

Александр Сергеевич СЕНЦОВ,

кандидат юридических наук, доцент, ORCID 0000-0002-6481-122X
Российская академия народного хозяйства и государственной
службы при Президенте Российской Федерации (г. Волгоград)
профессор кафедры уголовного права, уголовного
процесса и криминалистики Волгоградского
института управления (филиала РАНХиГС)
sentsov_1951@mail.ru

Владислава Владимировна ВОЛКОЛУПОВА,

ORCID 0009-0006-2604-3764
Санкт-Петербургский государственный
университет (г. Санкт-Петербург)
аспирант
volkolupova.v@yandex.ru

Научная статья
УДК 343.3/.7

ПЕРСПЕКТИВЫ КРИМИНАЛИЗАЦИИ НЕЗАКОННОГО ОБОРОТА ПЕРСОНАЛЬНЫХ ДАННЫХ: КРИТИЧЕСКИЙ АНАЛИЗ НОВОГО ЗАКОНОПРОЕКТА *

КЛЮЧЕВЫЕ СЛОВА. Персональные данные, незаконный оборот персональных данных, компьютерная информация, общественная опасность, преступление, уголовная ответственность, внесение изменений в законодательство.

АННОТАЦИЯ. *Введение.* В настоящее время в условиях построения информационного общества существует объективная потребность в усилении противодействия с использованием уголовно-правовых средств незаконному обороту компьютерной информации, содержащей персональные данные. В ходе проведенного авторами исследования, результаты которого излагаются в статье, были определены основные направления повышения эффективности и перспективы совершенствования уголовно-правовых мер, используемых для осуществления такого противодействия. Кроме того, рассматриваются общетеоретические вопросы, касающиеся социальной обусловленности и критериев криминализации незаконного оборота информации, содержащей персональные данные. **Методы.** При проведении исследования авторы использовали такие общенаучные и частнонаучные методы, как всеобщий диалектический метод научного познания, индукция, дедукция, анализ и синтез, логический, системно-структурный, догматический и др. **Результаты.** Сформулированы предложения о внесении изменений и дополнений в Особенную часть Уголовного кодекса Российской Федерации. Обоснована целесообразность включения в нее ст. 137.1, которая регламентировала бы ответственность за нарушение права на неприкосновенность персональных данных. Представлена авторская редакция этой статьи, что повышает практическую значимость проведенного исследования.

ВВЕДЕНИЕ

В современных условиях повсеместной информатизации и цифровизации общества и государство неизбежно сталкиваются с новыми угрозами информационной безопасности, в том числе связанными с неправомерным оборотом компьютерной информации, содержащей персональные данные. Использование в процессе сбора, обработки и хранения конфиденциальной ин-

формации новейших технических средств, активное развитие и популяризация маркетплейсов, сервисов доставки, социальных сетей и мессенджеров обуславливают необходимость разработки и принятия эффективных мер по защите персональных данных. Люди, пусть и неосознанно, всё чаще самостоятельно предоставляют доступ к своим персональным данным широкому кругу лиц, не задумываясь о возможном наступлении вслед-

* Статья представлена в редакцию для решения вопроса о возможности ее опубликования 15 октября 2024 г., одобрена к публикации 13 ноября 2024 г., то есть до принятия Федерального закона от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации», и не учитывает правовых реалий, сложившихся в связи с вступлением в силу названного нормативного правового акта.

Alexander S. SENTSOV,

Cand. Sci. (Jurisprudence), Associate Professor, ORCID 0000-0002-6481-122X
Russian Presidential Academy of National Economy
and Public Administration (Volgograd, Russia)
Professor of the Department of Criminal Law, Criminal Procedure and
Criminalistics at the Volgograd Institute of Management (branch of RANEPА)
sentsov_1951@mail.ru

Vladislava V. VOLKOLUPOVA,

ORCID 0009-0006-2604-3764
Saint-Petersburg State University (Saint-Petersburg, Russia)
Postgraduate Student
volkolupova.v@yandex.ru

PROSPECTS FOR CRIMINALIZING THE ILLEGAL TRAFFICKING OF PERSONAL DATA: A CRITICAL ANALYSIS OF THE NEW DRAFT LAW*

KEYWORDS. Personal data, illegal circulation of personal data, computer information, public danger, crime, criminal liability, amendments to legislation.

