Оригинальная статья / Original article

УДК 343.01

https://doi.org/10.21869/2223-1501-2023-13-5-75-86

Персональные данные в механизме уголовно-правовой охраны

Е. А. Русскевич[1] ✉

[1]Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)
ул. Садовая-Кудринская, д. 9, г. Москва 125993, Российская Федерация

✉ e-mail: russkevich@mail.ru

Резюме

Актуальность. *Обеспечение действенной защиты личных данных человека обладает высокой и непреходящей значимостью. Несмотря на предпринимаемые усилия, в России с каждым годом ситуация в этом отношении ухудшается – все чаще возникают инциденты с утечкой персональных данных миллионов граждан. Все это не только порождает недоверие к усилиям государства по построению цифровой экономики и электронного правительства, но и выступает мощной детерминантой целого ряда иных преступлений (прежде всего против собственности).*

Целью *является получение нового научного знания об особенностях, проблемах и перспективах уголовно-правовой охраны персональных данных личности.*

Задача *исследования состоит в выявлении проблем реализации механизма уголовно-правовой охраны персональных данных граждан.*

Методология. *Методологическую базу исследования составляют общенаучные и частнонаучные методы познания действительности, такие как анализ, синтез, индукция, формально-юридический, абстрактно-логический и другие.*

Результаты. *Автором проанализированы статистические данные о динамике посягательств на персональные данные в России, имеющаяся в открытом доступе правоприменительная практика, исследованы доктринальные источники и аналитические материалы, проведено интервьюирование специалистов. В совокупности это позволило сформулировать оригинальные положения, развивающие отечественную теорию уголовного права, выработать рекомендации, направленные на преодоление проблем правоприменения по делам о посягательствах на персональные данные.*

Выводы. *Цифровизация обусловила повышение социальной толерантности к нарушениям в сфере неприкосновенности персональных данных и частной жизни. Представляется перспективным реализовать модель дифференциации уголовной ответственности в зависимости от числа потерпевших от разглашения персональных данных. Механизм уголовно-правовой охраны требует совершенствования и с точки зрения развития технологий биометрических данных. Значимость подобной информации о личности требует дифференцированного подхода к установлению ответственности за неправомерные действия в отношении биометрии.*

Ключевые слова*: персональные данные; нарушение неприкосновенности частной жизни; биометрические данные; преступления; компьютерная информация.*

Финансирование: *Статья подготовлена в рамках госзадания «Российская правовая система в реалиях цифровой трансформации общества и государства: адаптация и перспективы реагирования на современные вызовы и угрозы (FSMW-2023-0006)», регистрационный номер: 1022040700002-6-5.5.1.*

Конфликт интересов*: Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Русскевич Е. А. Персональные данные в механизме уголовно-правовой охраны // Известия Юго-Западного государственного университета. Серия: История и право. 2023. Т. 13, № 5. С. 75–86. https://doi.org/10.21869/2223-1501-2023-13-5-75-86.

Поступила в редакцию 30.08.2023 Принята к публикации 28.09.2023 Опубликована 30.10.2023

Personal Data in the Mechanism of Criminal Law Protection

Evgeny A. Russkevich[1] ✉

[1]Kutafin Moscow State Law University (MSAL)
9 Sadovaya-Kudrinskaya Str., Moscow 125993, Russian Federation

✉ e-mail: russkevich@mail.ru

Abstract

Relevance. *Ensuring the effective protection of an individual's personal data is of high and enduring importance. Despite the efforts made, in Russia the situation in this regard is deteriorating every year - more and more incidents with the leakage of personal data of millions of citizens occur. All this not only generates distrust in the efforts of the state to build a digital economy and e-government, but also acts as a powerful determinant of a number of other crimes (primarily against property).*

The purpose is *to obtain new scientific knowledge about the features, problems and prospects of the criminal law protection of personal data of an individual.*

The objectives of the study *is to identify the problems of implementing the mechanism of criminal law protection of personal data of citizens.*

Methodology. *The methodological base of the research is made up of general scientific and particular scientific methods of cognition of reality, such as analysis, synthesis, induction, formal-legal, abstract-logical and others.*

Results. *In the course of the study, statistical data on the dynamics of infringement on personal data in Russia, law enforcement practice available in the public domain, doctrinal sources and analytical materials were analyzed, interviews were conducted with specialists. Taken together, this made it possible to formulate original provisions that develop the domestic theory of criminal law, to develop recommendations aimed at overcoming the problems of law enforcement in cases of infringement of personal data.*

