УДК 343.45
DOI: 10.26456/vtpravo/2022.3.141

СОЦИАЛЬНАЯ ОБУСЛОВЛЕННОСТЬ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ, СВЯЗАННЫЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ[1]

Е.В. Хохлова

ФГБОУ ВО «Юго-Западный государственный университет», г. Курск

Рассматривается проблема социальной обусловленности уголовно-правового запрета посягательств в отношении персональных данных человека. Объектом исследования являются общественные отношения, возникающие в связи с установлением уголовной ответственности за нарушения неприкосновенности персональных данных человека, а его целью – выявление оснований их уголовно-правовой охраны. Для достижения указанной цели применялись формально-юридический, системно-структурный методы юридической науки. Автор развивает и углубляет теорию в части социально-правового и криминологического обоснования криминализации рассматриваемых деяний. Делается вывод об обоснованности уголовно-правовой охраны персональных данных в связи с высокими рисками «деаномизации» для фундаментальных прав человека.

Ключевые слова: *персональные данные человека, социальная обусловленность, общественная опасность, нарушение неприкосновенности частной жизни человека, виртуализация, информационно-коммуникационные технологии.*

С развитием информационных технологий и их глобальным внедрением значительно увеличилось количество электронных баз, содержащих персональные данные о человеке, доступ к которым многократно увеличил риск вторжения в чужую частную жизнь. Так, в отчете экспертно-аналитического центра компании InfoWatch говорится, что в I половине 2022 г. количество утечек персональной информации ограниченного доступа в России составило 305, что на 45,9% больше, чем за тот же период 2021 г. Объем «утекшей» информации с персональными данными в нашей стране составил 187,6 млн. записей, что превышает численность всего российского населения [3].

Для понимания глобальности проблемы незаконного оборота персональных данных человека как одного из видов тайны приведем статистику состояния защищенности неприкосновенности частной жизни. В этих целях укажем в скобках количество пользователей различных приложений, плеймаркетов и прочих сервисов, чье право на анонимизацию частной жизни было нарушено. Среди допустивших попадание клиентской базы в открытые источники: Сбербанк (65 млн. россиян), «Почта России» (10 млн. данных отправителей и получателей), «ВымпелКом» («Билайн») (2 млн. абонентов); Служба доставки «Экспресс-курьер» (25 млн. пользователей) и др. В открытый доступ попали ФИО, дата рождения, гражданство, номера СНИЛС, ИНН, адреса места жительства, телефоны, фото, серии и номера паспорта, суммы дохода, электронная почта, пароли от аккаунтов, данные кредитных карт, банковские счета, авиа– и железнодорожные перелеты, сведения о недвижимости, о членах семьи и др. Беспрецедентное количество жертв позволяет говорить о гипертаргетированности этого вида преступности, то есть нацеленности на значительное число потерпевших. Активность злоумышленников в отношении именно этих данных объясняется их коммерциализацией и ликвидностью на «черном рынке», поскольку существует спрос на базы данных о российских гражданах. Очевидно, что количество случившихся только в последние годы инцидентов с массовой утечкой в открытый доступ персональных данных миллионов граждан подтверждает социальную обусловленность уголовной ответственности за посягательства в отношении персональных данных человека. Она определяется, прежде всего, объективной потребностью в защите права человека как субъекта персональных данных на неприкосновенность частной жизни, которое гарантируется ст. 23 и 24 Конституции РФ, а также его информационными правами, в том числе правом на свободу информации.

При сохранении дискуссии об основаниях уголовного запрета (или уголовной ответственности) учеными не опровергается тезис об отнесении законодателем того или иного деяния к категории преступных на основе оценки общественной опасности, раскрывающей его социальную природу. Норма уголовного закона должна предусматривать те и только те деяния, которые действительно опасны для общества и с которыми вести борьбу можно только уголовно-правовыми средствами [9, с.

[1] Работа подготовлена под научным руководством к.ю.н., доцента М.Н. Урда в рамках выполнения государственного задания на 2022г. «Трансформация частного и публичного права в условиях эволюционирующих общества и государства» (№ 0851-2020-0033).

6]. В теории уголовного права доказано, что общественная опасность преступления обладает признаком причинения общественным отношениям неизбежного или максимально вероятного вреда правоохраняемым благам, а в случае с персональными данными еще и множественного.

