

УДК 349
ББК 67.404.9

ТЕРЕШИН Марк Витальевич,
магистрант Департамента правового регулирования
экономической деятельности Финансового университета
при Правительстве Российской Федерации
e-mail: mtereshin@outlook.com

Научный руководитель:
РАХМАТУЛИНА Римма Шамильевна,
кандидат юридических наук, доцент
e-mail: rimin@mail.ru

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РФ И ЕС В КОНТЕКСТЕ ВСТУПЛЕНИЯ В СИЛУ ОБЩЕГО РЕГЛАМЕНТА ПО ЗАЩИТЕ ДАННЫХ (GDPR)

Аннотация. В статье анализируется состояние российского и европейского законодательства о персональных данных в связи со вступлением в силу Регламента Европарламента и Совета ЕС 2016/679 от 27.04.2016, более известного как GDPR. Проводится рассмотрение Регламента в сравнении с Федеральным законом № 152-ФЗ «О персональных данных», как специального нормативного правового акта, регулирующего рассматриваемый правовой институт в Российской Федерации. Делается вывод о том, что российское законодательство о персональных данных содержит некоторые недостатки, в частности отсутствие независимого органа по контролю за защитой персональных данных, которые могут быть нивелированы заимствованием соответствующих положений из Регламента и последующей гармонизацией законодательного регулирования в этой области в будущем.

Ключевые слова: персональные данные, GDPR, Общий Регламент ЕС по защите персональных данных, трансграничная передача и обработка данных, биометрические персональные данные, защита персональных данных.

TERESHIN Mark Vitalyevich,
master student of the Department of legal regulaton of Economic activities,
Financial University under the Government of the Russian Federation

Scientific supervisor:
RAKHMATULINA Rimma Shamiyevna,
PhD in Law, associate Professor

LEGAL REGULATION OF THE PROTECTION OF PERSONAL DATA IN THE RUSSIAN FEDERATION AND THE EU IN THE CONTEXT OF THE ENTRY INTO FORCE OF THE GENERAL DATA PROTECTION REGULATION (GDPR)

Annotation. The article is devoted to the analysis of the state of the Russian and European legislation on personal data in connection with the entry into force of the Regulation (EU) 2016/679 of the European Parliament and of the Council from 27.04.2016, better known as GDPR. GDPR Regulation is being considered in comparison with Federal Law No. 152-FZ «On Personal Data», as a special regulatory legal act regulating the legal institution in question in the Russian Federation. It is concluded that the Russian legislation on personal data contains some shortcomings, in particular, the lack of an independent body to control the protection of personal data, which can be offset by borrowing the relevant provisions from the GDPR Regulation and the subsequent harmonization of legislative regulation in this area in the future.

Key words: personal data, GDPR, EU General Data Protection Regulation, cross-border data processing and transfer, biometrical personal data, personal data protection.

Основы для законодательного регулирования персональных данных и их защиты начали закладываться ещё в 1950-х годах. По информации компании DLA Piper, по состоянию на сентябрь 2019 г., в том или ином виде законы, формирующие правовую базу по защите персональных данных, действуют в 111 странах мира, и Россия не стала исключением.

Первоначально, законодательство европейских стран затрагивало лишь вопросы защиты неприкосновенности частной жизни граждан. Но уже в 1970 г. в Гессене (земля ФРГ) вступил в силу первый в мире Закон о персональных данных и их защите. После этой даты и в других странах Западной Европы были приняты законодательные акты различного уровня, регулирующие защиту персональных данных в конкретной стране. Важным документом наднационального уровня стала Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» 1981 г. (далее — Конвенция СЕ 1981 г.), известная также как Конвенция 108, которая вступила в силу с 01.10.1985 г. На сегодняшний день участниками данной Конвенции являются 47 государств Совета Европы, среди которых и Российская Федерация. Что касается Евросоюза, здесь в 1995 г. была принята Директива № 95/46/ЕС «О защите физических лиц в условиях автоматизированной обработки персональных данных и о свободном обращении этих данных», действовавшая до 2018 г.