ANNOTATION. *Introduction.* Currently, in the context of building an information society, there is an objective need to strengthen counteraction with the use of criminal law means to illegal circulation of computer information containing personal data. In the course of the study conducted by the authors, the results of which are presented in the article, the main directions of increasing the efficiency and prospects for improving the criminal law measures used to implement such counteraction were identified. In addition, general theoretical issues related to the social determination and criteria for criminalization of illegal circulation of information containing personal data are considered. *Methods.* In conducting the study, the authors used such general scientific and specific scientific methods as the general dialectical method of scientific knowledge, induction, deduction, analysis and synthesis, logical, systemic-structural, dogmatic, etc. *Results.* Proposals are formulated to amend and supplement the Special Part of the Criminal Code of the Russian Federation. The expediency of including Art. 137.1 in it, which would regulate liability for violation of the right to inviolability of personal data, is substantiated. The author's version of this article is presented, which increases the practical significance of the conducted research.

ствие этого крайне негативных последствий [1]. Например, с помощью персональных данных о физическом лице возможно оформление на его имя кредитов, микрозаймов, совершение различных мошеннических действий, вымогательства, стalkerства¹ и др.

В современном обществе персональные данные становятся своеобразным товаром. И он пользуется повышенным спросом на нелегальных рынках, где ведется активная торговля информацией, содержащей конфиденциальные сведения, в том числе и о личности гражданина. В последние годы получают широкий общественный резонанс освещаемые в средствах массовой информации случаи массовой утечки персональных данных и их распространения путем размещения в социальных сетях и на интернет-сайтах. Хищения персональных данных нередко совершаются путем «хакерских атак», а утечки, как правило, связаны с неправомерным доступом к компьютерной информации, содержащей такие данные. Последствиями этих деяний оказываются масштабная компрометация тех или иных граждан и причинение огромного материального ущерба, заключающегося в расходах на устранение причиненного вреда (на это, по экспертным оценкам,

затрачивается несколько миллиардов рублей в год). Указом Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» одним из приоритетных направлений государственной политики признано принятие мер по снижению до минимально возможного уровня количества утечек персональных данных, а также минимизация случаев нарушения нормативных требований по их охране, обеспечение защиты конституционных прав и свобод человека и гражданина на при обработке персональных данных, в том числе с использованием информационных технологий (п. 57).

В системе имеющихся в распоряжении государственных органов приемов и средств правовой охраны персональных данных от неправомерного доступа к ним и их последующего использования в противоправных целях особое место занимает уголовное право. Оно является, хотя и самым репрессивным, но в то же время весьма эффективным способом защиты общественных отношений. Однако в нашей стране до сих пор незаконный оборот конфиденциальной информации, содержащей персональные данные, не криминализован, Уголовный кодекс Российской Федерации

* The article was submitted to the editors to decide on the possibility of its publication on October 15, 2024, approved for publication on November 13, 2024, that is, before the adoption of Federal Law No. 421-FZ of November 30, 2024 «On Amendments to the Criminal Code of the Russian Federation», and does not take into account the legal realities that have arisen in connection with the entry into force of the said regulatory legal act.

¹ Сталкерство (сленг.) – нежелательное навязчивое внимание к человеку, его преследование со стороны другого человека или группы людей.

(далее – УК РФ) не предусматривает ответственности за совершение подобного рода деяний. И это несмотря на то, что в современных условиях развития общества имеются и социальные, и криминологические основания для криминализации наиболее опасных форм оборота информации рассматриваемого нами вида [2, 3].

МЕТОДЫ

Методологическую основу исследования составили такие общенаучные и частнонаучные методы, как всеобщий диалектический метод научного познания, индукция, дедукция, анализ и синтез, системно-структурный, догматический и др. Используемые методы были необходимы для углубленного изучения проблем, относящихся к теме исследования, прежде всего для определения основных направлений усиления противодействия незаконному обороту компьютерной информации, содержащей персональные данные. Примененная методика позволила сформулировать ряд авторских предложений, направленных на совершенствование уголовно-правовых мер противодействия данному виду преступных деяний.