Conclusions. *Digitalization has led to an increase in social tolerance for violations in the field of inviolability of personal data and privacy. It seems promising to implement a model of differentiation of criminal liability depending on the number of victims of the disclosure of personal data. The mechanism of criminal law protection requires improvement in terms of the development of biometric data technologies. The significance of such personal information requires a differentiated approach to establishing responsibility for illegal actions in relation to biometrics.*

Keywords: *personal data; violation of privacy; biometric data; crimes; computer information.*

Funding: *The article was prepared within the framework of the state assignment "The Russian legal system in the realities of the digital transformation of society and the state: adaptation and prospects for responding to modern challenges and threats (FSMW-2023-0006)", Registration number 1022040700002-6-5.5.1.*

Conflict of interest: *The Author declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Russkevich E. A. Personal Data in the Mechanism of Criminal Law Protection. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law*. 2023; 13(5): 75–86. (In Russ.) https://doi.org/10.21869/2223-1501-2023-13-5-75-86

Received 30.08.2023 Accepted 28.09.2023 Published 30.10.2023

***

Введение

Задача охраны персональных данных личности при всей своей непреходящей значимости в современном теоретическом дискурсе оставляет ощущение какой-то общей капитуляции и разочарования в возможности перемены ситуации к лучшему. С технической точки зрения отстаивается представление о несовершенстве любого нынешнего и будущего программно-аппаратного решения защиты данных – обнаружение уязвимости всегда вопрос времени. Помимо этого, специалисты резюмируют, что, даже если система и будет эффективна перед внешними атаками, нельзя исключить риск

утечки информации изнутри. На основе проведенного анализа средств защиты мобильных устройств Д. А. Изергин делает неутешительный вывод, что их основное предназначение в обеспечении работоспособности самой системы, не учитывая риски компрометации личности владельца устройства различными приложениями либо набором сервисов [1, с. 5].

В правовом контексте довольно распространен тезис о бесперспективности преследования кого бы то ни было в условиях, когда сам пользователь ежедневно распространяет свои персональные данные самыми разными способами. Конечно, всегда остается шанс «поймать за руку» злоумышленника, но это не может изменить ситуацию принципиально. Безысходность.

В то же время, по данным Роскомнадзора, в России наблюдается беспрецедентно негативная тенденция в сфере защиты чувствительной информации о личной жизни человека: в 2021 г. было зафиксировано четыре крупных инцидента с персональными данными, когда в открытый доступ попало 2,7 млн записей, 2022 г. – более 140 случаев, когда утекло около 600 млн записей о гражданах, и только за семь месяцев 2023 г. зафиксировали свыше 150 подобных случаев[1]. Конечно же, приведенные показатели отражают динамику посягательств на персональные данные не в чистом виде, поскольку здесь же учтены факты распространения закрытой информации о переписке, статистике телефонных соединений, медицинских анализах, покупках и т. п. Вместе с тем понятно, что все это имеет ценность и привлекает интерес при возможности прямой или опосредованной персонификации. Поэтому, полагаем, можно уверенно опираться на статистику Роскомнадзора в оценке состояния защищенности персональных данных в России.

Здесь важно также задаться вопросом о том, насколько современный человек терпим к современной «цифровой прозрачности». Скептики небезосновательно пеняют на то, что рядовой пользователь сети Интернет не только не прибегает к элементарной цифровой гигиене в обращении с чувствительной информацией, но и сам, используя социальные сети и мессенджеры, гигабайтами ее распространяет. Действительно, онлайн-жизнь напоказ стала нормой для миллионов. В связи с этим вполне уверенно можно допустить повышение социальной толерантности к инцидентам утечки данных. Так, в личной беседе автора с одним из представителей IT-отрасли было сформулировано по этому поводу примерно следующее соображение: «Будет ли возмущен пользователь фактом открытости своих персональных данных, принимая во внимание, что в течение только прошедшего месяца он их указал на сайте знакомств, при доставке пиццы, оформляя карту лояльности в магазине, проходя онлайн-тест «Какое животное лучше всего описывает ваш характер» или «Каково древнее значение вашего имени (фамилии)»? Ответ очевиден». Некоторые исследователи в своих выводах заходят еще дальше и уже напрямую заявляют о том, что право на частную жизнь, на неприкосновенность персональных данных и современные технологии (например, Big Data) несовместимы между собой [2, с. 70; 3].

Сказанное может быть и имеет под собой реальные основания, но не отменяет главного – независимо от наблюдаемых изменений в сфере социальных коммуникаций на фоне процессов цифровизации человек имеет неотъемлемое право на обеспечение неприкосновенности сведений о себе [4; 5; 6; 7]. Изъятия возможны и должны быть четко определены законом. В остальном требуется эффектив-

[1] Личное делят: в РФ в 40 раз выросло количество утечек персональных данных // Известия. 2023. 7 августа. URL: https://iz.ru/1554402/alena-nefedova/lichnoe-deliat-v-rf-v-40-raz-vyroslo-kolichestvo-utechek-personalnykh-dannykh (дата обращения: 16.08.2023).

