DOI: 10.17803/1729-5920.2020.159.2.033-043

В. И. Солдатова*

Защита персональных данных в условиях применения цифровых технологий

Аннотация. В течение последних лет вопросы применения законодательства в области персональных данных стали предметом внимания ученых-юристов. С развитием цифровых технологий особую актуальность приобретает проблема защиты персональных данных. Значение персональных данных настолько велико, что некоторые ученые квалифицируют их как нематериальные блага.

В целях защиты интересов граждан наше государство принимает меры по локализации данных о гражданах путем законодательного регулирования российского сегмента Интернета. Применяются также и такие меры, как право на забвение и обезличивание персональных данных.

Однако, как показывает практика, в том числе и судебная, имеющиеся средства защиты персональных данных являются недостаточными в условиях использования новых технологий. Вместе с тем практика применения законодательства о персональных данных выявляет ряд проблем, которые требуют своего решения. Много вопросов вызывает в практике деятельности государственных органов отнесение к персональным данным конкретной информации о физических лицах. Согласно действующей редакции ст. 3 Федерального закона персональные данные представляют собой любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). При этом закон не определяет, какие конкретно данные о физическом лице относятся к персональным данным. В силу такого широкого понимания персональных данных и возникают вопросы об отнесении к ним той или иной информации о физическом лице. В связи с этим важной теоретической задачей представляется определение критериев отнесения конкретных сведений о лице к персональным данным.

Особенно актуальными являются усиление ответственности за нарушение законодательства о персональных данных, определение приоритетов в вопросе обеспечения нейтральности Интернета, решение проблемы соотношения открытого режима общедоступных данных и необходимости защиты персональных данных. По мнению автора, необходимо обеспечить с помощью комплекса мер приоритет обеспечения защиты персональных данных граждан. Эта проблема приобретает особое значение в связи с подготовкой новых законов о цифровом профиле гражданина.

Ключевые слова: персональные данные; согласие на обработку персональных данных; цифровая экономика; право на забвение; обезличивание персональных данных; категории персональных данных; биометрические персональные данные; Интернет; локализации баз с персональными данными; открытый режим общедоступных данных; цифровой профиль.

Для цитирования: *Солдатова В. И.* Защита персональных данных в условиях применения цифровых технологий // Lex russica. — 2020. — Т. 73. — № 2. — С. 33—43. — DOI: 10.17803/1729-5920.2020.159.2.033-043.

* *Солдатова Вера Ивановна,* кандидат юридических наук, доцент кафедры гражданского права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
vera1038@yandex.ru

Protection of Personal Data in Digital Environment

Vera I. Soldatova, Cand. Sci. (Law), Associate Professor of the Department of Civil Law, Kutafin Moscow State Law University (MSAL)
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
vera1038@yandex.ru

Abstract. In recent years, the application of legislation in the field of personal data has become the focus of attention of legal scholars. With the development of digital technologies, the problem of protection of personal data becomes especially urgent. The importance of personal data is so great that some scholars treat them as intangible goods.
In order to protect the interests of citizens, our State takes measures to localize citizens' personal data by statutory regulation of the Russian segment of the Internet. Such remedies as the right to be forgotten and personal data anonymization are also applied.
However, the practice, including judicial practice, shows that the available means of protection of personal data are insufficient in the context of new technologies. However, the practice of application of laws on personal data reveals a number of problems that need to be addressed. The attribution of specific information about natural persons to personal data leads to a number of questions with regard to the practice of the activities of state bodies. Under currently effective Article 3 of the Federal Law, the term personal data refers to any information relating directly or indirectly to a certain or definable natural person (subject of personal data). At the same time, the law does not specify which data about an individual refers to personal data. Due to this broad understanding of personal data, questions arise concerning the attribution of paticular information about an individual to personal data. In this regard, the definition of criteria for the attribution of specific information about a person to personal data becomes an important theoretical task.
The issues of primary concern include: 1) strengthening of responsibility for violation of personal data legislation; 2) giving priority to the issue of neutrality of the Internet, 3) solving the problem of the balance between direct access to publicly available data and the need to protect personal data. In the author's opinion, it is necessary to ensure by means of comprehensive measures the priority of protection of personal data of citizens. This problem is of particular importance in connection with the elaboration of new laws on the digital profile of citizens.
Keywords: personal data; consent to the processing of personal data; digital economy; right to be forgotten; personal data anonymization; categories of personal data; biometric personal data; Internet; localization of databases with personal data; direct access to publicly available data; digital profile.
Cite as: Soldatova VI. Zashchita personalnykh dannykh v usloviyakh primeneniya tsifrovykh tekhnologiy [Protection of Personal Data in Digital Environment]. *Lex russica*. 2020;73(2):33—43. DOI: 10.17803/1729-5920.2020.159.2.033-043. (In Russ., abstract in Eng.).