РЕЗУЛЬТАТЫ

В настоящее время в российском обществе всё активнее происходят такие экономические, политические и социальные, в том числе демографические и культурно-ценностные, преобразования, которые способствуют тому, что персональные данные личности становятся обязательным атрибутом не только межличностной коммуникации человека, но и его деятельности во всех сферах профессиональной, общественной и государственной жизни. В этих условиях возникла объективная потребность в переосмыслении существующих в правовой доктрине (и, в частности, в уголовно-правовой теории) некоторых устаревших идей и подходов, которые уже давно не отвечают новым реалиям, в том числе и связанных с оценкой регулятивных и превентивных возможностей уголовно-правовых предписаний, выраженных в нормах, направленных как на охрану конституционных прав и свобод человека и гражданина, так и на обеспечение информационной безопасности. Это в полной мере относится и к критической оценке имеющихся в УК РФ уголовно-правовых мер защиты персональных данных от неправомерного доступа к ним [4; 5, с. 12; 6].

Понятие «персональные данные» в уголовно-правовой доктрине однозначно не определено, относительно соотношения его объема и содержания с таким понятием, как «информация о частной жизни», имеется несколько существенно различающихся теоретических подходов [7, 8, 9]. Не прибегая к их подробному анализу, поскольку этому аспекту посвящены многочисленные публикации, отметим лишь, что легальное понятие «персональные данные» законодательно закреплено в п. 1 ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (в редакции от 8 августа 2024 г.) – это «любая информация, относящаяся к прямо или косвенно

определенному или определяемому физическому лицу (субъекту персональных данных)».

Федеральным законом от 30 декабря 2020 г. № 519-ФЗ в ст. 3 названного выше нормативного правового акта был введен п. 1.1, где закреплено определение особого вида персональных данных. Это «персональные данные, разрешенные субъектом персональных данных для распространения». Под таковыми понимаются «персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном» Федеральным законом «О персональных данных».

На наш взгляд, законодательное определение понятия «персональные данные» в целом вполне приемлемо, хотя и носит несколько абстрактный характер (термин «любая информация» логично было бы конкретизировать). Но даже при таком широком подходе законодателя к определению персональных данных, порождающем сложности в их разграничении со сведениями о частной жизни лица, сегодня представляется логичным и обоснованным включение в УК РФ нового уголовно-правового запрета, устанавливающего самостоятельную ответственность за незаконный оборот информации, нарушающей право на неприкосновенность персональных данных.

К числу аргументов, подтверждающих целесообразность криминализации данного вида общественно опасного поведения, можно отнести, в частности, и то, что основанное на законодательно закрепленных положениях право граждан на неприкосновенность их персональных данных, которое является структурным компонентом права на неприкосновенность частной жизни и имеет конституционно-правовую основу, в современной России, к сожалению, всё чаще подвергается негативному воздействию, в том числе и путем неправомерного доступа к персональным данным и последующего использования в целях совершения преступлений (например, посягающих на конституционные права и свободы личности, хищений чужого имущества в виде краж и мошенничества и др.) [10, 11].

По официальным данным Главного информационно-аналитического центра МВД России, в 2023 г. «было зарегистрировано 677,0 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 29,7% больше, чем за аналогичный период прошлого года. Их удельный вес увеличился с 26,5% в 2022 г. до 34,8% в 2023 г.»¹. В 2020 г. размер суммарного ущерба, причиненного вследствие утечек личных (персональных) данных, превысил 3 млрд рублей, а в 2022 г. увеличился уже до 8 млрд рублей (более чем в 2,6 раза). По сведениям, опубликованным органами внутренних дел, в декабре 2021 г. на темных сайтах в сети Интернет (в так называемом «даркнете») размещалось более

¹ Состояние преступности в России // МВД России: официальный сайт // URL: <https://мвд.рф/reports/item/47055751/> (дата обращения: 15.09.2024).

20 тысяч баз данных общим объемом, превышающим 10 Тб, содержащих сведения о 80% населения России¹.

В связи с этим представляет особый интерес рассмотренный Государственной Думой Российской Федерации в первом чтении законопроект № 502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации», направленный на усиление ответственности за незаконный оборот персональных данных и иные нарушения законодательства в этой сфере. В целях совершенствования уголовно-правовых средств противодействия преступности такого вида авторы законопроекта предлагают дополнить действующий УК РФ статьей 272.1 «Незаконное использование и (или) передача, 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».