ная реакция государства на инциденты неправомерного завладения и распространения чувствительной информации о личности. Кроме того, при заявленном росте терпимости пользователей к тому, что их персональные данные находятся в открытом доступе (тезис этот еще требует верификации)[1], в судебной практике можно обнаружить примеры, когда граждане активно защищают свои права в сфере оборота персональных данных, требуя соответствующих компенсаций от компаний, допустивших утечку чувствительной информации[2].

Методология

Исследование проведено на основе общепринятой методологии. В процессе подготовки представленных выводов и рекомендаций (каждое из которых отражает субъективный взгляд автора на проблему и не претендует на истинность) были задействованы анализ, синтез, формально-юридический и др. Использовались исключительно открытые источники: статьи, монографии, диссертации и иная литература по исследуемой проблематике. Материалы судебной практики были обобщены и изучены посредством обращения к базам справочных правовых систем. Отдельные положения работы обсуждались с представителями IT-отрасли, учеными и правоприменителями.

Результаты и их обсуждение

Персональные данные относятся к разряду той информации, значимость охраны которой всегда имела неоспоримый характер ввиду известного стремления человека к приватности [8; 9]. Не будет преувеличением утверждать о том, что в этом отношении неприкосновенность и защищенность персональных данных выступает неким обязательным элементом свободы человека в целом. Действительно, можно ли говорить о свободе «per se» в условиях, когда «не спрятаться, не скрыться» от неотступного общественного контроля либо еще более неуместного интереса отдельных лиц?

Предварительно следует также указать, что уголовно-правовое обеспечение защищенности оборота персональных данных является важным, но не основным и, конечно же, не первичным механизмом. В этом смысле прежде всего необходимо указать на совершенствование отечественного регулятивного законодательства и института ответственности компаний-операторов персональных данных. В этом отношении заслуживает внимания инициатива о введении оборотных штрафов за утечку данных[3].

Известным и показательным примером здесь выступает Общий регламент Европейского союза о защите персональных данных (General Data Protection Regulation – GDPR)[4]. Новый стандарт без преувеличения изменил само отношение бизнеса к защите чувствительной информации своих клиентов, заставил разработать либо принципиально усовершенствовать юридические и технические механизмы работы с персональными данными [10]. Убедительным стимулом к неукоснительному исполнению требований GDPR явились колоссальные штрафы: British Airways – 204 600 000 €, Mar-

[1] Здесь надо пояснить, что конкретные исследования в этой области автором обнаружены не были.

[2] К «Яндекс.Еде» подан коллективный иск из-за утечки персональных данных // Ведомости. 2022. 29 марта. URL: https://www.vedomosti.ru/media/articles/ 2022/03/29/915773-yandeksede-kollektivnii-isk?ysclid=lluo80foyl735074134 (дата обращения: 16.08.2023).

[3] Бизнес предложили штрафовать до 500 млн за утечку данных россиян // РБК. 2023. 27 июля. URL: https://www.rbc.ru/ technology_and_media/27/07/2023/64c15e069a79474102dac8b0?ysclid=llupgnmw2p69303543 (дата обращения: 18.08.2023).

[4] Общий регламент защиты персональных данных (GDPR) Европейского союза // GDPRTEXT. URL: https://gdpr-text.com/ru/ (дата обращения: 18.08.2023).

riott International, Inc. – 110 390 200 €, Googl LLC – 50 000 000 € и др.[1]

Надо признать, что в современных условиях развития информационных технологий проблема защиты персональных данных крайне осложнилась. Объясняется это всепроникающей природой цифровизации, при которой человеку, вступающему во взаимодействие с компонентами виртуальной среды, каждый раз приходится расставаться с данными о себе [11]. В результате сведения о нашей личности довольно быстро переходят в распоряжение многих субъектов. Почти одновременно с этим информация о пользователе сети Интернет приобретает статус товара, пользующегося высоким спросом на рынке.

