

И.Р. Бегишев, Д.В. Кирпичников

ПРОБЛЕМНЫЕ ВОПРОСЫ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обосновывается необходимость проработки моделей уголовно-правовой охраны общественных отношений, обеспечивающих законный режим хранения, передачи и обработки персональных данных. Исследована детерминационная взаимосвязь между повышением роли цифровых технологий и возникновением криминологических рисков в области уголовно-правовой охраны персональных данных. На основе анализа имеющихся определений понятия «персональные данные» формулируется вывод об излишней абстракции данной дефиниции. Вносятся отдельные предложения по совершенствованию механизмов уголовно-правовой охраны персональных данных.

Ключевые слова: *персональные данные, цифровые технологии, уголовно-правовая охрана, цифровая информация, предмет преступления.*

Внедрение цифровых технологий во многие сферы человеческой деятельности в настоящее время стало очевидным фактом. Цифровая информация является неотъемлемой частью социальных практик [1, с. 10] и составляет основу современных информационных отношений [2–5].

Названными обстоятельствами предопределяется переход основных потоков данных в цифровое пространство, что образует криминологические риски их перехвата, копирования и незаконного использования.

В настоящее время имеется тенденция увеличения количества исковых заявлений о защите персональных данных в различных областях деятельности общества [6, с. 30]. Совершенно справедливы опасения, высказываемые в связи с неконтролируемой массовой рассылкой электронных сообщений в мессенджерах, содержащих персональные данные лиц и используемых для оказания на них неправомерного воздействия в корыстных целях [7, с. 37].

Усложнение порядка и способов использования современных цифровых устройств образует риски неправомерного получения информации о частной жизни пользователей третьими лицами, при этом зачастую пользователи формируют угрозу утечки данных собственным вictimным поведением, пренебрегая сообщениями безопасного использования цифровых устройств и технологий.

Стоит согласиться с мнением О.С. Капинус, которая полагает, что «скорость и объемы обрабатываемой информации, а также относительная доступность ее противоправного получения, в том числе из государственных и частных баз данных, образуют необходимость усиления защиты конституционных прав и свобод человека и гражданина, закрепленных в ст.ст. 23 и 24 Конституции Российской Федерации, в том числе связанных с неприкосновенностью частной жизни, личной и семейной тайны при аккумулировании, передаче, копировании и использовании персональных данных» [8, с. 11].

В настоящее время возможность охраны общественных отношений, обеспечивающих защищенность персональных данных, наличествует только в пределах составов преступлений, описанных в ст.ст. 137 и 272 УК РФ. Однако вряд ли возможно утверждать, что признаки,

описывающие объекты данных составов, исчерпывающе охватывают всю множественность персональных данных, неправомерное воздействие на которые способно образовать достаточную общественную опасность и повлечь тяжкие последствия.

Так, признак «сведения о частной жизни лица», характеризующий предмет состава ст. 137 УК РФ, не обеспечивает полноту защиты персональных данных как сведений, прямо или косвенно связанных с личностью. Вопросы толкования понятия «сведения о частной жизни лица» разъяснены в определении Конституционного Суда Российской Федерации от 28 июня 2012 г. № 1253, из которого следует, что «в понятие “частная жизнь” включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества или государства, если носит непротивоправный характер» [9]. Думается, что подобное толкование исключает возможность отождествления персональных данных и сведений о частной жизни лица, поскольку как минимум сведения о государственном регистрационном знаке транспортного средства, находящегося в собственности лица (соответственно, персональные данные), не являются сведениями о частной жизни лица, поскольку подлежат контролю со стороны государства.

Аналогичная ситуация складывается применительно к ст. 272 УК РФ, защищающей только те общественные отношения, которые охраняют персональные данные, обращающиеся в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Однако использование термина «электрические сигналы» не совсем точно, поскольку оно не учитывает волоконно-оптические и электромагнитные линии связи [4, с. 24], в которых также циркулирует информация, относящаяся к персональным данным.

Мы согласны с точкой зрения Р.Р. Гайфутдинова, полагающего, что «...объектом уголовно-правовой охраны ст. 272 УК РФ персональные данные становятся в случае их обработки в автоматизированных вычислительных системах в виде электронной информации» [10, с. 159].

