УДК 34.096
DOI: 10.25688/2076-9113.2023.49.1.04

Л. Н. Бокова
Московский государственный областной педагогический университет,
Москва, Российская Федерация
E-mail: LN.Bokova@mgou.ru

ПРАВОВЫЕ ВОПРОСЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ГРАЖДАН В ЦИФРОВОМ ПРОСТРАНСТВЕ

Аннотация. В статье показано, что в условиях цифровизации важное значение для защиты персональных данных играют своевременные законодательные меры. Раскрываются тенденции, влияющие на ослабление защиты персональных данных. Подчеркивается, что защита персональных данных осуществляется через внесение соответствующих изменений в законодательство РФ. Обоснована целесообразность принятия норм, направленных на внедрение новых технологий хранения и обработки данных, в том числе персональных и обеспечивающих их защиту, а также контроль. Автор раскрывает важность реализации правовой защиты данных, отсутствие которой может иметь негативные последствия, как для субъекта персональных данных, так и для государства в целом. Сделан вывод о необходимости усиления ответственности за нарушения, связанных с обеспечением защиты данных. Широкая трактовка понятия «персональные данные» не позволяет зачастую однозначно определить, какая именно информация к ним относится, поэтому так важно найти баланс между нормами закона и практикой его применения, исключив любые злоупотребления.

Ключевые слова: персональные данные; цифровое пространство; законодательство; информационные технологии; права человека.

UDC 34.096
DOI: 10.25688/2076-9113.2023.49.1.04

L. N. Bokova
Moscow State Regional Pedagogical University,
Moscow, Russian Federation
E-mail: LN.Bokova@mgou.ru

LEGAL ISSUES OF PROTECTION OF PERSONAL DATA OF CITIZENS IN THE DIGITAL SPACE

Abstract. The article shows that in the context of digitalization, timely legislative measures play an important role in the protection of personal data. The trends affecting the weakening of personal data protection are revealed. It is emphasized that the protection of personal data is carried out through the introduction of appropriate changes to the legislation

of the Russian Federation. The expediency of adopting norms aimed at the introduction of new technologies for storing and processing data, including personal data and ensuring their protection, as well as control, is substantiated. The author reveals the importance of implementing legal data protection, the absence of which can have negative consequences both for the subject of personal data and for the state as a whole. It is concluded that it is necessary to strengthen responsibility for violations related to data protection. A broad interpretation of the concept of "personal data" often does not allow to unambiguously determine what kind of information relates to them, therefore it is so important to find a balance between the norms of the law and the practice of its application, eliminating any abuse.

Keywords: personal data; digital space; legislation; information technology; human rights.

Введение

Современный процесс повсеместной цифровизации существенно влияет на многие базовые параметры правового регулирования, обусловливает высокую динамику законотворчества, актуализирует исследование вопросов защиты прав и свобод человека в цифровой среде. Повышение роли информации, а также распространение все новых технологий ее передачи повышают актуальность проблемы защиты персональных данных. Все чаще пользователи цифровой среды сталкиваются с кражей и несанкционированным распространением их персональных данных в различных сферах, что влечет за собой как моральный, так и материальный вред.

Очевидно, что такая проблема широко распространена в незащищенных интернет-сетях, где накапливается огромный массив личной информации граждан из многочисленных баз данных. Негативную роль играют различного рода утечки персональных данных, как случайные, так и ставшие результатом действий злоумышленников.

Пользователи цифровых ресурсов в сети Интернет неизбежно оставляют цифровой след в виде паспортных данных, контактной информации, реквизитов банковских счетов, электронных транспортных билетов и прочих сведений. Из-за утечек такой информации, имеющей конфиденциальный характер, создаются цифровые портреты граждан, которые затем могут использоваться злоумышленниками[1].