Не является секретом, что существование программируемой (контекстной) рекламы, так или иначе, основывается на тщательно организованном механизме слежения за поведением личности в цифровом пространстве. Современный бизнес желает знать, что мы с высокой долей вероятности хотим купить в конкретное время и в конкретном месте. Это определит содержание баннеров, видеороликов, прерывающих трансляции в сети и др. [12, с. 219–268]

Как справедливо замечает Н. И. Пикуров: «Технологические прорывы в средствах коммуникации ставят человека перед выбором: либо решать многочисленные проблемы с помощью новейших средств общения, соглашаясь при этом на значительные риски разглашения сведений о себе, либо отказываться от достижений науки и техники. Этот выбор с давних времен знаком человечеству, и как всегда он делается в пользу новых технологий, даже при необходимости принесения в жертву прежних привычек и привязанностей» [13, с. 201].

Как известно, легальное определение персональных данных представлено в п. 1 ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Вместе с тем указанная дефиниция имеет настолько общий характер, что говорить о возможности ее непосредственного использования для конкретизации предмета преступного посягательства крайне затруднительно. Надо отметить, что это системная проблема, которая отмечается большинством специалистов. Так, например, И. Ю. Павлова указывает на отсутствие на законодательном уровне внятного соотношения между сведениями о клиенте, составляющими банковскую тайну, и персональными данными гражданина [14, с. 47]. С учетом этого закономерно, что защита персональных данных средствами отечественного уголовного закона до настоящего времени решается неоднозначно. В зависимости от конкретных обстоятельств могут быть задействованы разные статьи УК РФ.

Изучение материалов правоприменения позволяет выделить следующие подходы к квалификации общественно опасных посягательств на персональные данные:

– оценка содеянного в соответствии с нормами об ответственности за нарушение неприкосновенности частной жизни и (или) тайны переписки либо переговоров (ст. 137, 138 УК РФ)[2];

– квалификация действий, связанных с неправомерным использованием персональных данных личности для внесения в единый государственный реестр юриди-

[1] Самые крупные многомиллионные штрафы за нарушения GDPR в 2019 году // Медиацентр. URL: https://www.cloudav.ru/ mediacenter/security/gdpr-fines-summary/?ysclid= llusf9ema6333349009 (дата обращения: 18.08.2023).

[2] Приговор Ленинского районного суда города Пензы от 7 июня 2023 г. по делу № 1-53/2023 // Ленинский районный суд г. Пензы. URL: leninsky--pnz.sudzt.ru/ (дата обращения: 18.08.2023).

ческих лиц сведений о подставном лице (ст. 173.2 УК РФ)[1];

– квалификация посягательств на персональные данные как незаконного получения или разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ)[2];

– оценка содеянного как злоупотребления полномочиями (ст. 201, 285 УК РФ). В судебно-следственной практике подобное, как правило, имеет место в случаях распространения персональных данных личности из служебных баз данных. Так, Е., действуя из иной личной заинтересованности, вопреки интересам службы, используя свое служебное положение, находясь в помещении служебного кабинета, при помощи служебного компьютера, применив цифровой ключ, находящийся в его распоряжении, осуществил вход в ФИС «ГИБДД-М», откуда скопировал на принадлежащий ему мобильный телефон посредством фотографирования информацию в отношении В., а именно паспортные данные, сведения о месте ее жительства, номере мобильного телефона, адрес проживания В., сведения о принадлежащем В. паспорте гражданина Российской Федерации[3];

– квалификация посягательств на персональные данные, хранимые в цифровой форме, как преступлений в сфере компьютерной информации (ст. 272, 274.1 УК РФ)[4].

Такое многообразие форм реакции уголовного закона на инциденты с персональными данными объясняется отсутствием в УК РФ специальной нормы об ответственности за соответствующие посягательства. В отечественной доктрине уголовного права обосновываются предложения о криминализации нарушений в сфере оборота персональных данных. Так, В. А. Чукреев предлагает предусмотреть в ст. 137.1 УК РФ ответственность за незаконное изготовление, собирание, фальсификацию, хранение, уничтожение, распространение персональных данных, повлекшее тяжкие последствия [15]. В целом следует поддержать инициативу, направленную на установление самостоятельного уголовно-правового запрета за совершение посягательства на персональные данные. Однако же использование тяжких последствий в качестве криминообразующего признака представляется весьма спорным. Причин тому множество, главная из которых заключается в крайней неопределенности его содержания и известной ввиду этого непоследовательности правоприменения.

Регулятивное законодательство в сфере персональных данных устанавливает ряд фундаментальных ограничений: не допускается обработка персональных данных, несовместимая с целями их сбора; не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой; обрабатываемые персональные данные не

[1] Апелляционное постановление Аннинского районного суда Воронежской области от 22 марта 2021 г. по делу № 10-1/2021 // Аннинский районный суд Воронежской области. URL: anninsky--vzh.sudrf.ru / (дата обращения: 18.08.2023).

