)
6. Verdict of the Central District Court of Novosibirsk of February 1, 2021 in case No. 1-13/2021 (SPS "ConsultantPlus"). (In Russ.)
7. Verdict of the Novo-Savinovsky District Court of Kazan of July 1, 2019 No. 1-198/2019 (SPS "ConsultantPlus"). (In Russ.)
8. Verdict of the Kurgan City Court of the Kurgan Region of December 28, 2018 in case No. 1-709/18 (SPS "ConsultantPlus"). (In Russ.)
9. Appeal Decision of the Supreme Court of the Republic of Sakha (Yakutia) of December 1, 2020 in case No. 22-1827/2020 (SPS "ConsultantPlus"). (In Russ.)
10. Verdict of the Megino-Kangalassky District Court of the Republic of Sakha (Yakutia) of September 29, 2020 No. 1-75/2020 (SPS "ConsultantPlus"). (In Russ.)
11. *Kadnikov B. N.* Criminal Law Protection of Privacy: Synopsis of a Thesis for a Candidate Degree in Law Sciences. Moscow, 2008. (In Russ.)
12. *Chukreev V. A.* Personal Data, Including Biometric Data, as Subjects of Criminal Law Protection. *Bulletin of the O.E. Kutafin University (MSAL)*, 2022, no. 3. (In Russ.)
13. *Prosvetova O. B.* Protection of Personal Data: Thesis for a Candidate Degree in Law Sciences. Voronezh, 2005. (In Russ.)
14. URL: <https://sozd.duma.gov.ru/bill/502113-8> (date of application: 01.03.2024). (In Russ.)
15. *Khokhlova E. V.* Issues of Criminalization of Acts in Relation to Personal Data in the Context of Draft Law No. 502113-8. *News of South-West State University. Series: History and Law*, 2024, vol. 14, no. 1. (In Russ.)
16. Ruling of the Constitutional Court of the Russian Federation of March 26, 2019 No. 849-O (SPS "ConsultantPlus"). (In Russ.)
17. Ruling of the Constitutional Court of the Russian Federation of June 28, 2012 No. 1253-O (SPS "ConsultantPlus"). (In Russ.)
18. Resolution of the Constitutional Court of the Russian Federation of January 13, 2020 No. 1-P (SPS "ConsultantPlus"). (In Russ.)
19. Resolution of the Constitutional Court of the Russian Federation of May 25, 2021 No. 22-P "In the Case of Checking the Constitutionality of Paragraph 8 of Part 1 of Article 6 of the Federal Law 'On Personal Data' in Connection with the Complaint of the Limited Liability Company 'Medreyting'" (SPS "ConsultantPlus"). (In Russ.)
20. *Avakian S. A.* Constitutional Law of Russia: Textbook. In 2 vols. Moscow, 2014 (In Russ.)