Таким образом, с достаточной очевидностью образуются необходимость законодательного описания пер-

сональных данных как самостоятельного предмета состава преступления, что способно в полной мере исключить вышеописанную пробельность в охране общественных отношений.

Законодательное определение понятия, выступающего центром исследования, содержится в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных», согласно которому «персональными данными признается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)» [11]. Указанное определение несколько диссонирует с понятием, изложенным в ст. 2 Федерального закона от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» [12], согласно которому «к персональным данным следует относить сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность». Описанный дискурс определений не образует противоречия в правовом регулировании, поскольку последний из упоминаемых актов в настоящее время не действует. Однако мы находим возможным привести его в работе в целях иллюстрирования развития законодательной позиции относительно этого определения.

По нашему мнению, действующее определение понятия «персональные данные» обладает недопустимым уровнем законодательной абстракции, которая позволяет относить к рассматриваемой категории любую информацию, связанную с человеком. Относительную конкретизацию возможно обнаружить в положениях ст. 8 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»: «в общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных» [11]. Относительность конкретизации обусловлена употреблением оценочного признака «иные персональные данные», позволяющего относить к ним любую информацию лишь с тем ограничением, что источником ее распространения или предоставления должен быть непосредственно субъект персональных данных.

Для проведения сравнительно-правового анализа обратимся к положениям зарубежных правовых актов, раскрывающих рассматриваемое понятие. К примеру, согласно действующей редакции отраслевого закона Австрийской Республики, «персональные данные – информация, хранимая на носителе данных и имеющая отношение к некоему идентифицированному или имеющему высокую вероятность идентификации субъекту персональных данных» [13]. В данном определении обращает на себя внимание аналогичный отечественному законодательству уровень абстракции, вероятнее всего, вызванный фундаментальным характером правового акта.

Предположение о том, что законодательная абстракция присуща не только российскому праву, подтверждается при исследовании аналогичного закона

Королевства Дания. В данном законе исследуемое понятие определяется следующим образом: «Слова “персональные данные” должны пониматься как обозначение данных, которые могут быть отнесены к идентифицируемому индивидууму, даже если такое отнесение предполагает знание персонального регистрационного номера или любых подобных персональных средств идентификации такого индивидуума» [14].

Национальное законодательство Республики Беларусь содержит более узкие критерии определения персональных данных, хотя и включает такие формулировки, как «а также иные данные, позволяющие идентифицировать такое лицо» [15, с. 199].

Законодательство Республики Исландия «распространяет понятие “персональные данные” также на информацию о юридических лицах, указывая, что к персональным данным относятся данные, связанные с частными, финансовыми или иными делами индивидов, институтов, компаний и юридических лиц, которые эти лица обоснованно должны держать в секрете» [16].

Приводимая интерпретация закономерно требует некоторых пояснений. Во-первых, применять для целей уголовно-правовой охраны используемый в исландском законодательстве прием распространения понятия персональных данных на сведения о юридических лицах (хотя уголовно-процессуальным законодательством и предусмотрено, что потерпевшим является юридическое лицо в случае причинения вреда его имуществу или деловой репутации) не представляется возможным, поскольку общественные отношения, обеспечивающие охрану деловой репутации юридического лица, как обстоятельство, образующее характер общественной опасности, не являются достаточными для уголовной пенализации. Во-вторых, применение оценочного признака «данные, которые обоснованно должны держаться в секрете», создает риски формирования противоречивой судебной практики в части толкования понятия, не обеспечивает его формальную определенность, точность, ясность, недвусмысленность, согласованность и непротиворечивость в системе правового регулирования.

Вышеперечисленным не исчерпываются легальные определения понятия «персональные данные»; их синтез позволяет прийти к закономерному выводу об использовании излишней абстракции, что, возможно, вполне приемлемо для отраслевого законодательства, однако совершенно недопустимо применительно к конструированию состава преступления и закреплению его в уголовном законе. Сказанным мы исключаем возможность имплементации понятия, что предопределило бы переход к его самостоятельному формулированию, однако составление дефиниции также встречает существенные затруднения, вызванные дискурсом относительно окончательной формулировки понятия, и в научной среде.