В настоящее время практически во всех странах в экономической сфере широко используются цифровые технологии, и Россия не является исключением. Создание цифровой экономики является важной задачей нашего государства. Указом Президента РФ от 09.05.2017 № 203 была утверждена Стратегия развития информационного общества в Российской Федерации на 2017—2030 годы[1] (далее — Стратегия).

В соответствии со Стратегией целью развития информационной и коммуникационной инфраструктуры Российской Федерации является обеспечение свободного доступа граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления к информации на всех этапах ее создания и распространения (п. 27).

Указанная Стратегия определяет задачу по совершенствованию нормативно-правового регулирования в сфере обеспечения безопасной обработки информации (включая ее поиск, сбор, анализ, использование, сохранение и распространение) и применения новых технологий, уровень которого должен соответствовать развитию этих технологий и интересам общества (п. 31). Однако на данном этапе в этой сфере возникают новые проблемы, требующие правового регулирования.

Несомненно, что широкое применение цифровых технологий в самых разных сферах деятельности государства уже сегодня создает

[1] СЗ РФ. 2017. № 20. Ст. 2901.

условия «прозрачности» различных отношений, в которых участвуют государственные органы, некоммерческие организации и граждане. В ряде сфер экономики государство осуществляет контроль за деятельностью субъектов предпринимательской деятельности (например, банки контролируют финансовые операции юридических лиц и граждан). Многие банковские операции проводятся с использованием сети Интернет (открытие банком счетов юридическим и физическим лицам, зачисление и списание денежных средств со счетов). При этом, как обоснованно замечают некоторые авторы, доступность информации о субъектах и об объектах предпринимательских отношений в целом — это положительное явление, но возникает проблема защиты данных в сети Интернет[2].

Отношения по сбору, хранению, обработке и использованию информации регулируются различными нормативными актами, составляющими законодательство о персональных данных.

Говоря о законодательстве Российской Федерации о персональных данных, прежде всего следует назвать международный акт — Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, которую Россия ратифицировала еще до принятия Федерального закона «О персональных данных»[3].

Защита персональных данных в нашей стране осуществляется в рамках Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 31.12.2017)[4]. Статья 2 названного Закона прямо устанавливает, что его целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Данной норме Федерального закона «О персональных данных» корреспондирует правило ст. 152.2 Гражданского кодекса РФ об охране частной жизни гражданина.

Защите прав граждан служит также и установленная Федеральным законом «О персональных данных» (ч. 5 ст. 18) обязанность оператора, осуществляющего сбор персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», обеспечить запись, систематизацию, накопление, хранение, а также обновление, изменение, извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

Значение Федерального закона «О персональных данных» состоит в том, что он является основой правового регулирования сбора, обработки и использования персональных данных. Вместе с тем возникающие сегодня проблемы защиты персональных данных обусловлены недостаточной правовой регламентацией данных отношений.

Так, много вопросов вызывает в практике деятельности государственных органов *отнесение к персональным данным конкретной информации о физических лицах*. Согласно действующей редакции ст. 3 Закона персональные данные представляют собой любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Закон не определяет, какие конкретно данные о физическом лице относятся к персональным данным.

Заметим, что такое широкое понимание персональных данных было закреплено Федеральным законом от 25.07.2011 № 261-ФЗ, которым были внесены изменения в Федеральный закон «О персональных данных»[5]. До внесения этих изменений пункт 1 ст. 3 Федерального закона «О персональных данных» определял персональные данные как любую информацию, относящуюся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилию, имя, отчество, год, месяц, дату и место рождения, адрес, семейное, соци-

---

2 *Михайлов А. В.* Проблемы становления цифровой экономики и вопросы развития предпринимательского права // Актуальные проблемы российского права. 2018. № 11. С. 68—73.

3 Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» // СЗ РФ. 2005. № 52 (ч. 1). Ст. 5573.