[2] Приговор Володарского районного суда города Брянска от 12 августа 2022 г. по делу № 1-176/2022 // Судебные решения РФ. URL: http://www.судебныерешения.рф/70094325?ysclid=l046gurfpb679035552 (дата обращения: 18.08.2023).

[3] Приговор Никулинского районного суда города Москвы от 9 декабря 2022 г. по делу № 01-0627/2022 // Судебные решения РФ. URL: http://www.судебныерешения.рф/72679871?ysclid=lo46gwqy2076231617 (дата обращения: 18.08.2023).

[4] Приговор Кировского городского суда Мурманской области от 8 августа 2022 г. по делу № 1-53/2022 // Кировский городской суд Мурманской области. URL: http://ww.kir.mrm.sudrf.ru/ (дата обращения: 18.08.2023).

должны быть избыточными по отношению к заявленным целям обработки; не допускается обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Нельзя сказать о том, что нарушение соответствующих запретов не охватывается положениями УК РФ. В зависимости от обстоятельств дела и при наличии всех обязательных признаков состава преступления содеянное может быть квалифицировано в соответствии со ст. 201 или ст. 285 УК РФ.

Видимой особенностью посягательств на персональные данные является то, что довольно часто они одновременно затрагивают интересы сотен, тысяч, а иногда миллионов граждан. Здесь возникает сразу два вопроса: 1) как следует подходить к квалификации таких деяний в аспекте института множественности преступлений? 2) необходимо ли учитывать эту закономерность на уровне дифференциации ответственности за конкретные общественно опасные деяния?

В ситуациях, когда одно распространение информации затронуло миллионы пользователей (например, инцидент с утечкой данных клиентов СДЭК: 822 млн строк с информацией об ID, имени и фамилии клиента, адресе электронной почты и телефоне[1]), решение о квалификации содеянного по совокупности преступлений представляется крайне сомнительным. Вменение совокупности будет иметь, очевидно, искусственный характер – никаких миллионов самостоятельных преступлений в действительности не совершалось. Однократность самого деяния, равно как и наличие общего намерения на распространение персональных данных сразу многих пользователей, позволяет утверждать о наличии признаков единичного преступления с множественностью потерпевших [16, с. 201], характеризующегося следующими отличительными чертами: 1) направленностью посягательства на двух или более лиц; 2) причинением вреда нескольким потерпевшим в результате одного преступного деяния; 3) единством умысла виновного.

Вместе с тем с учетом действующей редакции УК РФ такое решение закономерно ставит вопрос о справедливости наказания. В этом отношении представляется перспективным реализовать модель дифференциации уголовной ответственности в зависимости от числа потерпевших от утечки персональных данных. Следует отметить, что подобное решение отчасти реализовано в УК Вьетнама применительно к преступлениям в сфере компьютерной информации. Согласно вьетнамскому уголовному законодательству, лицо подлежит более строгому наказанию в зависимости от количества пораженных устройств пользователей (от 50 до 200, от 200 до 500, свыше 500) [17].

До настоящего времени остается нерешенным вопрос относительно квалификации создания и использования поддельных аккаунтов в социальных сетях с указанием персональных данных конкретного человека (имени, фамилии, даты рождения и фото). Теоретики и практики соглашаются в том, что при наличии на то оснований такие действия могут содержать признаки клеветы (ст. 128.1 УК РФ). Однако это лишь при условии распространения недостоверных и порочащих сведений. Вместе с тем, когда поддельный аккаунт используется в иных целях (для рекламы товаров либо услуг), вопрос о правовой оценке содеянного

[1] СДЭК заявил об утечке данных российских и украинских пользователей // РБК. 2022. 28 февраля. URL: https://www.rbc.ru/rbcfreenews/621c80509a79474ce51bb699 (дата обращения: 15.07.2023).

уже является неоднозначным. Нельзя также не принимать во внимание, что в результате указанных действий могут наступить и иные неблагоприятные последствия (потеря работы, разрыв деловых отношений и др.). Возвращаясь к ранее отмеченной инициативе о специальной криминализации неправомерных действий в сфере оборота персональных данных, можно предположить, что данная проблема могла бы быть успешно решена в рамках такой нормы (например, при криминализации незаконного использования персональных данных, повлекшего существенное нарушение прав и свобод гражданина).

