Научная статья
УДК 343
doi 10.46741/2713-2811.2024.25.1.012

Проблемы уголовно-правовой охраны персональных данных в сети «Интернет»

ТАТЬЯНА ВЛАДИМИРОВНА КОРНИЛОВА

Вологодский институт права и экономики ФСИН России, Вологда, Россия, tatyana_vladi21@mail.ru, https://orcid.org/0000-0003-1978-9294

ЕГОР ОЛЕГОВИЧ ЛАПЕНКОВ

Вологодский институт права и экономики ФСИН России, Вологда, Россия, egorlapenkov@yandex.ru, https://orcid.org/0000-0001-8754-2264

Аннотация. В статье рассматриваются понятия персональных данных и личной информации пользователей сайтов в сети Интернет, а также поднимается проблема защиты этих данных, раскрываются существующие угрозы и пути их реализации, в том числе с помощью ужесточения уголовно-правовой ответственности. Анализируется международное и национальное законодательство, предлагаются возможные способы блокировки доступа третьих лиц к персональным данным онлайн-ресурсов.

Ключевые слова: персональные данные; уголовно-правовая защита персональных данных; информация; личная информация; сеть Интернет.

5.1.4. Уголовно-правовые науки.

Для цитирования: Корнилова Т. В., Лапенков Е. О. Проблемы уголовно-правовой охраны персональных данных в сети «Интернет» // Ius publicum et privatum: сетевой научно-практический журнал частного и публичного права. 2024. № 1 (25). С. 97–102. doi 10.46741/2713-2811.2024.25.1.012.

Original article

Problems of Criminal Law Protection of Personal Data on the Internet

TAT'YANA V. KORNILOVA

VILE of the FPS of Russia, Vologda, Russia, tatyana_vladi21@mail.ru, https://orcid.org/0000-0003-1978-9294

EGOR O. LAPENKOV

VILE of the FPS of Russia, Vologda, Russia, egorlapenkov@yandex.ru, https://orcid.org/0000-0001-8754-2264

Abstract. The article considers the concept of personal data and personal information of Internet users, as well as raises the problem of protecting this data, reveals existing threats and ways to implement them, including by tightening criminal liability. International and national legislation is analyzed, and possible ways to block third-party access to personal data of online resources are proposed.

Keywords: personal data; criminal law protection of personal data; information; personal information; the Internet.

5.1.4. Criminal law sciences.

For citation: Kornilova T.V., Lapenkov E.O. Problems of criminal law protection of personal data on the Internet. *Ius publicum et privatum: online scientific and practical journal of private and public law*, 2024, no. 1 (25), pp. 97–102. doi 10.46741/2713-2811.2024.25.1.012.

В условиях повсеместной цифровизации, а также совершенствования правовых систем появляются инновационные технологии, в том числе и в правовой сфере. Одним из молодых правовых институтов в Российской Федерации стал институт персональных данных. Впервые право на неприкосновенность частной жизни как самостоятельное право было сформулировано в Декларации прав и свобод человека и гражданина, принятой Верховным Советом РСФСР 22 ноября 1991 г. В 2000 г. в Совете Безопасности Российской Федерации была сформирована рабочая группа по подготовке проекта принятого впоследствии Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» [1].

Как любое нововведение в правовой отрасли, данный институт содержал в себе ряд неурегулированных вопросов. В частности, любое действие пользователей в сети Интернет имеет определенные риски, но применительно к персональным данным граждан Российской Федерации эти риски наиболее велики, поскольку представляют личную тайну и охраняются законодательством. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» относит персональные данные к конфиденциальной информации. Однако случаи хищения такой информации нередки. Так, только в 2020 г. было выявлено более десяти случаев масштабных краж личной информации участников различных организаций. Например, на продажу были выставлены персональные данные россиян, которые оформляли микрозаймы в 2017–2019 гг. В базе содержалось 12 млн записей с паспортными данными, телефонами и сведениями об электронных кошельках [2].

В связи с этим актуальность уголовно-правовой защиты персональных данных в сети Интернет в условиях постоянно совершенствующейся информационной сферы невероятно велика. Необходимо не только быстро реагировать на возникающие угрозы, но и быть на шаг впереди, чтобы защитить информацию пользователей от возможных угроз.