Технический прогресс и распространение Интернета заметно повлияли на возможности обработки, накопления и хранения персональных данных граждан. По этой причине Еврокомиссия в 2012 г. начала процесс по подготовке и имплементации новых положений в области работы с персональными данными в странах ЕС, которые вступили в силу с 25 мая 2018 г. под названием «Регламент № 2016/679 Европейского парламента и Совета ЕС “О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС”» (далее — Регламент). Субъектам накопления и обработки персональных данных даётся два года на приведение работы с персональными данными в соответствие с требованиями Регламента. Отметим, что Регламент носит не добровольный, а обязательный характер и должен напрямую применяться в странах - участницах ЕС (ст. 99).

В тексте Регламента законодатель сделал попытку установить единые для всех стран-участников правила обработки персональных данных, которые претерпели изменения для соответствия современному уровню развития информационных технологий. Вступление в силу Регламента

стало одной из наиболее значительных реформ сферы защиты персональных данных в Евросоюзе за последние 25 лет. В пояснительной записке к проекту Регламента законодателем было обозначено две основные причины его принятия: 1) повышение общего уровня развития общества и технологий, и связанные с ним угрозы правам и свободам личности при работе с его персональными данными; 2) непроработанность национального законодательства о персональных данных в отдельных странах Евросоюза. По мнению Ю. В. Травкина, вследствие продуманного подхода законодателей Евросоюза «европейский подход к проблеме работы с персональными данными в настоящее время получил значительное признание во всём мире» [8, с. 232].

Говоря об отечественном законодательстве, регулирующем сферу персональных данных, отметим, что оно также плотно связано с европейским. В частности, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ) был создан и принят в связи с ратификацией Российской Федерацией Конвенции СЕ 1981 г. и вследствие этого перенял многие её положения.

Несмотря на схожесть регулирования института персональных данных в России и Евросоюзе, в законодательстве имеются также и различия, которые могут влиять на трактовку некоторых понятий, а также на построение всей системы защиты персональных данных в целом. В связи с этим будет уместным и интересным сравнить эти системы между собой.

Согласно определению Закона № 152-ФЗ, персональные данные — это «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу» (называемому также субъектом персональных данных) (п. 1 ст. 3). Аналогично, в соответствии с п. 1 ст. 4 Регламента персональные данные — это «любая информация, относимая к определенному или определяемому физическому лицу (субъекту персональных данных)». Очевидно, что терминология используется весьма схожая, но Регламент более подробно определяет информацию, относящуюся к персональным данным. Отметим, что как Регламент, так и Закон № 152-ФЗ содержат широкое определение персональных данных. При этом А.А. Грибанов считает, что «только широкое определение позволяет эффективно достичь целей создания института охраны персональных данных» [5, с. 153], важнейшей из которых называются защита неприкосновенности личной жизни и семейной тайны (ст. 2 Закона № 152-ФЗ).

Статья 9 Закона № 152-ФЗ и ст. 7 Регламента указывают на необходимость получения согласия на обработку персональных данных

субъекта и уточняют особенности этого согласия. Регламент, к примеру, устанавливает требование о понятности и легкодоступности языка изложения этого согласия. Далее, согласие на обработку персональных данных должно запрашиваться отдельно от всех остальных условий и положений, при этом оно должно быть подробным (включать в себя все цели обработки) и явным (субъект должен явно поставить подпись или «галочку» на сайте о своём согласии, молчание не является согласием).