Высокая степень общественной опасности противоправных деяний с чужими персональными данными, во-первых, обусловлена последующим их использованием для совершения новых преступлений, а потому причиняемый от незаконного доступа и распространения личной информации вред не может быть минимизирован административной ответственностью. По данным нашего опроса, представители правоохранительных органов выделили две самые большие группы преступлений с персональными данными человека – против собственности (59,4%) и против конституционных прав и свобод человека и гражданина (31,8%). Как показывает следственно-судебная практика, после покупки на нелегальных сервисах в сети Интернет, занимающихся противоправным оборотом личной информации, конфиденциальные сведения о человеке (доходы, состояние здоровья, биометрия, генетика, собственность) используются для совершения правонарушений, в том числе преступлений.

Вред приобретает здесь иные качественно-количественные характеристики, что придает деяниям, связанным с персональными данными, свойство общественной опасности, отличающее его от административно-правовых нарушений. Он проявляется не только в самой «деаномизации», но и в увеличении риска наступления особой тяжести последствий для идентифицированного лица. В их числе дискредитация потерпевшего (опорочение чести и достоинства, деловой репутации), вымогательство денежных средств, а также мошеннические схемы с использованием личных данных о нем – получение микрозаймов по скан-копиям чужих паспортов, транзакции под «легендой» хищения с банкового счета денег злоумышленниками, оформление кредитов, в т.ч. с использованием методов социальной инженерии. Только в I квартале 2022 г. Банк России зафиксировал 258097 операций без согласия клиентов, объем которых составил 3 млн. 294 тыс. руб. Доля социальной инженерии, т.е. психологического манипулирования людьми, как правило, с использованием персональных данных для совершения определенных действий или разглашения конфиденциальной информации, составила 52,5% [10].

О других типичных способах использования расшифрованной личной информации свидетельствует обобщение следственно-судебной практики по делам, связанным с персональными данными человека. Среди них изготовление поддельных паспортов на чужое имя («кража личности»); создание «фирм-однодневок» для внесения в Единый государственный реестр юридических лиц сведений о подставном лице [16, с. 333]; создание электронных цифровых подписей и совершение юридически значимых действий (например, продажа квартиры); иные посягательства против собственности (покупки в интернет-магазинах, кражи с банковских счетов и др.). Как утверждают криминологи, личные данные жертвы создают анонимность для преступников и террористов и представляют угрозу как для национальной безопасности, так и для частных лиц [8, с. 437].

Во-вторых, социальный интерес в установлении уголовно-правового запрета на противоправный доступ к персональным данным человека и их незаконный оборот детерминирован не только массовостью и латентностью преступлений, а их организованным и профессиональным характером, трансграничными связями организованных групп и использованием иностранного сегмента сети Интернет. Правоохранительные органы выявляют многочисленные случаи размещения баз с персональными данными российских граждан на территории иностранных государств. Примером является кибератака на внутренние ресурсы РЖД жителя г. Краснодара, специалиста в IT-сфере. Используя для авторизации незаконно добытые учетные записи работников ОАО «РЖД» и 96 уникальных IP-адресов, он скопировал несколько сотен тысяч фотографий и другие персональные данные 700 тыс. руководства и сотрудников, включая имена, даты рождения, адреса, номера СНИЛС, должности, фотографии и номера телефонов. Впоследствии он опубликовал эту информацию на хостинге интернет-ресурса, расположенного в ФРГ [5].

В-третьих, деяния, связанные с незаконным нарушением сохранности персональных данных человека, создают угрозу причинения ущерба и государственной безопасности в том случае, когда речь идет о лицах, ее обеспечивающих. Криминальная практика последних лет подтверждает факты незаконного сбора персональных данных сотрудников правоохранительных органов и военнослужащих, что создает угрозу не только их жизни, здоровью, а также личной безопасности их родных и близких. Так, в 2022 г. по сообщениям Центра общественных связей ФСБ РФ, спецслужба пресекла деятельность группы из четырех сотрудников частного сыска и налоговых органов,

осуществлявших с 2019 г. в интересах третьих лиц, в том числе иностранных граждан, незаконный сбор персональной информации, позволяющей идентифицировать тридцать человек. Именно налоговики, имея доступ к базе данных «предоставляли через посредника информацию об источниках дохода физических лиц, счетах, открытых в кредитных организациях, адресах регистрации и имуществе, а также другие сведения, составляющие охраняемую законом тайну» [16].

В-четвертых, еще одним основанием для криминализации несанкционированного доступа к персональным данным человека, хранящимся на специальных ресурсах операторов, является материальный ущерб, который может быть причинен от их похищения. И речь идет не только об использовании конфиденциальной информации персонального характера для совершения новых преступлений, но о финансовых затратах, которые возникают при устранении последствий ее обнародования. Об этом на Петербургском международном экономическом форуме в 2022 г. заявил, в частности, зампред правления Сбербанка Станислав Кузнецов. В результате компрометации 13 млн. банковских карт Сбербанк был вынужден осуществить перевыпуск 1 млн. карт своих клиентов, ущерб от которого составил не менее 4,5 млрд. рублей. Другие 12 млн. карт принадлежат владельцам иных кредитных организаций, что только подтверждает тяжесть последствий «большой утечки» для всей отрасли [14].