Прежде чем перейти к рассмотрению основной проблемы – защите персональных данных в сети Интернет – следует проанализировать данное понятие, а также определить, какая именно информация подпадает под рассматриваемую категорию.

Согласно Федеральному закону «О персональных данных», персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Следует отметить, что данное понятие сформулировано очень широко, отсутствуют конкретизирующие положения или примеры, что создает сложности правоприменения не только для граждан, но и опытных юристов. К слову, одна из предыдущих редакций закона содержала более конкретизированный пере-

чень сведений, относящихся к данной категории, а именно: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Следует подчеркнуть, что такое широкое определение содержится и в международно-правовых документах. Например, ст. 2 Конвенции Совета Европы от 28.01.1981 № 108 «О защите индивидуумов (частных лиц) при автоматизированной обработке персональных данных» содержит следующее определение персональных данных: персональные данные означают любую информацию об определенном или поддающемся определению физическом лице («субъект данных»).

Такое широкое толкование имеет смысл, так как дает основание индивидуализации данного правового института к конкретным задачам в той или иной области его применения. Вместе с тем это же становится некой проблемой для правоприменителей и граждан. Не существует полного перечня информации, которая относится к понятию персональных данных, что вызывает определенные коллизии норм права и сложности для людей, которые пытаются сохранить личные данные о себе, что, как отмечает А. Г. Мираев, не позволяет сделать вывод о том, какая именно информация будет относиться к персональным данным [3, с. 77].

В сложившейся ситуации наиболее предпочтительным видится вариант применения ряда ограничительных принципов, что позволит интерпретировать конкретную информацию как персональные данные. Это в свою очередь позволит пользователям и обладателям личной информации определить границы ее использования и передачи другим лицам, а также правильно применять нормы российского законодательства о защите и охране персональных данных.

Несмотря на имеющиеся пробелы и недостатки в области определения информации, относящейся к персональным данным, немаловажным остается вопрос защиты таких данных от возможных угроз в сети Интернет, поскольку все больше граждан пользуются достижениями современного общества, такими как интернет-магазины, оформление сделок и договоров онлайн, регистрируются на различных сайтах и т. д. Во многом все эти операции связаны с предоставлением персональной информации, поскольку являются идентификатором личности и позволяют вести учет пользователей, их деятельности и др.

В сфере защиты персональных данных в сети Интернет существует ряд индивидуальных угроз, среди них:

– кибератаки на серверы, хранящие такую информацию, в целях преступного завладения ею, то есть ее хищение;

– незаконная передача такой информации организациями в целях получения материальной выгоды;

– искажение информации при ее использовании;

– самовольная передача такой информации гражданами в результате правовой неграмотности и неосведомленности о последствиях совершаемых действий.

Список угроз не является исчерпывающим, однако именно они представляют наибольшую опасность для персональных данных. Разберем каждую из них отдельно.

Начнем с последней угрозы, поскольку ее решение лежит на поверхности. Практически все в повседневной жизни сталкиваются с таким простым действием, как регистрация на каком-нибудь электронном сайте для получения доступа к информации или при оформлении онлайн-заказа и др. Однако даже такой процесс требует передачи сведений о фамилии, имени, отчестве человека, в ряде случаев паспортных данных, информации о

месте жительства и т. д., что относится к персональным данным, но далеко не каждый человек задумывается об этом. И причиной этому служит низкая правовая грамотность граждан Российской Федерации, которые свободно предоставляют операторам информацию о себе.

Для предотвращения нежелательного распространения персональной информации и в дальнейшем ее хищения, искажения или неправомерной передачи другим лицам необходимо повышать уровень правовой грамотности граждан. Иными словами, требуется проводить различные мероприятия с целью знакомства с основными положениями законодательства нашей страны, в простой и доступной форме для их правильного понимания и применения. Это могут быть лекции, беседы и т. д., статьи в Интернете, вложения с разъяснениями при передаче такой информации. При чем это должно осуществляется не как возможность, а как условие передачи информации, то есть лицо, желающее передать свои персональные данные какой-либо организации, должно не просто дать согласие на обработку и использование персональных данных, а конкретно ознакомиться с данной процедурой и возможными последствиями. Реализовать это можно, например, предусмотрев обязательное время перехода к следующему этапу регистрации.