Так, некоторые исследователи интерпретируют персональную информацию (употребляемый термин синонимичен понятию «персональные данные») как «факты, сообщения и мнения, которые связаны с данным человеком и относительно которых можно было бы ожидать, что он считает их интимными и конфиденци-

альными и, следовательно, желает остановить или по крайней мере ограничить их циркуляцию» [17]. Оценивать данное определение как удовлетворяющее требованиям построения эффективного правового регулирования не представляется возможным. Отмечая, что персональная информация должна считаться человеком интимной, автор предоставляет субъекту неоправданно широкую дискрецию при выборе спектра персональных данных.

Существует также мнение о том, что для уголовно-правовой охраны персональных данных не требуется формулирования их определения и выделения в качестве признака самостоятельного состава преступления, а обеспечение защиты указанных отношений возможно путем введения в УК РФ отдельной нормы о похищении у гражданина конфиденциальной информации [18, с. 114]. При этом предметом предлагаемого состава, по мнению автора, необходимо обозначить «конфиденциальную информацию гражданина». Полагаем, что рассматривать данное предложение как конструктивное нет достаточных оснований, поскольку потенциал абстракции применяемого словосочетания значительно превышает официальную трактовку понятия «персональные данные», что, очевидно, не соответствует требованиям формальной определенности правового регулирования и влечет невозможность для граждан соотносить свое поведение с требованиями нормативно-правовых актов.

Мы выражаем солидарность с теми исследователями, которые считают, что одним из возможных способов сужения понятия персональных данных может выступать имплементация ограничительных принципов, согласно которым будет определяться необходимость распространения правового режима персональных данных в отношении конкретной информации [19, с. 81].

Действительно, вряд ли возможно достаточно полное и всестороннее законодательное описание понятия «персональные данные» как признака, характеризующего предмет состава преступления, поскольку последний не поддается нормативному закреплению. Весь многообразный спектр массивов сведений о лице, неправомерным воздействием на которые может быть создана угроза причинения существенного вреда охраняемым уголовным законом общественным отношениям, настолько широк, что возможностей юридической техники для его нормативного закрепления на современном этапе недостаточно.

На основании изложенного сформулируем следующие исходные тезисы.

1. Персональные данные следует ограничить исключительно теми сведениями, апеллируя которыми в конкретных условиях места, времени и обстановки виновный создает угрозу наступлению общественно опасного результата либо превращает такую угрозу в действительность.

В обоснование данного тезиса укажем, что перечень персональных данных, посредством противоправного воздействия на которые возможно причинение существенного вреда общественным отношениям, как ранее отмечалось, крайне многогранен, и при его описании вряд ли возможно соблюдение консенсуса между аб-

страктностью и казуистикой: излишне абстрактное описание способно повлечь необоснованно широкое усмотрение правоприменителя и легализовать объективно-репрессивное применение уголовно-правовых мер воздействия за деяния, не образующие достаточной общественной опасности.

В свою очередь, казуальность описания выводит за рамки уголовно-правовой охраны перечень сведений, воздействие на которые причиняет существенный вред. В контексте изложения принципиально следующее: в зависимости от конкретных условий времени, места и обстановки перечень персональных данных, воздействие на которые причиняет существенный вред или создает непосредственную угрозу причинения такого вреда, различен. К примеру, если лицо является участником уголовного судопроизводства (например, свидетелем обвинения), сведения о месте его жительства, месте работы, средствах и маршрутах проезда и передвижения способны поставить его под угрозу, исходящую от заинтересованных лиц. При этом в иных ситуациях сведения о месте жительства таковой опасности не образуют. Исходя из вышеизложенного, не представляется возможным описать персональные данные иначе как с использованием оценочных признаков, наполнение содержанием которых – прерогатива правоприменителя. При этом указанное толкование должно происходить из конкретных фактических обстоятельств времени, места и обстановки, образующих действительную, реальную угрозу причинения существенного вреда общественным отношениям.