Отдельный вид персональных данных, которые присущи любому человеку с рождения, — это биометрические персональные данные. В соответствии со ст. 11 Закона № 152-ФЗ биометрические персональные данные — «это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых возможно установить его личность». Согласно п. 14 ст. 4 Регламента биометрические персональные данные — «это персональные данные, получаемые вследствие специальной технической обработки, связанные с физическими, психологическими и иными характеристиками физического лица, позволяющие однозначно идентифицировать конкретное физическое лицо или подтвердить его идентификацию». В качестве примера такого вида персональных данных могут быть изображения лица и отпечатки пальцев. А.А. Грибанов полагает, что содержащееся в отечественном Законе определение является более корректным и точным по сравнению с определением, закреплённым в Регламенте [5].

Далее, как Регламент, так и Закон № 152-ФЗ достаточно обширно определяют права субъекта этих данных. В обоих случаях люди могут ознакомиться с объёмом накопленной и обрабатываемой информации, а также изменить или вовсе удалить данные о себе из системы или хранилища. При этом в рассматриваемых правовых актах зафиксирован разный подход к реализации возможности ознакомления с данными. С одной стороны, по Закону № 152-ФЗ субъект имеет право получить сведения об обрабатываемых оператором данными путём направления запроса. С другой — по Регламенту оператор должен сам предоставить все сведения об обработке и накоплению данных в момент их получения от субъекта. Касательно удаления данных, Регламент определяет удаление информации как право субъекта данных, а по Закону № 152-ФЗ — как обязанность оператора. При этом в любом случае субъект всегда может отозвать своё согласие на обработку персональных данных о себе и затребовать их удаления у оператора.

При обработке данных в организации Закон № 152-ФЗ требует от организации-оператора

вести учёт деятельности по работе с персональными данными. Аналогично, Регламент также обязывает операторов вести учёт персональных данных в письменном или электронном виде. По Регламенту учёт обязаны проводить организации не менее чем с 250 сотрудниками, однако некоторые исследователи справедливо замечают, что такой учёт желателен в организациях любого размера [6].

Одно из заметных различий рассматриваемых правовых актов заключается в разнице по действию в пространстве, по кругу лиц, и во времени. В одном из аналитических обзоров Роскомнадзора указано, что норма о локализации персональных данных в российском законодательстве «применима к операторам, ведущих деятельность на территории России, вне зависимости от места регистрации и нахождения» [3]. Фактически, такой же принцип по распространению закона на иностранных лиц применяется в той или иной степени и к другим обязанностям, предусмотренным Законом № 152-ФЗ. Регламент тоже подразумевает действие его норм, в том числе в отношении иностранных лиц. Так, по ч. 2 ст. 3 Регламента, он применяется к обработке персональных данных субъектов на территории Евросоюза оператором, с местом нахождения за пределами ЕС в случаях, если обработка данных связана с предоставлением товаров или услуг таким субъектам персональных данных в ЕС независимо от их платности или бесплатности. Таким образом, в Регламенте не происходит ограничения сферы его действия по «национальному принципу».

Необходимость локализации персональных данных граждан, недавно закреплённая в российском законодательстве, тем не менее, подразумевает возможность трансграничной передачи персональных данных российских граждан. В контексте рассматриваемой темы сравнения отечественного и европейского законодательства отметим следующее.

Согласно ст. 12 Закона № 152-ФЗ, трансграничная передача персональных данных производится в государства, участвующие в рассмотренной ранее Конвенции СЕ 1981 г., а также в прочие страны, законодательство которых обеспечивает адекватный уровень защиты прав субъектов персональных данных. В свою очередь, Регламент устанавливает схожее определение трансграничной обработки данных и определяет необходимость уведомления субъектов персональных данных о рисках такой передачи и обработки. Регламент разрешает трансграничную обработку персональных данных в пределах единой группы компаний, но при этом обязывает их иметь единую корпоративную политику по охране и защите персональных данных субъектов.

