Юридические исследования
Правильная ссылка на статью:
Марушина В.А., Чугунов Д.К. К вопросу о государственной политике в сфере защиты персональных данных // Юридические исследования. 2024. № 5. DOI: 10.25136/2409-7136.2024.5.70842 EDN: LTSVRE URL: https://nbpublish.com/library_read_article.php?id=70842

К вопросу о государственной политике в сфере защиты персональных данных

Марушина Валентина Андреевна

ORCID: 0009-0000-1646-1539

магистр; юридический институт; Российский университет дружбы народов имени Патриса Лумумбы

111555, Россия, г. Москва, ул. Сталеваров, 10

Valelenziya82@yandex.ru

Чугунов Даниил Константинович

ORCID: 0000-0003-4506-8095

кандидат юридических наук

ассистент; юридический институт; Российский университет дружбы народов имени Патриса Лумумбы

119607, Россия, г. Москва, ул. Удальцова, 87к1

daniilchugunov@icloud.com

Статья из рубрики "Трансформация правовых систем"

DOI:

10.25136/2409-7136.2024.5.70842

EDN:

LTSVRE

Дата направления статьи в редакцию:

24-05-2024

Аннотация: Статья посвящена актуальным изменениям, касающимся совершенствования законодательства в области защиты персональных данных. В рамках исследуемого вопроса авторами проведен анализ ряда законодательных и подзаконных инициатив с целью оценки необходимости принятия соответствующих нововведений и их последующей реализации в рамках правоприменения. Авторами детально изучены положения проектов правовых актов, выделены вопросы, требующие дополнительной

конкретизации. В работе рассматриваются меры государственной политики РФ, связанные с: 1) предоставлением дополнительных полномочий силовым ведомствам в части доступа к информационным системам; 2) установлением требований к хранению информации и ее передачи; 3) ужесточением ответственности за утечку персональных данных; 4) дополнительными способами обеспечения безопасности российских информационных систем, уменьшением степени их зависимости от иностранных сервисов. В ходе рассмотрения данного вопроса авторами были использованы общенаучные и частнонаучные методы, в частности, такие как анализ, синтез, правовое прогнозирование и другие. Новизна работы заключается в исследовании тех изменений, которые планируется внести в нормативные правовые акты в ближайшем будущем, ранее подобные положения подробно не освещались в юридической науке. В результате проведенного исследования сделаны выводы о грамотном подходе государственной власти к модернизации нормативного регулирования в области защиты персональных данных в условиях серьезной необходимости обеспечения наиболее качественной защиты персональных данных, при этом авторами отмечены некоторые положения, требующие доработки со стороны законотворческих органов ввиду того, что на данный момент они либо носят абстрактный характер, либо вступают в противоречие с уже действующими правовыми нормами. Предполагается, что в последующем, после введения указанных изменений, можно будет оценить их эффективность уже в рамках правоприменения.

Ключевые слова:

персональные данные, государство, защита, информационные системы, силовые структуры, санкции, информация, российские сервисы, мошенничество, ответственность

Введение

Персональные данные, являясь объектом правового регулирования, представляют собой, в соответствии со статьей 3 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных», любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу, [1] и нуждаются в грамотном механизме обеспечения их защиты, который будет способствовать сохранению конфиденциальности информации и предотвращению их распространения третьим лицам. В настоящее время в условиях контрсанкционной политики Российской Федерации (далее – РФ) органы государственной власти уделяют отдельное внимание вопросам защиты персональных данных ввиду необходимости усовершенствования процедур их обработки, в том числе использования, передачи и т.д. Актуальность исследования обусловлена, во-первых, увеличением количества хакерских атак на российские интернет-сайты и информационные системы со стороны недружественных государств, а также ростом числа случаев мошенничества и утечки персональных данных, а во-вторых, как следствие, заинтересованностью как государства, так и юридических и физических лиц в обеспечении защиты информации, которая в процессе усложнения средств ее обработки в информационном пространстве в сети Интернет становится более уязвимой.