Безусловно, сама идея усиления уголовно-правового противодействия незаконному обороту информации, содержащей персональные данные (неправомерным получению, передаче, хранению в целях использования или предоставления третьим лицам и т.п.), представляется своевременной и заслуживает одобрения и поддержки [12, с. 91; 13]. Вместе с тем рассматриваемый законопроект, на наш взгляд, наряду с достоинствами не лишен недостатков: он содержит ряд концептуальных положений, оценка которых может быть неоднозначной, а в чем-то и критической.

ОБСУЖДЕНИЕ

Не прибегая к подробному анализу всех имеющихся в тексте законопроекта спорных положений и не вполне корректных формулировок, отметим лишь такие наиболее значимые из них, которые представляются нам уязвимыми для критики и даже могут быть оценены негативно.

1. В пояснительной записке к законопроекту его авторы указывают, что «для целей уголовного законодательства конкретизирован объект преступления посягательства (компьютерная информация), который содержит персональные данные, полученные незаконным путем. Это позволяет разграничивать новый состав УК РФ от правонарушений, ответственность за которые предусмотрена Кодексом Российской Федерации об административных правонарушениях в ст. 13.11 «Нарушение законодательства Российской Федерации в области персональных данных», а также иных составов преступлений». Иными словами, разработчики законопроекта в качестве основного непосредственного объекта преступления в новом составе, который предлагается закрепить в ст. 272.1 УК РФ, видят саму компьютерную информацию, содержащую персональные данные (статью рекомендуют поместить в гл. 28 «Преступления в сфере компьютерной информации»). Это, на наш взгляд, представляется далеко не бесспорным.

Во-первых, такой подход авторов законопроекта вряд ли можно признать методологически

оправданным, поскольку, несмотря на всё возрастающую социальную значимость компьютерной информации в условиях формирования современного информационного общества, всё-таки в настоящее время именно конституционные права и свободы личности являются самыми приоритетными в системе всех охраняемых правом социальных ценностей. Поэтому и рассматриваемое «право на неприкосновенность персональных данных» как один из компонентов более широкого конституционного права на неприкосновенность частной жизни должно, по нашему мнению, по-прежнему признаваться более значимым объектом уголовно-правовой охраны, чем информационная безопасность. Исходя из такого подхода, вполне логичным было бы признание именно этих интересов личности видовым объектом уголовно-правовой охраны предложенных для включения в УК РФ новых уголовно-правовых норм, в которых должны закрепляться самостоятельные составы преступлений, связанных с нарушением имеющего конституционную основу права на неприкосновенность персональных данных. Поэтому целесообразно эти новые уголовно-правовые запреты включить (с учетом значимости видового объекта посягательства) не в гл. 28, а в гл. 19 УК РФ «Преступления против конституционных прав и свобод человека и гражданина». Именно такая позиция в большей степени согласуется с человекоцентричностью права как относительно новым трендом, активно развивающимся в последние годы в российской правовой доктрине, основанном на идее о том, что именно человек должен находиться во главе всей правовой системы, а следовательно, именно обеспечение таких благ, как его права, свободы и законные интересы, должно стать приоритетом как для законотворческой, так и для правоприменительной деятельности [14, 15].

Таким образом, позиция авторов законопроекта, отраженная в предложенной ими к включению в кодекс статье, представляется не вполне корректной. Действительно, на современном этапе развития общества сама по себе любая социально-значимая информация, в том числе и содержащая персональные данные (и не только компьютерная, но и иных видов), безусловно, заслуживает признания ее вполне самостоятельной и всё более значимой ценностью («кто владеет информацией, тот владеет миром»). И более того, информация всё чаще выступает и в экономике, и в политике в качестве «специфического товара». Однако при всей ее значимости вряд ли информацию можно рассматривать как самостоятельный объект уголовно-правовой охраны. К тому же она еще не включена даже в число самостоятельных объектов гражданских прав (ст. 128 ГК РФ). По нашему мнению, сегодня логичнее признавать ее не объектом, а предметом преступления, также как, например, имущество в составах преступлений против собственности. А видовым объектом преступлений в сфере компьютерной информации (гл. 28 УК РФ) являются общественные отно-

¹ Состояние преступности в России // МВД России: официальный сайт // URL: <https://мвд.рф/reports/item/47055751/> (дата обращения: 15.09.2024).

шения, обеспечивающие такую разновидность общественной безопасности, как безопасность в сфере оборота компьютерной информации (информационная безопасность). Кроме того, как справедливо отмечает Б.С. Бембеева, понятия «персональные данные» и «компьютерная информация» не совпадают ни по своему объему, ни по содержанию, поскольку персональные данные могут храниться не только в «цифровой», но и в иной (бумажной) форме [16].