Безусловно, действующее правовое регулирование сферы защиты персональных данных подразумевает и санкции за нарушения в этой области, что объясняется общественной важностью данного института. Так, за несоблюдение отечественного законодательства персональных данных, включая вновь принятые требования о локализации данных, предусматривается административная ответственность (закрепленная в ст. 13.11 КоАП РФ), которая с 1 июля 2017 г. получила существенные изменения. К примеру, произошло изменение подведомственности дел о нарушении положений Закона № 152-ФЗ: теперь дела о нарушении в сфере защиты персональных данных может возбуждать не только прокурор, но и должностное лицо Роскомнадзора. В свою очередь, Регламент предусматривает возможность принятия мер юридического характера за нарушение его положений компетентными надзорными органами ЕС и отдельных государств - членов Евросоюза, в том числе возможность наложения административных штрафов. Размеры штрафов могут достигать до 20 млн евро или же исчисляться в размере 4% от оборота денежных средств организации (исходя из того, что больше). Одним из наиболее заметных примеров привлечения к ответственности иностранной компании за нарушение Регламента на сегодняшний день является штраф американской компании Google регулятором Франции (CNIL) в размере 50 млн евро за недостаточное информирование пользователей при получении согласия на обработку и использование их личных данных владельцам ОС Android [9].

Конечно, ни одна организация — оператор персональных данных не может быть полностью защищена от возможных утечек персональных данных или иной потери контроля над ними. При этом действия, которые должен предпринять оператор в этом случае, описываются только в Регламенте. Так, если утечка всё-таки произошла, организация обязана незамедлительно сообщить об этом обстоятельстве как самому субъекту персональных данных, так и в надзорный орган. В противном случае она может быть подвергнута наложению штрафа.

По итогам аналитического сравнения можно сделать вывод о том, что российское законодательство о персональных данных всё ещё имеет ряд недостатков, в том числе некоторые обязательства по Закону о персональных данных затруднительны для исполнения бизнесом, либо же требуют значительных капиталовложений. Однако в целом отечественное законодательство о регулировании персональных данных (кроме некоторых нерешённых вопросов, например, по мнению Э.В. Талапиной, отсутствие независимого органа по контролю за обработкой персональных

данных) [7, с. 140] соответствует мировым стандартам. Эксперты Института исследований интернета высказали мнение о том, что регулирование деятельности провайдеров и интернет-компаний в части накопления и обработки данных их пользователей в России является одной из наиболее непроработанных сфер защиты персональных данных и частично вступает в противоречие с Регламентом [4, с. 3].

Напротив, Регламент содержит достаточно много удачных положений и подходов к правоприменению, которые можно будет успешно реализовать в отечественном правовом регулировании института защиты персональных данных. В то же время согласимся с тем, что и Регламент был принят не столько для помощи бизнесу, сколько для защиты частных лиц — субъектов персональных данных, что может негативно повлиять на рынок, так как интересы частных лиц и бизнеса в этом вопросе не всегда совпадают. В практическом плане у компаний, использующих в своём бизнесе и обрабатывающих персональные данные пользователей из Евросоюза и Российской Федерации, появляется обязанность соблюдать как Закон № 152-ФЗ, так и Регламент, что означает двойную нагрузку на бизнес.

Доработка Закона № 152-ФЗ, с учётом вступившего в силу Регламента, способствовала бы унификации российского и европейского законодательства об охране и защите персональных данных, более широким возможностям субъектов персональных данных управлять своими данными, а также развитию бизнеса и повышению инвестиционной привлекательности Российской Федерации.

Список литературы:

[1] Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) «О персональных данных» // СЗ РФ. – 2006. - N 31 (ч. 1), ст. 3451.

[2] Регламент (ЕС) 2016/679 Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)» [рус., англ.] (Принят в г. Брюсселе 27.04.2016) // СПС «КонсультантПлюс».

[3] Аналитический обзор международного опыта по локализации баз данных, содержащих персональные данные граждан [Электронный ресурс]. 2018. URL: https://pd.rkn.gov.ru/docs/Obzor_po_lokalizacii.docx (дата обращения: 30.09.2019).