21. *Saveliev A. I.* Scientific and Practical Article-by-Article Commentary on the Federal Law "On Personal Data". Moscow, 2017. (In Russ.)
22. *Bundin M. V.* Personal Data in the Restricted Access Information System: Thesis for a Candidate Degree in Law Sciences. Moscow, 2017. (In Russ.)
23. *Dmitrik N. A.* History, Meaning and Prospects of the Institute of Personal Data. *Bulletin of Civil Law*, 2020, no 3. (In Russ.)
24. *Romashov P. A.; Kuznetsova O. A., Golubtsov V. G., Borisevich G. Ia., Borovykh L. V., Vasilieva Iu. V., Mikhailov S. G., Poliakov S. B., Telegina A. S., Shershen T. V. (eds.).* On the Right to Privacy in the Digital Age. *Perm Law Almanac: An Annual Scientific Journal*, 2019, no. 1. (In Russ.)
25. URL: <http://legislation.council.gov.ru/activity/activities/parliamentary/127610/> (date of application: 15.03.2024). (In Russ.)
26. Verdict of the Justice of the Peace of the Judicial District No. 1 of the Frunzensky District of Vladimir of March 15, 2021 in case No. 1-2/2021 (SPS "ConsultantPlus"). (In Russ.)
27. Verdict of the Justice of the Peace of the Judicial District No. 1 of the Rtischevsky District of May 8, 2018 in case No. 1-19/2018. (SPS "ConsultantPlus"). (In Russ.)
28. *Vladimirova T. N. et al.* Risks of Internet Communication of Children and Youth: Textbook. Moscow, 2019. (In Russ.)
29. *Budanov S. A.* Legal Provision of Information Security of Minors: Synopsis of a Thesis for a Candidate Degree in Law Sciences. Voronezh, 2006. (In Russ.)
30. *Budanov S. A., Gavrilov S. T.* Information Security of Minors: Legal Aspect. *The Territory of Science*, 2015, no. 2. (In Russ.)
31. Decree of the Government of the Russian Federation of April 28, 2023 No. 1105-R "On Approval of the Concept of Information Security of Children in the Russian Federation and Invalidation of the Decree of the Government of the Russian Federation of 22 December 2015 No. 2471-R" (SPS "ConsultantPlus"). (In Russ.)
32. Regulation of the European Parliament and of the Council of the European Union 2016/679 of April 27, 2016 on the protection of individuals in the processing of personal data and on the free circulation of such data, as well as on the repeal of Directive 95/46/EC (General Regulation on the Protection of Personal Data) (SPS "Garant"). (In Russ.)
33. *Vlasenko M. S.* Ensuring the Information Security of Minors on the Internet: The Current State and Improvement of Legal Regulation. *Bulletin of VUiT*, 2019, no. 3. (In Russ.)
34. Federal Law No. 152-FZ of July 27, 2006 "On Personal Data" (SPS "ConsultantPlus"). (In Russ.)
35. Resolution of the Plenum of the Supreme Court of the Russian Federation of December 25, 2018 No. 46 "On Certain Issues of Judicial Practice in Cases of Crimes Against the Constitutional Rights and Freedoms of Man and Citizen (Articles 137, 138, 138.1, 139, 144.1, 145, 145.1 of the Criminal Code of the Russian Federation)" (SPS "ConsultantPlus"). (In Russ.)
36. *Kalashnikova E. E.* Criminal Law Enforcement of the Inviolability of Information About Private Life: Thesis for a Candidate Degree in Law Sciences. Moscow, 2001. (In Russ.)

37. *Zherebkin V. P.* Criminal Law Protection of Private Life: Thesis for a Candidate Degree in Law Sciences. Saratov, 2003. (In Russ.)

38. *Doronin A. M.* Criminal Liability for Unlawful Access to Computer Information: Synopsis of a Thesis for a Candidate Degree in Law Sciences. Moscow, 2003. (In Russ.)

39. *Vorobiev V. V.* Crimes in the Field of Computer Information: Legal Characteristics of Compositions and Qualifications: Synopsis of a Thesis for a Candidate Degree in Law Sciences. Nizhny Novgorod, 2000. (In Russ.)

40. *Kopyriulin A. N.* Crimes in the Field of Computer Information: Criminal Law and Criminological Aspects: Synopsis of a Thesis for a Candidate Degree in Law Sciences. Tambov, 2007. (In Russ.)

41. *Efremova M. A.* Criminal Law Protection of Information Security. Moscow, 2018. (In Russ.)

42. Official Review of the Supreme Court of the Russian Federation of January 11, 2023 n 4-vs-79/23 (SPS "ConsultantPlus"). (In Russ.)

Сведения об авторах:

А. В. Малешина – кандидат юридических наук.

А. С. Озерова – аспирант.

Information about the authors:

A. V. Maleshina – PhD in Law.

A. S. Ozerova – Postgraduate Student.

Статья поступила в редакцию 24.12.2024; одобрена после рецензирования 14.01.2025; принята к публикации 19.03.2025.

The article was submitted to the editorial office 24.12.2024; approved after reviewing 14.01.2025; accepted for publication 19.03.2025.