Основная часть

1. Государство, преследуя цель обеспечения эффективной защиты отдельной категории лиц наиболее значимых персональных данных, предусматривая особый порядок их обработки, выступило с инициативой, связанной с предоставлением силовым структурам

доступа к государственным и иным информационным системам, содержащим данные об отдельной категории лиц – сотрудников таких ведомств. Такой законопроект был внесен в Государственную Думу РФ в 2023, но на данный момент прошел только первое чтение. Обусловлено это, в том числе, тем, что предлагаемый в первоначальной редакции текст требует внесения соответствующих поправок.

Поскольку данное нововведение связано с доступом силовых структур не только к государственным, но и частным сервисам, разрабатываемым компаниями, оно окажет значительное влияние на бизнес-сектор. При этом, несмотря на значимость цели введения соответствующих изменений, предлагаемая инициатива не была поддержана представителями бизнеса. Объясняется это тем, что информационные системы, в которых крупные компании хранят данные о своих клиентах (пользователях), зачастую связаны между собой. Такая взаимосвязь и, следовательно, взаимодействие может выражаться в виде обмена данными, распределенного выполнения поисковых запросов и согласованного изменения базы данных [3]. Соответственно, по мнению представителей бизнес-сектора, установление особого порядка, в рамках которого сотрудникам силовых ведомств будет предоставлен прямой доступ к таким информационным системам, будет нарушать целостность их функционирования и создаст для бизнеса угрозу нарушения других законов [14]. Исходя из положений нынешней редакции, предполагается, что ведомства смогут получить удаленный доступ к персональным данным в той или иной информационной системе, однако в таких ситуациях возникает риск непередачи данных (вносимых представителями силовых структур изменений) между информационными системами, который приведет к их несвязанности, а значит, повлечет за собой угрозу их бесперебойной работы. Стоит также отметить, что возможность удаленного доступа в определенной степени повышает риски утечки персональных данных, потому что такая информация будет раскрываться большому кругу технических специалистов, у которых есть доступ к базам данных и которые будут видеть вносимые изменения.

Во избежание вышеупомянутых рисков в настоящий момент рассматривается возможность достижения поставленной цели посредством установления несколько измененного механизма, в рамках которого, в соответствии с Постановлением Правительства РФ, у силовых структур появится доступ к не ко всей информационной системе, а к отдельным «полям» информационных баз данных. При этом представляется грамотным сделать акцент на том факте, что с технической стороны реализация данной процедуры потребует дополнительного комплекса действий и серьезных технических и финансовых затрат, что также отразится на оперативности процесса введения рассматриваемого механизма.

В частности, кредитные организации также имеют определенные опасения по поводу того, что в случае принятия данного закона информация о сотрудниках Минобороны, ФСБ, ФСО и т.д., у которых открыты банковские счета, может подлежать редактированию или даже удалению со стороны спецслужб, что может привести к коллизии предлагаемых к принятию изменений и требований, установленных Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 07.08.2001 N 115-ФЗ и Федеральным законом «О банках и банковской деятельности» от 02.12.1990 N 395-1, поскольку текст законопроекта не предполагает внесения изменений в указанные акты. Помимо этого, возникает вопрос о возможности обеспечения исполнения банковской тайны в случаях, когда силовые структуры смогут получать доступ к персональным данным, а также осуществлять их обработку. Так, в рамках внесения поправок в рассматриваемый законопроект, на наш взгляд, необходимо учесть соответствующие положения,

связанные с банковской деятельностью и предусмотреть способ, позволяющий преодолеть упомянутые коллизии. Схожие противоречия могут возникнуть в сфере оказания услуг связи.

Учитывая особенности правового регулирования сферы защиты персональных данных [4], полагаем, что стоит отметить следующее: законопроектом предлагается обязать операторов информационных систем выявлять сведения о ведомственной принадлежности сотрудников [10] силовых структур и информировать об этом соответствующие ведомства, однако, что конкретно подразумевается под такими сведениями, не конкретизируется. В имеющейся в настоящий момент редакции законопроекта не установлено, какую именно информацию необходимо сообщать в ведомства, является ли перечень таких данных закрытым и т.д., что в дальнейшем может послужить причиной возникновения правовой неопределенности в данном вопросе. Так, из вышеизложенного следует, что, оценивая важность предлагаемых изменений, в рамках установления особого порядка обработки персональных данных сотрудников силовых структур, представляется верным внести дополнительные коррективы во избежание коллизий или пробелов в правовом регулировании рассматриваемой сферы.