2. Небесспорным представляется и ограничение сферы действия предлагаемой в законопроекте новой уголовно-правовой нормы, а также распространение запрета только на незаконный оборот лишь таких персональных данных, которые уже представлены «в форме электрических сигналов, независимо от средств их хранения, обработки и передачи», то есть ставших компьютерной информацией (в смысле примечания к ст. 272 УК РФ). Столь необоснованно ограниченная уголовно-правовая защита персональных данных явно не согласуется с нормативными предписаниями отраслевого законодательства, прежде всего – с положениями, закрепленными в Федеральном законе «О персональных данных». В этом законе нормативные требования, регламентирующие процедуру получения и обработки персональных данных, распространяются не только на содержание деятельности по использованию компьютерной техники в названных целях, но и на иные виды деятельности (первичный сбор, хранение и систематизацию персональных данных «вручную», чтобы в дальнейшем использовать специальное оборудование и электронные средства их обработки при переводе в «цифровую» форму). А из содержания предлагаемой в законопроекте статьи остается неясным, как же квалифицировать действия, предусмотренные в ее диспозиции (ч. 1 ст. 272.1), если они были совершены в отношении персональных данных, хотя и на стадии их сбора или хранения, но до перевода в «цифровой формат»?

3. Можно отметить и еще одну неоднозначную особенность предлагаемой в законопроекте статьи: в ней недостаточно четко определены критерии отграничения основного состава преступления, предусмотренного в ее части первой, от сходного состава административного правонарушения, закрепленного в ст. 13.11 КоАП РФ. Очевидно, что диспозиция предлагаемой уголовно-правовой нормы (ч. 1 ст. 272.1 УК РФ) является бланкетной (прямое указание на незаконность совершаемых альтернативных действий), а состав преступления – формальным по своей конструкции, и деяние признается оконченным преступлением уже с момента совершения лицом любого из перечисленных в диспозиции альтернативных действий (например с момента начала сбора информации). Поэтому в правоприменительной практике неиз-

бежно возникнут сложности при разграничении таких понятий, как «сбор» (ст. 272.1) и «обработка» (ст. 13.11 КоАП РФ), поскольку понятием «обработка» охватывается и «сбор».

4. В тексте предлагаемой в законопроекте статьи, к сожалению, иногда встречаются слишком уж «аморфные» и «расплывчатые» формулировки, которые характеризуются чрезмерной неопределенностью и не вполне согласуются с вытекающим из принципа законности требованием «определенности уголовно-правового запрета» [17, 18, 19].

Такие альтернативные действия, как «иное вмешательство в их функционирование» (*функционирование средств обработки компьютерной информации – А.С., В.В.*) или осуществленные «иным незаконным путем», не исключают произвольного распространительного толкования этих признаков правоприменителем. Чрезмерно оценочными представляются и такие формулировки, как «обеспечение функционирования информационных ресурсов» (непонятно, какое имеется в виду «обеспечение»?), «исключительно для личных и семейных нужд» и т.п. Названные оценочные признаки тоже не исключают их либо очень широкого, либо чрезмерно узкого толкования, что «размывает» основание уголовной ответственности и не вполне согласуется с принципом законности.

Такое обилие оценочных признаков, не исключая их произвольного толкования правоприменителем и гражданами, явно не согласуется с правовой позицией Конституционного Суда Российской Федерации, сформулированной им в своих постановлениях от 27 мая 2008 г. № 8-П/2008, от 25 апреля 2018 г. № 17-П/2018 и др. Согласно этой позиции: «неоднозначность, неясность и неопределенность закона порождают возможность неоднозначного истолкования и, следовательно, произвольного применения его норм – в противоречие ... конституционным принципам»¹; «...требования четкости и недвусмысленности правовых норм, их согласованности в системе правового регулирования имеют особую значимость для уголовного законодательства, являющегося по своей природе исключительным средством...»².

5. Небезупречными представляются и предлагаемые в законопроекте санкции, предусмотренные по квалифицированным и особо квалифицированным составам, выделенным из основного состава преступления (ч. 1 ст. 272.1 УК РФ). Они явно не согласованы ни с санкциями, установленными ст.ст. 137, 138 УК РФ, ни с санкциями, закрепленными в ст.ст. 272, 273 УК РФ.