2. Признаки, характеризующие деяние в составе посяательства на персональные данные, требуют детальной проработки и предметного описания, поскольку, как справедливо замечено Ю.Е. Пудовочкиным и Д.А. Дорогиным, в случае если признаки действия в законе не описываются и законодатель ограничивается только описанием общественно опасных последствий, их причиной может быть признано любое поведение, виновно приведшее к наступлению результата [20], что может повлечь неконструктивное применение нормы.

По нашему убеждению, признак «неправомерный доступ», описывающий деяние в составе преступления, предусмотренного ст. 272 УК РФ, представляется конструктивным для целей уголовно-правовой охраны персональных данных и может быть заимствован. Законодателем не приводится разъяснения неправомерного доступа, что вызывает необходимость обращения к иным нормативно-правовым актам для его уяснения. Так, в п. 6 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» указано, что доступ к информации есть возможность получения информации и ее использования [21].

Как нам представляется, достаточно успешно признак неправомерного доступа описан в методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [22]. Согласно данному документу под неправомерным доступом следует понимать незаконное либо не разрешенное собственником или иным законным владель-

цем использование возможности получения информации. При этом неправомерным считается доступ, полученный в отношении информации, для которой законом установлен специальный режим ее использования и охраны (персональные данные вполне охватываются этим понятием). Акцентируем внимание на наличии здесь обязательного условия – обеспеченности информации специальными средствами защиты. То есть в ситуациях, когда персональные данные находятся на носителе, доступ к которому не обеспечен специальными средствами защиты (парольная защита, средства идентификации и аутентификации, шифрование), констатировать неправомерность доступа не представляется возможным.

3. Следует установить те общественно опасные последствия, которые могут наступить в результате преступных посягательств.

По своей сути любое воздействие на персональные данные, сообразующееся с уголовно-правовыми средствами реагирования, можно описать как неправомерный доступ, т.е. любые деяния, которые приводят к нарушению конфиденциальности персональных данных. При этом для образования достаточной общественной опасности нарушение режима конфиденциальности персональных данных должно альтернативно влечь наступление или создавать непосредственную угрозу наступления общественно опасных последствий в виде:

- причинения смерти субъекту персональных данных;
- причинения тяжкого или средней тяжести вреда здоровью субъекта персональных данных;
- уничтожения или повреждения имущества субъекта персональных данных в значительном размере;
- нарушения неприкосновенности частной жизни субъекта персональных данных;
- нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений субъекта персональных данных;

– внедрения в информационно-телекоммуникационные устройства, используемые субъектом персональных данных, вредоносной компьютерной программы либо иной компьютерной программы, заведомо предназначенной для неправомерного доступа к иным конфиденциальным сведениям;

- применения насилия к субъекту персональных данных;
- распространения сведений, порочащих субъекта персональных данных или его близких лиц;
- жестокого обращения с субъектом персональных данных или систематического унижения его человеческого достоинства.

Различность объектов в перечисленных последствиях обуславливает необходимость расположения их в квалифицированных составах преступления сообразно повышению степени общественной опасности и усилению ответственности.

4. Использование специальных технических средств, предназначенных для негласного получения информации, однозначно предопределяет противоправность воздействия на персональные данные вне зависимости от наступления общественно опасных последствий. Иными словами, мы полагаем возможным сформулировать квалифицированный состав посягательства на персональные данные, предусматривающий в качестве квалифицирующего признака способ (с использованием специальных технических средств, предназначенных для негласного получения информации), сконструировав его как формальный. Заметим, что общественная опасность способа может быть выражена в равной степени нарушением систем защиты цифровой информации, что также требует нормативного закрепления в качестве признака состава.

5. Принимая во внимание, что в зависимости от статуса субъекта персональных данных характер общественной опасности преступления может дифференцироваться, предлагаем в квалифицированный состав преступления ввести признак «объект государственной охраны», характеризующий потерпевшего.