4 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». // СЗ РФ. 2006. № 31 (ч. 1). Ст. 3451.

5 Федеральный закон от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон “О персональных данных”» // СЗ РФ. 2011. № 31. Ст. 4701.

альное, имущественное положение, образование, профессию, доходы, другую информацию. Таким образом, ранее действовавшая редакция Закона определяла неполный перечень информации, относящейся к персональным данным.

Внесение изменений в Федеральный закон «О персональных данных» и закрепление нового понятия персональных данных было вызвано необходимостью приведения Закона в соответствие с Конвенцией 1981 г.[6], согласно ст. 2 (а) которой термин «персональные данные» означает любую информацию об определенном или поддающемся определению физическом лице. Следовательно, приведенная дефиниция понятия «персональные данные» появилась в результате имплементации в российское законодательство положений международного акта.

Федеральный закон «О персональных данных» выделяет несколько категорий персональных данных.

Специальные категории персональных данных, к которым относятся расовая, национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимная жизнь (ч. 1 ст. 10). Эти данные имеют особый режим обработки: обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных ч. 2 ст. 10 Закона.

Кроме того, Закон выделяет *биометрические персональные данные*. К ним относятся сведения, которые характеризуют физиологические и биологические особенности человека, на основе которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных. Закон установил специальный режим обработки этих данных — они могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением установленных законом случаев (например, в связи с реализацией международных договоров Российской Федерации, в связи с осуществлением правосудия и др.).

Отметим, что в законодательстве отсутствует перечень биометрических персональных данных. Примерный перечень содержат разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30.08.2013[7]. Согласно названным Разъяснениям к биометрическим персональным данным относятся физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и др.), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта. Отметим, что названный акт по своей юридической силе не является нормативным. Полагаем, что перечень биометрических персональных данных должен содержаться не в ведомственном акте, а нормативном акте Правительства РФ.

Постановление Правительства РФ от 30 июня 2018 г. № 772 определяет следующие виды биометрических персональных данных физического лица — гражданина Российской Федерации:

— данные изображения лица человека, полученные с помощью фото-, видеоустройств;
— данные голоса человека, полученные с помощью звукозаписывающих устройств[8].

В настоящее время некоторые российские банки осуществляют сбор биометрических данных клиентов в целях получения клиентами услуг любого банка дистанционно. В этом случае возможно открывать счета и вклады,

---

[6] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28.01.1981) // СПС «КонсультантПлюс».

[7] Разъяснения Роскомнадзора от 30.08.2013 «Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки» // СПС «КонсультантПлюс».

[8] Постановление Правительства РФ от 30.06.2018 № 772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации» // СЗ РФ. 2018. № 28. Ст. 4234.

получать кредиты в удобное для клиентов время. Процедура сбора биометрических данных добровольная и бесплатная, осуществляется только с согласия клиента. В целях безопасности биометрические данные хранятся в Единой биометрической системе (ЕБС) отдельно от персональных данных. При желании клиентов эти данные можно удалить из базы через Портал госуслуг[9].

Банк России направил банкам информационное письмо от 1 марта 2019 г., в котором разъяснил порядок регистрации клиента в Единой системе идентификации и аутентификации (ЕСИА) и сбора биометрических данных в Единую биометрическую систему. ЦБ РФ указал на необходимость четко разъяснять клиентам, в какую именно биометрическую систему передаются их данные — в ЕБС или собственную систему банка. Заметим, что названное письмо Банка России не носит нормативный характер.

Федеральный закон «О персональных данных» определяет также категорию *персональных данных общего характера* — это любая информация, относящаяся к прямо или косвенно определенному физическому лицу (ст. 3). Таким образом, Закон содержит основной признак персональных данных — информация относится к прямо или косвенно определенному или определяемому физическому лицу, т.е. *возможна идентификация субъекта*. Заметим, что действующая редакция ст. 128 ГК РФ не предусматривает в числе объектов гражданских прав информацию, хотя ранее информация относилась к этим объектам.

В литературе справедливо отмечается, что персональные данные общего характера являются самыми сложными и запутанными для понимания и интерпретации... Точная идентификация лица будет иметь место в случае соотнесения информации с фамилией, именем и отчеством (при наличии) лица. Именно данные сведения являются основным идентификатором гражданина в гражданском обороте, поскольку гражданин приобретает и осуществляет права и обязанности под своим именем (п. 1 ст. 19 ГК РФ)[10].