ЗАКЛЮЧЕНИЕ

Подведя итоги проведенного нами исследования, мы сформулировали следующие основные выводы и предложения:

1. В представленной в Государственную Думу Российской Федерации редакции законопроекта

¹ Постановление Конституционного Суда Российской Федерации от 27.05.2008 № 8-П/2008 «По делу о проверке конституционности положения части первой статьи 188 Уголовного кодекса Российской Федерации в связи с жалобой гражданки М.А. Асламазян».

² Постановление Конституционного Суда Российской Федерации от 25.04.2018 № 17-П «По делу о проверке конституционности пункта 2 примечаний к статье 264 Уголовного кодекса Российской Федерации в связи с запросом Ивановского областного суда».

№ 502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации», направленный на усиление ответственности за незаконный оборот персональных данных и иные нарушения законодательства в этой сфере, не в полной мере согласуется с существующими и устоявшимися в уголовно-правовой науке теоретическими взглядами и представлениями о критериях криминализации общественно опасного поведения. Он не решает многих объективно имеющих в настоящее время проблем, связанных с необходимостью усиления противодействия незаконному обороту информации, содержащей персональные данные. И потому, на наш взгляд, законопроект требует корректировки.

Представляется, что законодателю целесообразно создать такой правовой механизм уголовно-правового воздействия на незаконный оборот информации, содержащей персональные данные, который не только реально защищал бы информационную безопасность, но и обеспечивал бы право личности на неприкосновенность персональных данных.

2. В целях усиления противодействия незаконному обороту персональных данных нами предлагается дополнить гл. 19 УК РФ статьей 137.1, изложив ее в следующей редакции:

Статья 137.1. Нарушение права на неприкосновенность персональных данных.

1. Незаконные собирание и (или) хранение, а равно использование, передача, доступ или предо-

ставление персональных данных, в том числе содержащихся в компьютерной информации, без согласия их правообладателя, повлекшие существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, – наказываются ...

2. Те же деяния, совершенные:

а) группой лиц по предварительному сговору;

б) лицом с использованием своего служебного положения;

в) в отношении заведомо несовершеннолетнего или недееспособного лица;

г) с причинением крупного ущерба, –

наказываются ...

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные:

а) организованной группой;

б) в целях совершения тяжкого или особо тяжкого преступления, –

наказываются ...

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, повлекшие тяжкие последствия, –

наказываются ...

Примечание.

Крупным ущербом в настоящей статье признается ущерб в сумме, превышающей двести пятьдесят тысяч рублей, а особо крупным ущербом – превышающей один миллион рублей. ■

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алексеева А.П. Профилактика правонарушений в России: законодательные основы и перспективы реализации // Преступность, уголовная политика, уголовный закон: Сборник научных трудов. Саратов: Саратовская государственная юридическая академия, 2013. С. 549-551.
2. Рязанова Е.Н. Ответственность за распространение персональных данных как способ противодействия правонарушениям в сфере информационно-коммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. 2022. № 3 (95). С. 118-123.
3. Жук О.Д. Об усилении уголовной ответственности за незаконный оборот персональных данных физических лиц, за неправомерный доступ к таким персональным данным, распространение и использование их в преступных целях // Законодательство. 2024. № 2. С. 58-62.
4. Пименова Е.С. О необходимости введения уголовной ответственности за утечку персональных данных // Проблемы правоохранительной деятельности на современном этапе: сборник трудов II Всероссийской (с международным участием) научно-практической конференции. Кострома, 2023. С. 421-425.
5. Капинус О.С. Безопасность персональных данных как один из важнейших объектов конституционно-правовой охраны // Вестник Университета прокуратуры Российской Федерации. 2018. № 6 (68). С. 10-15.
6. Абдурахманова Э. Х., Саркарова Д.С. Проблемы защиты права граждан на неприкосновенность частной жизни и персональных данных в России в условиях цифровизации // Евразийский юридический журнал. 2023. № 7 (182). С. 83-84.
7. Филатова М.А. Персональные данные как предмет преступного посягательства // Уголовное право. 2019. № 2. С. 51-58.
8. Наумов В.Б., Архипов В.В. Понятие персональных данных: интерпретация в условиях развития информационно-телекоммуникационных технологий // Российский юридический журнал. 2016. № 2. С. 186-196.
9. Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. М.: Статут, 2011. 131 с.
10. Алихаджиева И.С. О новых способах совершения преступлений с использованием персональных данных // Вестник Прикамского социального института. 2024. № 1 (97). С. 22-30.
11. Арсланова А.Р. Преступления, связанные с хищением персональных данных с использованием информационных и телекоммуникационных технологий // Актуальные проблемы государства и общества в области обеспечения прав и свобод человека и гражданина. 2021. № 1. С. 329-334.