Кроме того, видится эффективным введение презумпции того, что если в соглашении с пользователем прямо не предусмотрено согласие на распространение персональных данных, то право распространения данных у оператора отсутствует (ч. 4 ст. 10.1 Закона «О персональных данных») [4].

Следует согласиться с мнением Е. Г. Дмитриевой, которая предлагает добавить требование о том, что оператор должен разместить на сайте/платформе типовую форму, позволяющую отозвать согласие на обработку и распространение персональных данных в электронном виде непосредственно на самой платформе [4].

Что же касается других угроз, то здесь их решение не является таким простым.

Рассматривая возможные кибератаки на хранилища информации с персональными данными клиентов различных организаций, важно отметить, что решение этой проблемы становится возможным только при создании надежных и действенных механизмов электронной защиты информации. Видится наиболее целесообразным привлекать государство и его возможности для решения данной проблемы, поскольку затрагиваются интересы как отдельных людей, так и всего общества в целом, а согласно основным положениям законодательства нашей страны обеспечение и защита прав и свобод человека и гражданина являются приоритетными задачами.

Рассматривая остальные угрозы, необходимо подчеркнуть, что законодателем предусмотрена различная ответственность за совершение данных правонарушений. Это применимо и в случае хищения персональных данных.

Статья 24 Федерального закона «О персональных данных» прямо определяет виды ответственности. Лица, виновные в нарушении требований закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Так, например, взлом аккаунтов электронной почты либо социальных сетей определяется как нарушение тайны переписки, за совершение которого предусмотрена уголовная ответственность:

а) наложение штрафа в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев;

б) привлечение к обязательным работам на срок до трехсот шестидесяти часов;

в) привлечение к исправительным работам сроком до одного года [5, с. 90].

Однако по общему количеству совершаемых преступлений в данной сфере, а также по имеющейся тенденции к росту их числа можно сделать вывод о низкой эффективности данных мер, несмотря на их уголовно-правовой характер. В целях повышения эффективности мер защиты в первую очередь видится ужесточение санкций за совершенные деяния. Основными правовыми нормами, охраняющими персональные данные, являются ст. 137, 140 и 272 УК РФ. На наш взгляд, целесообразно ужесточить санкцию именно за преступные деяния, указанные в ст. 137 и 272 УК РФ, а конкретно за незаконное распространение или собирание информации, а также за неправомерный доступ к ней.

В ч. 1 ст. 137 УК РФ необходимо увеличить размер штрафа до 500 тыс. руб., а также срок наказания в виде лишения свободы до 5 лет, аналогичные изменения внести и в ст. 272 УК РФ в целях обеспечения усиления уголовно-правовой охраны исследуемого института.

Также дополнительными мерами профилактики данных преступлений могут выступать:

1. Организация и проведение внешних независимых проверок по факту утечки или хищения персональных данных.

2. Создание упрощенных внесудебных механизмов защиты прав граждан в случаях неправомерного использования персональных данных. В частности, возможно создание института уполномоченного по правам человека в сфере защиты персональных данных [4].

3. Разработка систем и способов вычисления лиц, совершивших посягательства на персональные данные и др.

Что касается искажения личной информации пользователей, то здесь возможными мерами предупреждения может выступать создание системы учета и контроля баз данных, в которых хранится указанная информация, а также разработка специальных каналов передачи такой информации, в рамках которой должен быть предусмотрен механизм проверки достоверности передаваемой информации на предмет ее искажения и правомерности.

Также общим профилактическим средством может стать установление законодателем сроков хранения персональных данных, организация проверки и контроля их соблюдения. В рамках этого механизма может быть предусмотрена возможность подтверждения или изменения данных в целях продления или возобновления срока.

В рамках глобальной профилактической деятельности государства по предупреждению и пресечению правонарушений в области защиты персональных данных граждан необходимо усилить контроль за данной сферой, предусмотрев создание специальных подразделений, в функциональные обязанности которых было бы внесено данное положение, а также уделить внимание вопросу уголовной ответственности за соответствующие преступления.