Отдельного внимания заслуживает проблема специальной охраны биометрических персональных данных [18; 19]. Специалистами отмечается, что вероятность ошибки при использовании биометрии составляет 1: 10 000 000. При такой декларируемой надежности государством взят курс на широкое использование биометрии при выдаче документов и совершении иных юридически значимых действий. Не отстает в этом отношении и бизнес, внедряя технологии идентификации клиентов по биометрии при совершении финансовых операций. Вместе с тем уже известны инциденты несанкционированного доступа и копирования биометрических персональных данных человека. Так, в марте 2019 г. злоумышленник позвонил в одну британскую энергетическую компанию и представился руководителем головной компании из Германии. Директор, доверившись голосу по телефону, решил, что разговаривает со старшим руководителем. Последний распорядился осуществить транзакцию венгерскому поставщику. В результате этого компании был причинен ущерб в размере 243 000 долл. [20]

С учетом изложенного можно сделать вывод, что отечественный механизм уголовно-правовой охраны требует совершенствования с точки зрения развития технологий биометрических персональных данных. Полагаем, что значимость подобной информации о личности требует дифференцированного подхода к установлению ответственности за неправомерные действия в отношении биометрии.

Выводы

Уголовно-правовое обеспечение неприкосновенности персональных данных не теряет своей актуальности в современных условиях. Цифровизация обусловила повышение социальной толерантности к нарушениям в сфере неприкосновенности персональных данных и частной жизни. Вместе с тем развитие электронного правительства и цифровой экономики в России требует построения и реализации эффективных юридических и технических механизмов работы с персональными данными.

Совершенствование уголовно-правовой охраны оборота персональных данных должно предваряться и (или) сопровождаться изменением отечественного регулятивного законодательства и института ответственности компаний-операторов персональных данных. В этом отношении заслуживает поддержки инициатива о введении оборотных штрафов за утечку данных.

Перспективными направлениями изменения отечественного уголовного закона в целях повышения защиты персональных данных граждан представляются: 1) специальная криминализация нарушений в сфере оборота персональных данных; 2) дифференциация уголовной ответственности за посягательство на персональные данные в зависимости от количества потерпевших; 3) дифференциация уголовной ответственности за посягательство на биометрические персональные данные.

Список литературы

1. Изергин Д. А. Выявление каналов компрометации персональных данных пользователей мобильных устройств на основе интеллектуальных технологий: дис. … канд. техн. наук. СПб., 2022. 179 с.

2. Privacy, Big Data, and the public good: frameworks for engagement / J. Lane, V. Stodden, S. Bender, H. Nissenbaum. Cambridge: Cambridge University Press, 2014. 344 p.

3. Савельев А. И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 43–66.

4. Волкова А. Ю. Персональные данные как объект уголовно-правовой охраны // Уголовное право: стратегия развития в XXI веке. 2023. № 3. С. 132–137.

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. Хохлова Е. В. Социальная обусловленность уголовной ответственности за преступления, связанные с персональными данными // Вестник Тверского государственного университета. Серия: Право. 2022. № 3 (71). С. 141–148.

7. Шутова А. А. Социальная обусловленность существования норм об уголовной ответственности за посягательства на персональные данные // Вестник Нижегородской академии МВД России. 2015. № 4 (32). С. 332–335.

8. Ефремова М. А. Информация с ограниченным доступом как объект уголовно-правовой охраны // Вестник Казанского юридического института МВД России. 2012. № 4 (10). С. 102–106.

9. Камалова Г. Г. Теоретико-правовые аспекты эволюции прав человека в условиях цифровизации и внедрения технологии искусственного интеллекта // Вестник Удмуртского университета. Серия: Экономика и право. 2021. Т. 31, вып. 4. С. 662–668.

10. Шебанова Н. А. Охрана персональных данных: опыт Европейского сообщества // Журнал Суда по интеллектуальным правам. 2019. № 25. С. 5–14.

11. Минбалеев А. В., Сторожакова Е. Э. Проблемы правовой охраны персональных данных в процессе использования нейронных сетей // Вестник Университета имени О. Е. Кутафина (МГЮА). 2023. № 2 (102). С. 71–79.

12. Черешнев Е. Как остаться человеком в эпоху расцвета искусственного интеллекта. М.: Альпина Паблишер, 2022. 484 с.

13. Пикуров Н. И. Персональные данные, «большие данные» и частная жизнь: сложные вопросы уголовно-правовой оценки незаконного оборота // Эффективность уголовно-правового, криминологического и уголовно-исполнительного противодействия преступности: материалы XII Российского конгресса уголовного права, состоявшегося 28–29 мая 2020 г. М.: Юрлитинформ, 2020. С. 201–205.

14. Павлова И. Ю. Соотношение правового регулирования банковской тайны и персональных данных гражданина в свете новелл законодательства о персональных данных // Государственная служба и кадры. 2021. № 3. С. 43–47.

15. Чукреев В. А. Персональные данные, в том числе биометрические данные, как предметы уголовно-правовой охраны // Вестник Университета имени О. Е. Кутафина. 2022. № 3. С. 107–116.