В-пятых, в качестве одного из социальных обоснований уголовной ответственности за преступления с персональными данными человека является ежегодная положительная динамика их совершения с использованием информационных технологий (прежде всего, хакерские атаки на информационные ресурсы посредством вирусных программ). Именно этот способ многократно повышает степень общественной опасности деяний, при совершении которых для неправомерного доступа к соответствующим объектам используются компьютерные системы или сети.

В-шестых, негативным следствием перехода общества в цифровую эпоху явилась все большая «миграция» преступлений, связанных с персональными данными, в киберпространство [13, с. 73]. Это способствовало массовому распространению в теневом сегменте Интернета анонимной информации о личности пользователей как своего рода «товара», кибер-сталкингу, когда персональные данные жертвы было получены с помощью кражи онлайн-личности (в соцсетях, на веб-сайтах и через поисковые системы), кибербуллингу, диффамации и др.

На процесс криминализации посягательств в отношении информации ограниченного доступа существенное влияние оказывают и социально-психологические основания, в том числе общественная психология и правосознание [7, с. 67]. О том, что россияне усматривают особую опасность в получении и использовании своих персональных данных третьими лицами, их передаче от одних компаний к другим в коммерческих и иных целях, подтверждают результаты опроса ВЦИОМ: 58% респондентов считают, что доступ третьих лиц к их данным может представлять для них личную угрозу [11].

Среди правовых оснований криминализации деяний, посягающих на безопасность персональных данных человека, особое значение приобретают положения международных актов. Мировым сообществом фундаментальное право на неприкосновенность частной жизни, включая право на защиту персональных данных человека, признается особо охраняемой категорией, о чем провозглашается в преамбуле Конвенции Совета Европы «О защите личности в связи с автоматизированной обработкой персональных данных» (Конвенция 108) [1]. Государства, ее подписавшие, подтверждают приверженность свободе информации, невзирая на границы, и признают необходимость уважения неприкосновенности частной жизни и свободного обмена информацией между народами. Как участница Конвенции с 2001 г. Российская Федерация, ратифицировавшая ее Федеральным законом от 19.12.2005 № 160-ФЗ, возложила на себя международно-правовые обязательства по принятию надлежащих санкций по защите личных данных в национальном праве.

Традиционно в научных исследованиях в качестве другого из социально-криминологических оснований общественной опасности приводится показатель распространённости (массовости) того или иного посягательства, однако подобный анализ исключен ввиду объективных причин. В государственной системе учета преступлений деяния, предметом которых являются персональные данные человека либо они используются для совершения других преступлений, не выделяются специально [6, с. 11]. Косвенно судить о состоянии с защитой персональных данных человека позволяет приведенная выше статистика, подтверждающая не только особую тяжесть последствий в

виде причинения вреда (жизни, чести и достоинству, материального ущерба и др.), но и его множественность с огромным числом потерпевших.

При рассмотрении проблемы социальной обусловленности любого уголовно-правового запрета учеными-юристами обсуждается вопрос о том, достигает ли деяние той степени вредоносности, при которой можно говорить о совершении именно преступления, возможно ли эффективное противодействие деянию без применения уголовно-правовых средств иными, более мягкими мерами. О том, что только административно- и гражданско-правовыми мерами обеспечить защиту граждан от незаконного доступа и оборота их персональных данных невозможно, подтверждает неэффективность административных средств борьбы с правонарушениями в этой сфере. Имеющиеся в арсенале административного законодательства составы правонарушений не обладают достаточным превентивным потенциалом для предупреждения противоправных деяний, связанных с персональными данными, хотя бы потому, что применяемые размеры штрафов не способны обеспечить их надлежащую охрану. По ч. 6 ст. 13.11 КоАП РФ в случае необеспечения сохранности персональных данных, если это повлекло в том числе распространение либо иные неправомерные действия в отношении персональных данных, первый штраф для юридических лиц составляет от пятидесяти тысяч до ста тысяч рублей. Так, штраф, который назначил суд по ст. 13.11 КоАП РФ компании «Гемотест» за утечку 30 млн. личных данных клиентов, составил всего 60 тыс. руб. [4].