Проблему, связанную с использованием и защитой персональных данных, обострила внешнеполитическая ситуация, которая повлекла ряд ограничений доступа к популярным интернет-платформам на территории России. Для обхода блокировок особый интерес граждане проявляют к использованию технологий зашифрованного подключения к сети — VPN-сервисам. Однако такие сервисы нередко сами являются инструментом хищения персональных данных пользователей. VPN-сервисы могут без разрешения получать конфиденциальную

[1] Заявлено в Роскомнадзоре // Коммерсантъ. 2022. 14 сентября.

информацию и распространять ее в незащищенную цифровую среду. Кроме того, существует риск при загрузке подобного приложения установить вредоносную программу, которая будет передавать личные данные третьим лицам. При этом сам владелец устройства может долгое время не подозревать, что его персональные данные похищены.

Прежде чем говорить о применении VPN-сервисов в государственных структурах и связанных с этим рисках, следует изучить риски утечек наиболее чувствительных данных, включая конфиденциальную информацию. Способы хищения данных также прогрессируют, как и методы, обеспечивающие их защиту. Этому способствуют не только новые технологические решения, но и методы социальной инженерии. Они позволяют получить информацию от граждан, которые в итоге добровольно сообщают свои данные злоумышленникам. При помощи этих сведений можно легко похитить деньги, другие данные или нанести иной серьезный ущерб гражданину. Также злоумышленники часто распространяют фишинговые рассылки — это своего рода ссылки-приманки, которые подстраиваются под определенный информационный повод, основаны на личных предпочтениях потенциальной жертвы, используют ее потребности и интересы. Например, в условиях специальной военной операции и частичной мобилизации было отмечено несколько случаев, когда в стране распространялось вредоносное программное обеспечение под видом электронных повесток и информации о сборе гуманитарной помощи[2].

В целом фишинговое мошенничество представляет собой продвинутый с технической точки зрения и достаточно распространенный прием для выманивания данных пользователей. Наиболее часто угроза представлена на различных интернет-площадках, в социальных сетях и мессенджерах, электронной почте, поисковых системах, программных приложениях, при использовании устаревшего антивирусного программного обеспечения. В этих условиях право как регулятор общественных отношений должно своевременно реагировать на новые возникающие угрозы и обеспечивать эффективную защиту прав и законных интересов всех добросовестных пользователей сети Интернет, число которых в условиях перехода к новому технологическому укладу будет только увеличиваться.

Методы

Методологической основой исследования стал формально-юридический метод, акцентирующий внимание на содержании норм права, направленных на защиту персональных данных. Также были использованы общенаучные методы анализа и синтеза.

[2] Лаборатория Касперского» сообщила о вредоносном ПО под видом повесток // РБК. 2022. 6 октября.

Основное исследование

Проблема незащищенности персональных данных возникает из-за возрастающей скорости процессов цифровизации, допускаемой в отдельных случаях излишней спешки и, как следствие, неприятие многих социально-технологических новаций обществом, которое воспринимает их как риски, что порой вполне справедливо.

Развитие информационного общества и связанных с ним технологий представляется объективной реальностью, которая в то же время требует взвешенного стратегического подхода [1, с. 42]. В Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы отмечена необходимость внедрения новых технологий, в том числе направленных на защиту данных. Но такое внедрение ни в коем случае не должно нарушать основополагающие права человека.

Несоблюдение разумного баланса и необходимой осторожности в процессе цифровизации сферы государственных услуг и механизмов получения информации может привести к нарушению прав граждан, предусмотренных Конституцией РФ и, как следствие, вызвать серьезные социальные риски. Из этого следует, что устанавливаемые правом система и принципы информационной безопасности должны своевременно меняться, качественно совершенствоваться, а юридическая ответственность за утечку данных должна быть соразмерной ущербу.

Руководствуясь Указом Президента Российской Федерации от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», Правительство Российской Федерации утвердило новое положение о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе и о структурном подразделении, обеспечивающем информационную безопасность. В данном положении определены новые трудовые компетенции, которые позволят обеспечить создание устойчивой инфраструктуры, которая может снизить риск утечки данных.