16. Актуальные проблемы уголовного права: курс лекций / под ред. О. С. Капинус; рук. авт. кол. К. В. Ображиев. М.: Академия Генеральной прокуратуры Российской Федерации, 2015. 484 с.

17. Русскевич Е. А., Ву Тхи Хуен, Нгуен Тиен Дат. Уголовная ответственность за преступления в сфере компьютерной информации по законодательству Социалистической Республики Вьетнам // Журнал зарубежного законодательства и сравнительного правоведения. 2021. Т. 17, № 6. С. 38–47.

18. Брызгин А. А., Минбалеев А. В. Правовой режим биометрических персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2012. № 2 (4). С. 35–41.

19. Архипов В. В., Наумов В. Б. Теоретико-правовые вопросы охраны прав человека при использовании биометрических данных системами искусственного интеллекта: европейский опыт // Вестник Удмуртского университета. Серия: Экономика и право. 2022. Т. 32, № 1. С. 109–118.

20. Stupp C. Fraudsters Used ai to mimic ceo’s voice in unusual cybercrime case // The Wall Street Journal. 2019. August 30. URL: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 (дата обращения: 18.08.2023).

References

1. Izergin D. A. Vyyavlenie kanalov komprometacii personal'nyh dannyh pol'zovatelej mobil'nyh ustrojstv na osnove intellektual'nyh tekhnologij. Diss. kand. tekhn. nauk [Identification of channels for compromising personal data of users of mobile devices based on intelligent technologies. Cand. eng. sci. diss.]. St. Petersburg, 2022. 179 p.

2. Lane J., Stodden V., Bender S., Nissenbaum H. Privacy, Big Data, and the public good: frameworks for engagement. Cambridge, Cambridge University Press, 2014. 344 p.

3. Savel'ev A. I. Problemy primeneniya zakonodatel'stva o personal'nyh dannyh v epohu "Bol'shih dannyh" (Big Data) [Problems of application of legislation on personal data in the era of "Big Data" (Big Data)]. *Pravo. Zhurnal Vysshej shkoly ekonomiki = Law. Journal of the Higher School of Economics*, 2015, no 1, pp. 43–66.

4. Volkova A. Y. Personal'nye dannye kak ob"ekt ugolovno-pravovoj ohrany [Personal data as an object of criminal law protection]. *Ugolovnoe pravo: strategiya razvitiya v XXI veke = Criminal law: development strategy in the XXI century*, 2023, no. 3, pp. 132–137.

5. Kapinus O. S. Bezopasnost' personal'nyh dannyh kak odin iz vazhnejshih ob"ektov konstitucionno-pravovoj ohrany [Security of personal data as one of the most important objects of constitutional and legal protection]. *Vestnik Universiteta prokuratury Rossijskoj Federacii = Bulletin of the University of the Prosecutor's Office of the Russian Federation*, 2018, no. 6 (68), pp. 10–15.

6. Hohlova E. V. Social'naya obuslovlennost' ugolovnoj otvetstvennosti za prestupleniya, svyazannye s personal'nymi dannymi [Social conditionality of criminal liability for crimes related to personal data]. *Vestnik Tverskogo gosudarstvennogo universiteta. Seriya: Pravo = Bulletin of Tver State University. Series: Law,* 2022, no. 3 (71), pp. 141–148.

7. Shutova A. A. Social'naya obuslovlennost' sushchestvovaniya norm ob ugolovnoj otvetstvennosti za posyagatel'stva na personal'nye dannye [Social conditionality of the existence of norms on criminal liability for attacks on personal data]. *Vestnik Nizhegorodskoj akademii MVD Rossii = Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia,* 2015, no. 4 (32), pp. 332–335.

8. Efremova M. A. Informatsiya s ogranichennym dostupom kak ob"ekt ugolovno-pravovoj ohrany [Information with limited access as an object of criminal law protection]. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia*, 2012, no. 4 (10), pp. 102–106.

9. Kamalova G. G. Teoretiko-pravovye aspekty evolyutsii prav cheloveka v usloviyah tsifrovizatsii i vnedreniya tekhnologii iskusstvennogo intellekta [Theoretical and legal aspects of the evolution of human rights in the context of digitalization and the introduction of artificial intelligence technology]. *Vestnik Udmurtskogo universiteta. Seriya: Ekonomika i pravo = Bulletin of the Udmurt University. Series: Economics and Law,* 2021, vol. 31, no. 4, pp. 662–668.