Таким образом, масштабность проблемы защиты личной информации в России со всей очевидностью свидетельствует о необходимости и оправданности установления уголовно-правового запрета в отношении деяний, совершаемых с использованием персональных данных человека или против них. Обусловленность этого запрета определяется общественной опасностью этих преступлений, выраженной в общественной ценности нарушаемых прав и свобод человека (неприкосновенность частной жизни, жизнь, собственность, честь, достоинство), распространенностью, глобальной компьютеризированностью, виртуализацией, латентностью и социально вредными последствиями.

Список литературы

1. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в Страсбурге 28.01.1981 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».
2. Афанасьева О.В. Право на неприкосновенность частной жизни. Укрепляет ли его закон о персональных данных? // Общественные науки и современность. 2011. № 6. С. 76–88.
3. В России резко участились кражи персональных данных – число похищенных записей превысило население страны. Отчёт об утечках данных за I полугодие 2022 года [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/analitika/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda (дата обращения: 09.08.2022).
4. «Гемотест» оштрафовали на 60 тыс. руб. за утечку персональных данных [Электронный ресурс]. URL: https://www.kommersant.ru/doc/5480244 (дата обращения: 17.08.2022).
5. Жителю Краснодарского края предъявлено обвинение в совершении киберпреступлений [Электронный ресурс]. URL: https://zmsut.sledcom.ru/news/item/1417513 (дата обращения: 17.08.2022).
6. 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.
7. Коробеев А.И. Советская уголовно-правовая политика: проблемы декриминализации и пенализации. Владивосток: Изд.-во Дальневост. ун-та, 1987. 268 с.
8. Криминология / под ред. В.Н. Кудрявцева и В.Е. Эминова. 5-е изд., перераб. и доп. М.: Норма-ИНФРА-М, 2022. 800 с.
9. Кудрявцев В.Н. Криминализация: оптимальные модели // Уголовное право в борьбе с преступностью. М.: Изд-во ИГиП АН СССР, 1981. С. 3–10.
10. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств [Электронный ресурс]. URL: https://cbr.ru/analytics/ib/review_4q_2022/(дата обращения: 01.09.2022).
11. Персональные данные в интернете: угроза утечки и как с ней бороться [Электронный ресурс]. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/personalnye-dannye-v-internete-ugroza-utechki-i-kak-s-nei-borotsja (дата обращения: 17.08.2022).
12. Переписка и геоданные россиян могли утекать зарубежным мошенникам [Электронный ресурс]. URL:https://iz.ru/1385527/2022-08-26/perepiska-i-geodannye-rossiian-mogli-utekat-zarubezhnym-moshennikam (дата обращения: 17.08.2022).

13. Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дис. ... д-ра юрид. наук. М., 2021. 521 с.

14. Сбер оценивает ущерб от перевыпуска скомпрометированных в России карт в 4,5 млрд. рублей [Электронный ресурс]. URL: https://www.gazeta.ru/business/news/2022/06/16/17944346.shtml (дата обращения: 17.08.2022).

15. ФСБ РФ разоблачила сливавших иностранцам данные о военнослужащих [Электронный ресурс]. URL: https://iz.ru/1352429/2022-06-20/fsb-rf-razoblachila-slivavshikh-inostrantcam-dannye-o-voennosluzhashchikh (дата обращения: 23.08.2022).

16. 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.

Об авторе:

ХОХЛОВА Елена Васильевна – аспирантка ФГБОУ ВО «Юго-Западный государственный университет» (305040, г. Курск, ул. 50 лет Октября, 94), e-mail: khokhlova1975@bk.ru, ORCID 0000-0002-0743-4667

SOCIAL RESPONSIBILITY FOR PERSONAL DATA OFFENCES

E.V. Khokhlova

Southwest State University, Kursk

The problem of social conditionality of the criminal law prohibition of encroachments against personal data of a person is being considered. The object of the study is social relations arising in connection with the establishment of criminal liability for violations of the inviolability of personal data of a person, and its purpose is to identify the grounds for their criminal protection. For this purpose, formal-legal, system-structural methods of legal science were used. The author develops and deepens the theory in terms of socio-legal and criminological justification for the criminalization of the crimes in question. It is concluded that the criminal law protection of personal data is justified in connection with the high risks of «deanomization» for fundamental human rights.
Keywords: *personal human data, social conditioning, social danger, violation of human privacy, virtualization, information and communication technologies.*

About author:

KHOKHLOVA Elena – graduate student of the Southwest State University, 305040, Kursk, 50 years of October, 94 St., ORCID 0000-0002-0743-4667, e-mail: khokhlova1975@bk.ru

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