[4] Анализ возможных последствий и влияния Регламента GDPR ЕС на бизнес российских операторов персональных данных (телекоммуни-

кационные компании, интернет-компании), предоставляющих услуги через интернет для лиц в странах ЕС в контексте действующего и вступающего с силу регулирования в РФ. - М.: Институт исследования Интернета, 2017. - 196 с.

[5] Грибанов А.А. Общий регламент о защите персональных данных (General Data Protection Regulation): идеи для совершенствования российского законодательства // Закон. - 2018. - № 3. - С. 149 - 162.

[6] Заведенская А. Влияние GDPR на российских операторов персональных данных [Электронный ресурс]. 05.08.2015. URL: https://www.ussc.ru/news/novosti/vliyanie_gdpr_na_rossiyskikh_operatorov_personalnykh_dannykh/ (дата обращения: 30.09.2019).

[7] Талапина Э.В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды ИГП РАН. - 2018. - № 5. - С. 117 - 149.

[8] Травкин Ю. Персональные данные. - М.: Амалданик, 2007. - 430 с.

[9] La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de la société GOOGLE LLC. [франц.] [Электронный ресурс]. 21.01.2019. URL: <https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la> (дата обращения: 30.09.2019).

Spisok literatury:

[1] Federal'nyj zakon ot 27.07.2006 N 152-FZ (red. ot 31.12.2017) «O personal'nyh dannyh» // SZ RF. - 2006. - N 31 (ch. 1), st. 3451.

[2] Reglament (ES) 2016/679 Evropejskogo parlamenta i Soveta Evropejskogo Soyuzа «O zashchite fizicheskikh lic pri obrabotke personal'nyh dannyh i o svobodnom obrashchenii takih dannyh, a takzhe ob otmene Direktivy 95/46/ES (Obshchij Reglament o zashchite personal'nyh dannyh)» [rus.,

angl.] (Prinyat v g. Bryussele 27.04.2016) // SPS «Konsul'tantPlyus».

[3] Analiticheskij obzor mezhdunarodnogo opyta po lokalizacii baz dannyh, sodержashchih personal'nye dannye grazhdan [Elektronnyj resurs]. 2018. URL: https://pd.rkn.gov.ru/docs/Obzor_po_lokalizacii.docx (data obrashcheniya: 30.09.2019).

[4] Analiz vozmozhnyh posledstvij i vliyaniya Reglamenta GDPR ES na biznes rossijskikh operatorov personal'nyh dannyh (telekommunikacionnye kompanii, internet-kompanii), predostavlyayushchih uslugi cherez internet dlya lic v stranah ES v kontekste dejstvuyushchego i vstupayushchego s silu regulirovaniya v RF. - М.: Institut issledovaniya Interneta, 2017. - 196 s.

[5] Griбанov А.А. Obshchij reglament o zashchite personal'nyh dannyh (General Data Protection Regulation): idei dlya sovershenstvovaniya rossijskogo zakonodatel'stva // Закон. - 2018. - № 3. - С. 149 - 162.

[6] Zavedenskaya А. Vliyanie GDPR na rossijskikh operatorov personal'nyh dannyh [Elektronnyj resurs]. 05.08.2015. URL: https://www.ussc.ru/news/novosti/vliyanie_gdpr_na_rossiyskikh_operatorov_personalnykh_dannykh/ (data obrashcheniya: 30.09.2019).

[7] Talapina E.V. Zashchita personal'nyh dannyh v cifrovuyu epohu: rossijskoe pravo v evropejskom kontekste // Trudy IGP RAN. - 2018. - № 5. - С. 117 - 149.

[8] Travkin Yu. Personal'nye dannye. - М.: Амалданик, 2007. - 430 с.

[9] La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de la société GOOGLE LLC. [franc.] [Elektronnyj resurs]. 21.01.2019. URL: <https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la> (data obrashcheniya: 30.09.2019).