12. Соколова Ю.А., Науменко А.М. Защита персональных данных граждан: законодательные новеллы и перспективы // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2023. № 12 (163). С. 89-94.

13. Солдатов Н.С., Кочергина Д.Е. Проблемные аспекты персональных данных как объекта уголовно-правовой охраны в Российской Федерации // Вестник образовательного консорциума Среднерусский университет. Серия: Юриспруденция. 2023. № 21. С. 4-6.

14. Бастрыкин А.И. Конституционные права и свободы человека как высшая ценность государства и общества // Конституционные права и свободы человека как высшая ценность государства и общества: сборник научных трудов Всероссийской научно-практической конференции. М., 2023. С. 13-19.

15. Соловьев В.Ю., Соловьева Н.П. Права и свободы человека и гражданина как высшая ценность государства в контексте Конституции и действующего законодательства // Научное пространство: актуальные вопросы, достижения и перспективы развития: Сборник научных трудов по материалам XXV Международной научно-практической конференции. Анапа, 2024. С. 69-76.

16. Бембеева Б.С. Право на защиту персональных данных и различные категории персональных данных // Право в сфере Интернета: Сборник статей. М.: СТАТУТ, 2018. С. 48-61.

17. Наумов А.В. Конкретизация Конституционным судом принципа законности Уголовного кодекса РФ // Уголовное право. 2018. № 1. С. 88-94.

18. Галкин Д.В. О конкретизации и специализации запретов в уголовном законодательстве России // Уголовное право как средство управления обществом. Liber amicorum: Материалы всероссийской научно-практической конференции. М., 2022. С. 63-66.

19. Мартыненко Н.Э. Определенность уголовного закона // Труды Международного симпозиума «Надежность и качество». 2005. Т. 1. С. 453-454.

REFERENCES

1. Alekseyeva A.P. Profilaktika pravonarusheniy v Rossii: zakonodatel'nyye osnovy i perspektivy realizatsii // Prestupnost', ugovlnaya politika, ugovlnyy zakon: Sbornik nauchnykh trudov. Saratov: Saratovskaya gosudarstvennaya yuridicheskaya akademiya, 2013. S. 549-551.

2. Ryazanova Ye.N. Otvetstvennost' za rasprostraneniye personal'nykh dannykh kak sposob protivodeystviya pravonarusheniyam v sfere informatsionno-kommunikatsionnykh tekhnologiy // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2022. № 3 (95). S. 118-123.

3. Zhuk O.D. Ob usilenii ugovlnoy otvetstvennosti za nezakonnyy oborot personal'nykh dannykh fizicheskikh lits, za nepravomernyy dostup k takim personal'nym dannym, rasprostraneniye i ispol'zovaniye ikh v prestupnykh tselyakh // Zakonodatel'stvo. 2024. № 2. S. 58-62.

4. Pimenova Ye.S. O neobkhodimosti vvedeniya ugovlnoy otvetstvennosti za utechku personal'nykh dannykh // Problemy pravookhranitel'noy deyatel'nosti na sovremennom etape: sbornik trudov II Vserossiyskoy (s mezhdunarodnym uchastiyem) nauchno-prakticheskoy konferentsii. Kostroma, 2023. S. 421-425.

5. Kapinus O.S. Bezopasnost' personal'nykh dannykh kak odin iz vazhneyshikh ob'yektov konstitutsionno-pravovoy okhrany // Vestnik Universiteta prokuratury Rossiyskoy Federatsii. 2018. № 6 (68). S. 10-15.

6. Abdurakhmanova E. Kh., Sarkarova D.S. Problemy zashchity prava grazhdan na neprikosnovennost' chastnoy zhizni i personal'nykh dannykh v Rossii v usloviyakh tsifrovizatsii // Yevraziyskiy yuridicheskiy zhurnal. 2023. № 7 (182). S. 83-84.