Важно отметить, что успешная деятельность всех структур государства основана на том доверии, которое испытывают граждане по отношению к власти и ее действиям. Утечки персональных данных подрывают доверие граждан к деятельности государства по регулированию общественных отношений. Согласно последним исследованиям, граждане не уверены в том, что они способны самостоятельно защитить свои данные. В 2021 году в Роскомнадзор поступило более 38 тыс. жалоб граждан на неправомерную обработку их данных. В основном жалуются на следующие категории операторов персональных данных: интернет-сайты; организации, осуществляющие управление жилым фондом; банки и иные организации, связанные с финансовой сферой. Эксперты отмечают, что защита должна быть обеспечена только за счет объединения усилий государства и компаний. Вопросы оборота и защиты персональных

данных граждан являются одним из государственных приоритетов в России. Статья 71 Конституции Российской Федерации предусматривает обеспечение безопасности личности, общества и государства при разделении, применении информационных технологий и обороте цифровых данных.

Президент Российской Федерации В. В. Путин инициировал процесс создания государственной системы защиты информации: «Нужно укреплять оборону отечественного цифрового пространства — здесь не должно быть слабых мест. Принципиально важно свести на нет риски утечек конфиденциальной информации и персональных данных граждан, в том числе за счет более строгого контроля правил использования служебной техники, коммуникаций, связи»[3].

В фокусе внимания остается защита прав и интересов граждан при нарушениях и незаконных действиях, которые связаны с использованием персональных данных. В этих целях в 2021 году был создан Центр правовой помощи гражданам в цифровой среде. В 2022 году большая часть обращений, поступивших в центр, касались обработки личной информации без согласия человека, использования мошенниками конфиденциальных сведений и неправомерного задействования персональных данных в рекламных целях.

Как следует из доклада Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека «Цифровая трансформация и защита прав граждан в цифровом пространстве», который был подготовлен в 2021 году, персональные данные должны обрабатываться законно, справедливо и прозрачно[4].

Федеральное законодательство об использовании цифровых и иных новых технологий, в том числе и о защите персональных данных, все время развивается и совершенствуется, в него вносятся необходимые изменения и дополнения, направленные на повышение эффективности защиты прав граждан [3, с. 32]. В 2020 году федеральным законодательством была предусмотрена возможность граждан самостоятельно предпринимать действия по ограничению оборота личных данных, без соответствующего согласия. Также граждане получили право обратиться к оператору персональных данных с требованием удалить их данные из общего доступа без каких-либо дополнительных условий.

Подверглись изменению и требования к операторам, которые обязаны информировать Роскомнадзор об осуществлении любой обработки персональных данных граждан. Кроме того, оператор должен обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

---

[3] В. В. Путин 20 мая 2022 года на заседании Совета Безопасности [Электронный ресурс] // Президент России: официальный сайт. URL: http://www.kremlin.ru/events/president/news/68451

[4] URL: https://ifap.ru/pr/2021/n211213a.pdf

Среди наиболее актуальных проблем в области соблюдения законодательства остается невыполнение требований Федерального закона от 2 декабря 2019 года № 405-ФЗ, касающегося локализации данных граждан на территории Российской Федерации. Кодексом Российской Федерации об административных правонарушениях предусмотрена ответственность оператора за невыполнение данного требования. На практике это означает, что при сборе персональных данных оператор обеспечивает обработку данных с использованием баз данных, находящихся на территории Российской Федерации.

Для соблюдения законодательства о локализации данных ужесточена трансграничная обработка персональных данных.

С 1 марта 2023 года оператор персональных данных обязан уведомлять Роскомнадзор о трансграничной обработке персональных данных. При этом у Роскомнадзора появились полномочия по запрету или ограничению предоставления персональных данных иностранным организациям и физическим лицам, а также в случае необходимости запрашивать у иностранных обработчиков персональных данных сведения об их защите.

Принятые за последние годы важные изменения законодательных норм не охватывают всех проблем, существующих в сфере защиты персональных данных [2, с. 46]. К числу таких проблем относится избыточность требований к чрезмерной детализации персональных данных, которые в целом могут быть не нужны для оказания соответствующей услуги[5].