ЛИТЕРАТУРА

1. *Ефремова М.А.* Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий. М. : Юрлитинформ, 2015. 200 с.
2. *Бегишев И.Р.* Понятие и виды преступлений в сфере обращения цифровой информации : дис. ... канд. юрид. наук. Казань, 2017. 204 с.
3. *Нечаева Е.В., Латыпова Э.Ю., Гильманов Э.М.* Посягательства на цифровую информацию: современное состояние проблемы // Человек: преступление и наказание. 2019. Т. 27, № 1. С. 80–86.
4. *Бегишев И.Р., Бикеев И.И.* Преступления в сфере обращения цифровой информации. Казань : Изд-во Казанского инновационного ун-та, 2020. 300 с.
5. *Хисамова З.И.* Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий : дис. ... канд. юрид. наук. Краснодар, 2016. 222 с.
6. *Бегишев И.Р.* Безопасность критической информационной инфраструктуры Российской Федерации // Безопасность бизнеса. 2019. № 1. С. 27–32.
7. *Латыпова Э.Ю.* Некоторые аспекты уголовной ответственности за деяния, посягающие на неприкосновенность частной жизни // Экономика и право. 2019. № 2. С. 35–45.
8. *Катинус О.С.* Безопасность персональных данных как один из важнейших объектов конституционно-правовой охраны // Вестник Университета прокуратуры Российской Федерации 2018. № 6 (68). С. 10–15.
9. *Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации* : определение Конституционного Суда Российской Федерации от 28.06.2012 № 1253-О [Текст определения официально опубликован не был]. URL: <https://www.garant.ru/products/ipo/prime/doc/70105530/> (дата обращения: 03.05.2020).
10. *Гайфутдинов Р.Р.* Уголовно-правовая характеристика посягательств на персональные данные, обрабатываемые в автоматизированных системах // Ученые записки Казанского университета. Сер. Гуманитарные науки. 2014. Т. 156, № 4. С. 158–164.

11. *О персональных данных* : федеральный закон от 27.07.2006 № 152-ФЗ // Собрание законодательства Российской Федерации. 2006. № 31 (часть I). Ст. 3451.
12. *Об информации*, информатизации и защите информации : федеральный закон от 20.02.1995 № 24-ФЗ // Собрание законодательства Российской Федерации. 1995. № 8. Ст. 609.
13. *Bundesgesetz über den Schutz personenbezogener Daten* (Datenschutzgesetz – DSG). Federal Act concerning the Protection of Personal Data (DSG). URL: https://www.ris.bka.gv.at/Dokumente/ErV/ERV_1999_1_165/ERV_1999_1_165.html (das Datum des Zuganges: 20.04.2020).
14. *Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger* (databeskyttelsesloven). URL: <https://www.retsinformation.dk/eli/lt/2018/502> (accessed: 20.04.2020).
15. *Вабищевич В.В.* Определение персональных данных в целях их уголовно-правовой охраны // Правовая культура в современном обществе : сб. науч. ст. Могилев : Могилев. ин-т МВД, 2018. С. 198–203.
16. *Lög um persónuvernd og vinnslu persónuupplýsinga*. URL: <https://www.althingi.is/lagas/nuna/2018090.html> (accessed: 20.04.2020).
17. *Wacks R.* The protection of Privacy. Sweet & Maxwell. London : Sweet & Maxwell, 1980. 185 p.
18. *Старцева Н.В.* К вопросу об уголовно-правовой охране персональных данных клиентов банка // Пробелы в российском законодательстве. 2011. № 4. С. 112–115.
19. *Мираев А.Г.* Понятие персональных данных в Российской Федерации и Европейском союзе // Юридическая наука. 2019. № 5. С. 76–82.
20. *Пудовочкин Ю.Е., Дорогин Д.А.* Учение о преступлении и о составе преступления : учеб. пособие. М. : Рос. гос. ун-т правосудия, 2017. 387 с.
21. *Об информации*, информационных технологиях и о защите информации : федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства Российской Федерации. 2006. № 31 (часть I). Ст. 3448.
22. *Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации*. URL: <https://genproc.gov.ru/documents/nauka/execution/document-104550> (дата обращения: 20.04.2020).