2. Отдельное внимание уделим вопросу хранения персональных данных организаторами распространения информации (далее – ОРИ) и их передачи по требованию силовых служб. После принятия пакета антитеррористических поправок («закон Яровой») ОРИ обязаны хранить информацию о фактах приема, передачи, доставки <…> сообщений пользователей [8], а также информацию об этих пользователях в течение одного года. Перечень информации, подлежащей хранению и предоставлению силовым ведомствам, закреплен в Постановлении Правительства РФ от 23.09.2020 N 1526 и с недавнего времени включает в себя не только данные о регистрационных данных пользователя, но и о его геолокации и средстве платежа. Таким образом, с одной стороны, появляются определенные дополнительные средства «контроля» за действиями пользователей, с другой – расширение перечня сведений, подлежащих хранению, связано с необходимостью повышения эффективности оперативно-розыскной деятельности для обеспечения общественной безопасности. С той же целью планируется дополнить перечень данными о сетевых адресах и портах пользователя, сетевых адресах и портах коммуникационного интернет-сервиса [11]. При этом, стоит отметить, что в законодательстве отсутствует определение понятия «сетевой порт», в то время как Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» содержит определение «сетевого адреса», ввиду чего использование данного понятия в подзаконном акте не вызывает дополнительных вопросов. В целом, благодаря доступу к сетевым адресам и портам, спецслужбы смогут выявить по IP-адресу и порту пользователя, разместившего противоправные сведения или совершившего иные противоправные деяния, в особенности в условиях санкционного давления со стороны недружественных стран, и защите персональных данных пользователей от актов мошенничества в сети. Отметим, что, на наш взгляд, данные изменения положительно повлияют на статистику раскрываемости преступлений и в определенной степени облегчат поиск преступников.

3. Ввиду участившихся случаев утечки персональных данных в рамках анализа принимаемых мер государственной политики акцентируем внимание на изменениях ряда положений, касающихся ответственности за нарушение порядка обработки персональных данных. На данный момент в законодательстве установлен максимальный размер штрафа за утечку персональных данных для юридических лиц, который составляет 100 тысяч рублей, однако санкции, установленные в ч.1 ст.13.11 Кодекса РФ об административных

правонарушениях (далее – КоАП РФ), не учитывают серьезность последствий, которые повлекли за собой такие утечки, при этом наступившие последствия могут быть совершенно разные, что в целом может нарушать принцип соразмерности наказания за совершенное правонарушение, следовательно, положение требует дополнительной конкретизации.

В связи с вышеизложенным отметим, что необходимость установить градацию ответственности в зависимости от объема так называемой «утекшей» информации уже обсуждается на законодательном уровне. Помимо этого, за повторные нарушения юридическими лицами требований по обработке персональных данных, повлекших за собой утечку, государство планирует ввести оборотные штрафы, составляющие не фиксированную для всех сумму или установленный диапазон, а выражающиеся в процентах совокупного размера суммы выручки, полученной от реализации всех товаров (работ, услуг), за календарный год, предшествующий году, в котором было выявлено административное правонарушение [11]. Безусловно, предлагаемые изменения в части назначения административного наказания действительно являются достаточно жесткими, однако, мы полагаем, что установление таких штрафов окажет превентивное воздействие на операторов обработки персональных данных. Компании, не желающие терять значительную часть своего дохода, будут более ответственно следить за соблюдением требований в области персональных данных, что будет способствовать уменьшению количества случаев утечки.