10. Shebanova N. A. Ohrana personal'nyh dannyh: opyt Evropejskogo soobshchestva [Protection of personal data: the experience of the European community]. *Zhurnal Suda po intellektual'nym pravam = Journal of the Intellectual Property Rights Court*, 2019, no. 25, pp. 5–14.

11. Minbaleev A.V., Storozhakova E. E. Problemy pravovoj ohrany personal'nyh dannyh v processe ispol'zovaniya nejronnyh setej [Problems of legal protection of personal data in the process of using neural networks]. *Vestnik Universiteta imeni O. E. Kutafina (MGYUA) = Bulletin Kutafin Moscow State Law University (MSAL),* 2023, no. 2 (102), pp. 71–79.

12. Chereshnev E. Kak ostat'sya chelovekom v epohu rastsveta iskusstvennogo intellekta [How to remain human in the heyday of artificial intelligence]. Moscow, Al'pina Publ., 2022. 484 p.

13. Pikurov N. I. Personal'nye dannye, "bol'shie dannye" i chastnaya zhizn': slozhnye voprosy ugolovno-pravovoj otsenki nezakonnogo oborota [Personal data, "big data" and private life: complex issues of criminal law assessment of illicit trafficking]. *Effektivnost' ugolovno-pravovogo, kriminologicheskogo i ugolovno-ispolnitel'nogo protivodejstviya prestupnosti. Materialy XII Rossijskogo kongressa ugolovnogo prava* [Efficiency of criminal law, criminological and penitentiary counteraction to crime: materials of the XII Russian Congress of Criminal Law]. Moscow, Yurlitinform Publ., 2020, pp. 201–205.

14. Pavlova I. Y. Sootnoshenie pravovogo regulirovaniya bankovskoj tajny i personal'nyh dannyh grazhdanina v svete novell zakonodatel'stva o personal'nyh dannyh [Correlation of legal regulation of banking secrecy and personal data of a citizen in the light of novelties of legislation on personal data]. *Gosudarstvennaya sluzhba i kadry = State Service and Personnel,* 2021, no. 3, pp. 43–47.

15. Chukreev V. A. Personal'nye dannye, v tom chisle biometricheskie dannye, kak predmety ugolovno-pravovoj ohrany [Personal data, including biometric data, as subjects of criminal law protection]. *Vestnik Universiteta imeni O. E. Kutafina = Bulletin of the Kutafin Moscow State Law University (MSAL)*, 2022, no. 3, pp. 107–116.

16. Aktual'nye problemy ugolovnogo prava [Actual problems of criminal law]; ed. O. S. Kapinus; hands ed. count K. V. Obrazhiev. Moscow, Academy of the General Prosecutor's Office of the Russian Federation Publ., 2015. 484 p.

17. Russkevich E. A., Vu Thi Huen, Nguen Tien Dat. Ugolovnaya otvetstvennost' za prestupleniya v sfere komp'yuternoj informatsii po zakonodatel'stvu Socialisticheskoj Respubliki V'etnam [Criminal liability for crimes in the field of computer information under the legislation of the Socialist Republic of Vietnam]. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya = Journal of Foreign Legislation and Comparative Law*, 2021, vol. 17, no. 6, pp. 38–47.

18. Bryzgin A. A., Minbaleev A. V. Pravovoj rezhim biometricheskih personal'nyh dannyh [Legal regime of biometric personal data]. *Vestnik UrFO. Bezopasnost' v informacionnoj sfere = Bulletin Ural Federal District. Security in the information sphere*, 2012, no. 2 (4), pp. 35–41.

19. Arhipov V. V., Naumov V. B. Teoretiko-pravovye voprosy ohrany prav cheloveka pri ispol'zovanii biometricheskih dannyh sistemami iskusstvennogo intellekta: evropejskij opyt [Theoretical and legal issues of human rights protection when using biometric data by artificial intelligence systems: European experience]. *Vestnik Udmurtskogo universiteta. Seriya: Ekonomika i pravo = Bulletin of the Udmurt University. Series: Economics and Law*, 2022, vol. 32, no. 1, pp. 109–118.

20. Stupp C. Fraudsters Used ai to mimic CEO's voice in unusual cybercrime case. *The Wall Street Journal,* 2019, August 30. URL: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 (accessed: 18.08.2023).

Информация об авторе / Information about the Author

Русскевич Евгений Александрович, доктор юридических наук, доцент, профессор кафедры уголовного права, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), г. Москва, Российская Федерация,
e-mail: russkevich@mail.ru,
ORCID: 0000-0003-4587-8258

Evgeny A. Russkevich, Doctor of Sciences (Juridical), Professor of the Department of Criminal Law, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation,
e-mail: russkevich@mail.ru,
ORCID: 0000-0003-4587-8258