Для улучшения ситуации с защищенностью персональных данных в России представители Института конкурентной политики и регулирования рынков НИУ ВШЭ рекомендуют усилить ответственность для виновников, расширить практику использования независимого аудита и страхования рисков. Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации подготовлен проект федерального закона об оборотных штрафах за утечку данных[6]. Проектом предполагается пересмотреть штрафы и ввести персональную ответственность за утечку данных.

Наряду с ужесточением ответственности за цифровые преступления рассматриваются механизмы страхования рисков от утечек данных, которые в том числе позволят компенсировать ущерб пострадавшим гражданам. Минцифры России предлагает меры, частично аналогичные оборотным штрафам. Однако при этом не уточняется, станет ли так называемое киберстрахование обязательным[7].

В свою очередь, представители бизнеса полагают иначе. По словам руководителя информационной безопасности компании «Инфобип» Д. Лукаша, «прежде чем вводить оборотные штрафы, стоит поработать над прозрачностью

---

[5] Защита персональных данных: обзор последних нововведений // СПС «Гарант». 16 сентября 2021 года.

[6] См.: СПС «Консультант.Плюс».

[7] Киберстраховой случай // Коммерсантъ. 2022. 7 ноября.

законодательства о персональных данных, простотой его применения, неотвратимостью наказания, гражданско-правовыми возможностями субъекта персональных данных»[8].

Вывод

Защита персональных данных в условиях цифрового общества представляется важной проблемой, требующей соответствующего правового регулирования, непрерывного совершенствования действующего законодательства сообразно новым появляющимся рискам.

Одним из основных инструментов государства в вопросе усиления защиты прав граждан — субъектов персональных данных — является постоянное совершенствование отраслевой нормативной базы и мониторинг его практической эффективности. Особенно важным это представляется при обострении внешних угроз информационной безопасности, а также на проявляющемся фоне неготовности технологий к современным кибератакам.

Тенденции последних лет показывают, что нарушение российского законодательства в области персональных данных обходится дешевле, чем его исполнение. Несмотря на значительные изменения законодательства, ситуация принципиально не меняется. В этих условиях увеличение размера штрафа является одним из направлений для внесения изменений в законодательство.

Литература

1. Корчагина Т. М., Николаев А. И. Российский конституционализм в условиях новой информационной реальности // Вестник МГПУ. Серия «Юридические науки». 2020. № 7. С. 42–47.

2. Николаев А. И. Вопросы цифровизации права в современной юридической доктрине // Вестник МГПУ. Серия «Юридические науки». 2019. № 4. С. 44–48.

3. Пашенцев Д. А. Основные направления и особенности развития законодательства в условиях цифровизации и перехода к новому технологическому укладу // Вестник МГПУ. Серия «Юридические науки». 2021. № 3. С. 31–39.

Literatura

1. Korchagina T. M., Nikolaev A. I. Rossijskij konstitucionalizm v usloviyax novoj informacionnoj real`nosti // Vestnik MGPU. Seriya «Yuridicheskie nauki». 2020. № 7. S. 42–47.

2. Nikolaev A. I. Voprosy` cifrovizacii prava v sovremennoj yuridicheskoj doktrine // Vestnik MGPU. Seriya «Yuridicheskie nauki». 2019. № 4. S. 44–48.

[8] Устранить течь: вступают в силу масштабные изменения о персональных данных» // Известия. 2022. 31 августа.

3. Pashencev D. A. Osnovny`e napravleniya i osobennosti razvitiya zakonodatel`stva v usloviyax cifrovizacii i perexoda k novomu texnologicheskomu ukladu // Vestnik MGPU. Seriya «Yuridicheskie nauki». 2021. № 3. S. 31–39.

Статья поступила в редакцию: 04.12.2022;
одобрена после рецензирования: 20.12.2022;
принята к публикации: 22.12.2022.

The article was submitted: 04.12.2022;
approved after reviewing: 20.12.2022;
accepted for publication: 22.12.2022.