Вполне логично, что изменения, касающиеся введения оборотных штрафов, вызвали неоднозначное мнение среди представителей бизнес-сектора. К примеру, Сбербанк на данный момент поддерживает идею налагать такие штрафы лишь в исключительных случаях, аргументируя свою позицию тем, что предлагаемые нововведения не дифференцирует объективную сторону состава административного правонарушения по принципу характера действий оператора данных [15]. Другие банки же полагают, что введение оборотных штрафов в размере до 500 млн руб. необоснованно. Стоит отметить, что рассматриваемая мера, в случае ее принятия, с одной стороны, может способствовать достижению поставленной законодателем цели: столь серьезные санкции будут мотивировать организации обеспечивать надлежащую обработку персональных данных, что значительно уменьшит вероятность их утечки, с другой – негативно сказаться на экономической деятельности субъектов малого и среднего бизнеса, для которых уплата такого штрафа может ставить под угрозу их дальнейшую экономическую активности и существование в целом.

4. Наконец, целесообразно выделить еще одну меру государственной политики – установление требования о переходе на российские средства авторизации для обеспечения надлежащей степени безопасности в условиях противодействия международным санкциям. Со вступлением в силу Федерального закона от 31.07.2023 г. № 406-ФЗ, вносящего изменения в Федеральный закон от 27 июля 2006 года N 149-ФЗ «Об информации, информационных технологиях и о защите информации», для доступа к информации, размещенной на сайте, принадлежащем российскому юридическому или физическому лицу, необходимо пройти авторизацию одним из установленных законом способов. К ним относится, в частности, авторизация по номеру мобильного телефона или через единую систему идентификации и аутентификации. По словам депутата Государственной Думы РФ Антона Горелкина, целью таких нововведений является снижение зависимости российского сегмента интернета от зарубежных программных решений. Данное требование представляется крайне значимым и обусловлено, прежде всего, необходимостью защиты данных авторизированных пользователей от действий,

совершаемых со стороны недружественных государств, направленных на подрыв информационной системы РФ. Вместе с тем следует, что подобные изменения потребуют от компаний значительных финансовых затрат, однако уже обсуждается вопрос о стимулировании бизнес-сектора осуществить данную процедуру. Так, Правительство РФ рассматривает возможность предоставления льготных кредитов для перехода организаций на российский софт с целью уменьшить издержки компаний при соблюдении возложенной на них государством обязанности, и ответственность за ее несоблюдение на данный момент не установлена. Таким образом, бизнесу предоставляется возможность для реализации положений законодательства, однако в дальнейшем, введение таких норм вполне возможно. Важный акцент необходимо сделать на схожесть публичных и частных интересов в рассматриваемом вопросе, поскольку как государство, так и частные компании в своей деятельности стремятся обеспечить надлежащую защиту персональных данных. А когда совпадают интересы бизнеса и государства, особенно в условиях санкционного давления, принятие необходимых изменений представляется вполне реализуемым шагом.

Заключение

Таким образом, подводя итог всему вышесказанному, стоит отметить следующие выводы.

1. Государство стремится выработать новые механизмы для защиты наиболее значимых персональных данных, отдельное внимание в рамках которых уделяется порядку доступа силовых структур к данным своих сотрудников; при этом, оценивая целесообразность таких нововведений, отмечается, что их реализация потребует комплексного технического сопровождения. В рамках предлагаемых нововведений в ходе анализа конкретных правовых норм отмечены некоторые аспекты, требующие дополнительной доработки во избежание возникновения коллизий и пробелов.

2. Расширение перечня информации, подлежащей хранению и передаче (по запросу) силовым ведомствам, оказывает положительное влияние для содействия оперативным службам в пресечении преступных деяний, соответственно, полагаем, что данное изменение является целесообразным.

3. Ужесточение ответственности за утечку персональных данных, в том числе введение оборотных штрафов, представляя собой меру превентивного воздействия на компании, которая должна способствовать повышению качества защиты организациями данных своих клиентов, является вынужденным шагом со стороны государства, способствующим усилению контроля организациями процессов обработки персональных данных. Однако, на наш взгляд, необходимо при этом учитывать возможности не только крупных компаний, но и представителей среднего и малого бизнеса, для которых выплата таких сумм штрафов может поставить под угрозу деятельность компании в целом.