7. Filatova M.A. Personal'nyye dannyye kak predmet prestupnogo posyagatel'stva // Ugolovnoye pravo. 2019. № 2. S. 51-58.

8. Naumov V.B., Arkhipov V.V. Ponyatiye personal'nykh dannykh: interpretatsiya v usloviyakh razvitiya informatsionno-telekommunikatsionnykh tekhnologiy // Rossiyskiy yuridicheskiy zhurnal. 2016. № 2. S. 186-196.

9. Petrykina N.I. Pravovoye regulirovaniye oborota personal'nykh dannykh. Teoriya i praktika. M.: Statut, 2011. 131 s.

10. Alikhadzhiyeva I.S. O novykh sposobakh soversheniya prestupleniy s ispol'zovaniyem personal'nykh dannykh // Vestnik Prikamskogo sotsial'nogo instituta. 2024. № 1 (97). S. 22-30.

11. Arslanova A.R. Prestupleniya, svyazannyye s khishcheniyem personal'nykh dannykh s ispol'zovaniyem informatsionnykh i telekommunikatsionnykh tekhnologiy // Aktual'nyye problemy gosudarstva i obshchestva v oblasti obespecheniya prav i svobod cheloveka i grazhdanina. 2021. № 1. S. 329-334.

12. Sokolova Yu.A., Naumenko A.M. Zashchita personal'nykh dannykh grazhdan: zakonodatel'nyye novelly i perspektivy // Nauka i obrazovaniye: khozyaystvo i ekonomika; predprinimatel'stvo; pravo i upravleniye. 2023. № 12 (163). S. 89-94.

13. Soldatov N.S., Kochergina D.Ye. Problemnyye aspekty personal'nykh dannykh kak ob'yekta ugovlno-pravovoy okhrany v Rossiyskoy Federatsii // Vestnik obrazovatel'nogo konsortsiuma Srednerusskiy universitet. Seriya: Yurisprudentsiya. 2023. № 21. S. 4-6.

14. Bastykin A.I. Konstitutsionnyye prava i svobody cheloveka kak vysshaya tsennost' gosudarstva i obshchestva // Konstitutsionnyye prava i svobody cheloveka kak vysshaya tsennost' gosudarstva i obshchestva: sbornik nauchnykh trudov Vserossiyskoy nauchno-prakticheskoy konferentsii. M., 2023. S. 13-19.

15. Solov'yev V.Yu., Solov'yeva N.P. Prava i svobody cheloveka i grazhdanina kak vysshaya tsennost' gosudarstva v kontekste Konstitutsii i deystvuyushchego zakonodatel'stva // Nauchnoye prostranstvo: aktual'nyye voprosy, dostizheniya i perspektivy razvitiya: Sbornik nauchnykh trudov po materialam XXV Mezhdunarodnoy nauchno-prakticheskoy konferentsii. Anapa, 2024. S. 69-76.

16. Bembejeva B.S. Pravo na zashchitu personal'nykh dannykh i razlichnyye kategorii personal'nykh dannykh // Pravo v sfere Interneta: Sbornik statey. M.: STATUT, 2018. S. 48-61.

17. Naumov A.V. Konkretizatsiya Konstitutsionnym sudom printsipa zakonnosti Ugolovnoy kodeksa RF // Ugolovnoye pravo. 2018. № 1. S. 88-94.

18. Galkin D.V. O konkretizatsii i spetsializatsii zapretov v ugolovnom zakonodatel'stve Rossii // Ugolovnoye pravo kak sredstvo upravleniya obshchestvom. Liber amicorum: Materialy vserossiyskoy nauchno-prakticheskoy konferentsii. M., 2022. S. 63-66.

19. Martynenko N.E. Opredelennost' ugolovnoy zakona // Trudy Mezhdunarodnogo simpoziuma «Nadezhnost' i kachestvo». 2005. T. 1. S. 453-454.

Авторы заявляют об отсутствии конфликта интересов.

Авторами внесён равный вклад в написание статьи.

The authors declare no conflicts of interests.

The authors have made an equal contribution to the writing of the article.

© Сенцов А.С., Волколупова В.В., 2024.

ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ

Сенцов А.С., Волколупова В.В. Перспективы криминализации незаконного оборота персональных данных: критический анализ нового законопроекта // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2024. № 4 (78). С. 16-23.