Problems of Personal Data Protection in Criminal Law

Ugolovnaya yustitsiya – Russian Journal of Criminal Law, 2020, no. 15, pp. 11–16. DOI: 10.17223/23088451/15/3

Ildar R. Begishev, Kazan Innovative University named after V.G. Timiryasov (Kazan, Russian Federation). E-mail: begishev@mail.ru

Danila V. Kirpichnikov, Kazan Innovative University named after V.G. Timiryasov (Kazan, Russian Federation). E-mail: danila667@outlook.com

Keywords: personal data, digital technologies, criminal law protection, digital information, subject of crime.

The article substantiates the need for developing models of criminal law protection of public relations, providing a legal regime for the personal data storage, transfer and processing. The authors have investigated the determination relationship between the increasing role of digital technology and emerging criminological risks in the personal data protection. Having analyzed the existing definitions of the central concept of “personal data” in regulatory legal acts of the Russian Federation and a number of foreign countries and drawing on scholarly opinion, the authors conclude about an excessive abstraction of this definition. In the summary, the authors present the initial theses of understanding personal data as an object that forms public relations under the protection of criminal law. They also propose some ideas for improving the mechanisms of criminal law protection of personal data.

References

1. Efremova, M.A. (2015) *Ugolovnaya otvetstvennost' za prestupleniya, sovershaemye s ispol'zovaniem informatsionno-telekommunikatsionnykh tekhnologiy* [Criminal liability for crimes committed using information and telecommunication technologies]. Moscow: Yurlitinform.
2. Begishev, I.R. (2017) *Ponyatie i vidy prestupleniy v sfere obrashcheniya tsifrovoy informatsii* [The concept and types of crimes in digital information circulation]. Law Cand. Diss. Kazan.
3. Nechaeva, E.V., Latypova, E.Yu. & Gilmanov, E.M. (2019) Attacks on digital information: the current state of the problem. *Chelovek: prestuplenie i nakazanie*. 27(1). pp. 80–86. (In Russian). DOI: 10.33463/1999-9917.2019.27(1-4).1.080-086
4. Begishev, I.R. & Bikeev, I.I. (2020) *Prestupleniya v sfere obrashcheniya tsifrovoy informatsii* [Crimes in the circulation of digital information]. Kazan: Kazan Innovative University.
5. Khisamova, Z.I. (2016) *Ugolovno-pravovye mery protivodeystviya prestupleniyam, sovershaemym v finansovoy sfere s ispol'zovaniem informatsionno-telekommunikatsionnykh tekhnologiy* [Criminal law measures to counter crimes in the financial sphere using information and telecommunication technologies]. Law Cand. Diss. Krasnodar.
6. Begishev, I.R. (2019) Security of Critical Information Infrastructure of the Russian Federation. *Bezopasnost' biznesa – Business Security*. 1. pp. 27–32. (In Russian).
7. Latypova, E.Yu. (2019) Nekotorye aspekty ugolovnoy otvetstvennosti za deyaniya, posyagayushchie na neprikosновенность chastnoy zhizni [Some aspects of criminal liability for acts that infringe on privacy]. *Ekonomika i pravo*. 2. pp. 35–45.
8. Kapinus, O.S. (2018) Bezopasnost' personal'nykh dannykh kak odin iz vazhneyshikh ob'ektov konstitutsionno-pravovoy okhrany [The security of personal data as one of the most important objects of constitutional protection]. *Vestnik Universiteta prokuratury Rossiyskoy Federatsii*. 6(68). pp. 10–15.
9. The Constitutional Court of the Russian Federation. (2012) *Opredelenie Konstitutsionnogo Suda Rossiyskoy Federatsii ot 28 iyunya 2012 g. № 1253-O “Ob otkaze v prinyatii k rassmotreniyu zhaloby grazhdanina Supruna Mikhaila Nikolaevicha na narushenie ego konstitutsionnykh prav stat'ey 137 Ugolovnogo kodeksa Rossiyskoy Federatsii”*. *Tekst Opredeleniya ofitsial'no opublikovan ne byl* [Definition No. 1253-O of the Constitutional Court of the Russian Federation dated June 28, 2012, “On the refusal to accept for consideration a complaint of citizen Suprun Mikhail Nikolaevich about violation of his constitutional rights by Article 137 of the