4. В условиях санкционного давления государство заинтересовано в обеспечении наиболее эффективной защиты персональных данных, а также функционировании российских информационных систем без привязки к иностранным сервисам, для чего принимает соответствующие меры. А благодаря тому, что интересы представителей бизнеса в данном вопросе совпадают с государственными, реализация данного механизма, предполагается, не повлечет дополнительных противоречий и сложностей.

Оценивая государственную политику РФ в области защиты персональных данных на современном этапе, подчеркнем, что выбран правильный вектор развития, предлагаемые меры представляются вполне целесообразными, однако ряд из них необходимо более детально проработать для того, чтобы вступившие изменения максимально четко и

непротиворечиво встроились в существующую систему правового регулирования. Предполагается, что в последующем, после вступления в силу данных нововведений, можно будет оценить их эффективность уже в рамках правоприменения.

Библиография

1. Алямкин С. Н. Персональные данные как объект правового регулирования: понятие и способы защиты // Мир науки и образования. 2016. №4 (8). – URL: https://amnko.ru/index.php/russian/journals/ (дата обращения: 19.05.2024).
2. Белая К.В. К вопросу о понятии и правовом регулировании банковской тайны // Скиф. 2019. №4 (32). – URL: https://sciff.ru/arhiv/vypusk-4-32-aprel-2019/?ysclid=lwyuhndsca49258301 (дата обращения: 20.05.2024).
3. Гнедков А.В., Нищик А.В. Особенности распространения персональных данных в последней редакции законодательства о персональных данных // Научно-методическое обеспечение оценки качества образования. 2022. №1 (15). – URL: http://www.xn--23-mlclgj2f.xn--p1ai/docs/rip/2022/nmg_15.pdf?ysclid=lx02e6sdv525955833 (дата обращения: 12.05.2024).
4. Ендольцева Е. В., Ендольцева Ю. В. Механизм противодействия бесконтрольному распространению персональных данных, способствующему совершению преступных посягательств на права и законные интересы субъектов персональных данных // Вестник УЮИ. 2023. №3 (101). URL: URL: https://vestnik-uyi.editorum.ru/ru/nauka/issue/4526/view (дата обращения: 19.05.2024).
5. Канашевский В. А. Юридические проблемы использования российскими банками облачных услуг зарубежных провайдеров // Lex Russica. 2019. №3 (148). URL: https://crimescience.ru/wp-content/uploads/2017/05/LEX-Russica_3_2019.pdf (дата обращения: 20.05.2024).
6. Кузьмин Юрий Анатольевич Кража персональных данных (криминологический аспект) // Oeconomia et Jus. 2020. №3. – URL: https://oecomia-et-jus.ru/archive/year-2020/number-3/ (дата обращения: 15.05.2024).
7. Семерханов И. А., Муромцев Д. И. Интеграция информационных систем на основе технологии связанных данных // Научно-технический вестник информационных технологий, механики и оптики. 2013. №5 (87). – URL: https://ntv.ifmo.ru/ru/publications/2013/publications_2013.htm?ysclid=lwyuix0l4e896249375 (дата обращения: 12.05.2024).
8. Синкевич Е. Е. Правовые аспекты реализации права гражданина Российской Федерации о хранении и распространении персональных данных в условиях общественного развития и мировой глобализации // Среднерусский вестник общественных наук. 2015. №6. – URL: http://orelvestnik.ru/arhiv-nomerov/ (дата обращения: 24.05.2024).
9. Такидзе Д. Т. Защита персональных данных в России // Вестник магистратуры. 2021. №5-4 (116). – URL: https://magisterjournal.ru/numbers.htm?ysclid=lwyujuxjob306028265 (дата обращения: 20.05.2024).
10. Трофимова И. А. Административная ответственность за нарушение правил обработки и хранения персональных данных // Закон и право. 2018. №9. – URL: http://www.unity-dana.ru/magazines/zakon-i-pravo/zhurnal-zakon-i-pravo-09-2018-/ (дата обращения: 21.05.2024)

Результаты процедуры рецензирования статьи

Рецензия скрыта по просьбе автора