В качестве решения проблемы нами предлагается ввести ряд ограничительных принципов, которые позволят интерпретировать конкретную информацию как персональные данные:

– указание на принадлежность сведений конкретному человеку;

– наличие в предоставляемых сведениях человека его биологических, социальных и документарных характеристик.

Таким образом, следует отметить, что существуют проблемы не только в области защиты персональных данных в сети Интернет, но и в таких первичных, базовых аспектах, как определение и толкование понятия «персональные данные», категории информации, относимой к таким данным, и др. Необходимы комплексный подход к решению обозначенных проблем и постепенное внедрение систем и механизмов защиты (правовых например,

ужесточение уголовно-правовой ответственности за преступления против персональных данных, технических, направленных на устранение имеющихся угроз и законодательных пробелов). Особое внимание следует уделить государственному контролю и надзору в данной сфере.

СПИСОК ИСТОЧНИКОВ

1. Важорова М. А. История возникновения и становления института персональных данных // Государство и право: теория и практика : материалы междунар. науч. конф. Челябинск, 2011. С. 33–38.
2. Громкие случаи утечек персональных данных в России в 2019–2020 годах. URL: https://ria.ru/20200623/1573379104.html (дата обращения: 26.09.2022).
3. Мираев А. Г. Понятие персональных данных в Российской Федерации и Европейском союзе // Юридическая наука. 2019. № 5. С. 76–82.
4. Дмитриева Е. Г. Проблемы защиты персональных данных в цифровом мире и пути их решения // Право и бизнес. 2021. № 3. С. 18–23.
5. Давыдова О. Б. Защита персональных данных // Вестник науки и образования. 2018. № 6 (42). С. 89–90.

REFERENCES

1. Vazhorova M.A. History of the emergence and formation of the Institute of personal data. In: *Gosudarstvo i pravo: teoriya i praktika: materialy Mezhdunar. nauch. konf.* [State and law: theory and practice: proceedings of the International scientific conference]. Chelyabinsk, 2011. Pp. 33–38. (In Russ.).
2. *Gromkie sluchai utechek personal'nykh dannykh v Rossii v 2019–2020 godakh* [High-profile cases of personal data leaks in Russia in 2019–2020]. Available at: https://ria.ru/20200623/1573379104.html (accessed September 26, 2022).
3. Miraev A.G. The concept of personal data in the Russian Federation and the European Union. *Yuridicheskaya nauka = Legal Science*, 2019, no. 5, pp. 76–82. (In Russ.).
4. Dmitrieva E.G. Problems of personal data protection in the digital world and ways to solve them. *Pravo i biznes = Law and Business*, 2021, no. 3, pp. 18–23. (In Russ.).
5. Davydova O.B. Protection of personal data. *Vestnik nauki i obrazovaniya = Bulletin of Science and Education*, 2018, no. 6 (42), pp. 89–90. (In Russ.).

СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

ТАТЬЯНА ВЛАДИМИРОВНА КОРНИЛОВА – кандидат психологических наук, начальник отделения организации и координации научно-исследовательской деятельности и международного сотрудничества организационно-научного отдела Вологодского института права и экономики ФСИН России, Вологда, Россия, tatyana_vladi21@mail.ru, https://orcid.org/0000-0003-1978-9294

ЕГОР ОЛЕГОВИЧ ЛАПЕНКОВ – курсант 5 курса юридического факультета Вологодского института права и экономики ФСИН России, Вологда, Россия, egorlapenkov@yandex.ru, https://orcid.org/0000-0001-8754-2264

TAT'YANA V. KORNILOVA – Candidate of Sciences (Psychology), Head of the Department of Organization and Coordination of Research Activities and International Cooperation of the Organizational and Research Department of the VILE of the FPS of Russia, Vologda, Russia, tatyana_vladi21@mail.ru, https://orcid.org/0000-0003-1978-9294

EGOR O. LAPENKOV – 5th year cadet of the Law Faculty of the VILE of the FPS of Russia, Vologda, Russia, egorlapenkov@yandex.ru, https://orcid.org/0000-0001-8754-2264

Статья поступила 23.12.2023