- Criminal Code of Russia”. The text of the Definition was not officially published]. [Online] Available from: <https://www.garant.ru/products/ipo/prime/doc/70105530/> (Accessed: 03.05.2020).
10. Gayfutdinov, R.R. (2014) Criminal Characteristics of Infringement on Personal Data Undergoing Automated Processing. *Uchenye zapiski Kazanskogo universiteta. Seriya: Gumanitarnye nauki – Proceedings of Kazan University. Humanities Series*. 156(4). pp. 158–164. (In Russian).
 11. The Russian Federation. (2006) Federal’nyy zakon ot 27 iyulya 2006 g. № 152-FZ “O personal’nykh dannyykh” [Federal Law No. 152-FZ dated July 27, 2006, “On personal data”]. *Sobranie zakonodatel’sva Rossiyskoy Federatsii – Legislative Bulletin of the Russian Federation*. 31(1). Art. 3451.
 12. The Russian Federation. (1995) Federal’nyy zakon ot 20 fevralya 1995 g. № 24-FZ “Ob informatsii, informatizatsii i zashchite informatsii” [Federal Law No. 24-FZ dated February 20, 1995, “On information, informatization and information protection”]. *Sobranie zakonodatel’sva Rossiyskoy Federatsii – Legislative Bulletin of the Russian Federation*. 8. Art. 609.
 13. Austria. (n.d.) *Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz – DSGVO)*. [Online] Available from: https://www.ris.bka.gv.at/Dokumente/ErV/ERV_1999_1_165/ERV_1999_1_165.html (Accessed: 20.04.2020).
 14. Denmark. (2018) *Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)*. [Online] Available from: <https://www.retsinformation.dk/eli/lt/2018/502> (Accessed: 20.04.2020).
 15. Vabishchevich, V.V. (2018) Opredelenie personal’nykh dannyykh v tselyakh ikh ugovno-pravovoy okhrany [The definition of personal data for the purpose of their criminal legal protection]. In: Demidov, I.A. (ed.) *Pravovaya kul’tura v sovremennom obshchestve* [Legal Culture in Modern Society]. Mogilev: Mogilev Institute of the Ministry of Internal Affairs. pp. 198–203.
 16. Iceland. (2018) *Lög um persónuvernd og vinnslu persónuupplýsinga*. [Online] Available from: <https://www.althingi.is/lagas/nuna/2018090.html> (Accessed: 20.04.2020).
 17. Wacks, R. (1980) *The Protection of Privacy*. London: Sweet & Maxwell.
 18. Startseva, N.V. (2011) To the problem of the criminal-legal protection of bank clients’ personal data. *Probely v rossiyskom zakonodatel’sve – Gaps in Russian Legislation*. 4. pp. 112–115. (In Russian).
 19. Miraev, A.G. (2019) The concept of personal data in the Russian Federation and the European Union. *Yuridicheskaya nauka – Legal Science*. 5. pp. 76–82. (In Russian).
 20. Pudovochkin, Yu.E. & Dorogin, D.A. (2017) *Uchenie o prestuplenii i o sostave prestupleniya* [The doctrine of the crime and elements of crime]. Moscow: Russian State University of Justice.
 21. The Russian Federation. (2006) Federal’nyy zakon ot 27 iyulya 2006 g. № 149-FZ “Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii” [Federal Law No. 149-FZ dated July 27, 2006, “On information, information technologies and information protection”]. *Sobranie zakonodatel’sva Rossiyskoy Federatsii – Legislative Bulletin of the Russian Federation*. 31(1). Art. 3448.
 22. Office of the Prosecutor General of the Russian Federation. (n.d.) *Metodicheskie rekomendatsii po osushchestvleniyu prokurorskogo nadzora za ispolneniem zakonov pri rassledovanii prestupleniy v sfere komp’yuternoy informatsii* [Guidelines for the implementation of prosecutorial supervision of the implementation of laws in the investigation of crimes related to computer information]. [Online] Available from: <https://genproc.gov.ru/documents/nauka/execution/document-104550> (Accessed: 20.04.2020).