Косвенная идентификация прямо не указывает на имя или фамилию конкретного лица, но с ее помощью можно отнести к персональным данным информацию, содержащую описание индивидуальных характеристик лица, позволяющих отличить его от других субъектов. К такой косвенной идентификации, по мнению А. И. Савельева, относятся, например, данные о трафике (метаданных), в частности, сведения об установленных соединениях с указанием времени и продолжительности соединения, номеров или IP-адресов устройств, участвующих в коммуникации, на основании которых лицо может быть косвенно идентифицировано. В некоторых случаях лицо может быть идентифицировано на основании таких косвенных данных, как его логин, используемый в различных интернет-сервисах; данных с камер видеонаблюдения, реквизитов банковской карты, сведений о принадлежащей лицу собственности и пр.[11]

Таким образом, в законодательстве отсутствует даже примерный перечень персональных данных о лице, а также четкие критерии отнесения конкретных сведений о лице к персональным данным. Это порождает вопросы о возможности отнесения к персональным данным тех или иных сведений о лице, что особенно актуально в условиях использования цифровых технологий.

При отсутствии правовой определенности в вопросе отнесения к персональным данным конкретных сведений о лице представляет интерес позиция судов. Примером может служить спор между Управлением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Центральному федеральному округу (далее — заявитель) и ПАО «МГТС» (далее — общество, ответчик)[12]. Управление обратилось в Арбитражный суд г. Москвы с требованием о привлечении ПАО «МГТС» к административной ответственности по ч. 3 ст. 14.1 КоАП РФ на основании протокола об административном правонарушении № 01-1-41-16-16 от 11.01.2016.

В соответствии с ч. 3 ст. 14.1 КоАП РФ осуществление предпринимательской деятель-

[9] URL: https://news.rambler.ru/other/42629530/?utm_content=rnews&utm_medium=read_more&utm_source=copylink (дата обращения: 28.08.2019).

[10] *Савельев А. И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных. М. : Статут, 2017.

[11] *Савельев А. И.* Указ. соч.

[12] Постановление Девятого арбитражного апелляционного суда от 23.05.2016 № 09АП-17574/2016 // СПС «КонсультантПлюс».

ности с нарушением условий, предусмотренных специальным разрешением (лицензией), влечет наложение административного штрафа на юридических лиц в размере от 30 тыс. до 40 тыс. руб.

ПАО «МГТС», по мнению заявителя, осуществляло лицензируемый вид деятельности — оказание телематических услуг связи с нарушением лицензионных условий, предусмотренных специальным разрешением (лицензией). По результатам проверки было установлено, что ответчик передает партнерам сведения об абоненте, включающие поисковые запросы абонентов, интернет-адреса веб-страниц, посещаемых абонентами, тематику информации, размещенной на посещаемых абонентами интернет-ресурсах, IP-адрес абонента, достаточные для формирования рекламного профиля абонента, необходимого для предоставления ему адресной рекламной информации, что подтвердилось в ходе проверки снятым скриншотом передаваемой информации.

Было установлено, что информация, получаемая от оператора связи, позволяет прямо или косвенно идентифицировать пользователя как определенное физическое лицо (субъект персональных данных).

Суд посчитал, что данными, позволяющими идентифицировать абонента или его конечное оборудование, являются: фамилия, имя, отчество или псевдоним абонента-гражданина, адрес абонента (адрес установки оконечного оборудования), абонентские номера, другие данные, позволяющие идентифицировать абонента или его оконечное оборудование, сведения баз данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента.

ПАО «МГТС» на основании договора предоставляло другому юридическому лицу (ООО «ОБМР») сведения об абонентах (пользователях): случайный идентификатор (Cookie «UID») в HTTP-запросе пользователя, позволяющий отличить трафик пользователя от трафика других пользователей для получения списка его предпочтений; IP-адрес из IP-пакета HTTP-запроса пользователя, позволяющий получить географическое положение пользователя с точностью определения до названия населенного пункта; User-Agent HTTP-запроса пользователя, позволяющий получить модель устройства или типа браузера, используемого пользователем; время просмотра веб-страниц (HTTP-запроса пользователя), позволяющее оценить частоту, с которой пользователь проявляет те или иные предпочтения; URL-адрес и заголовок Referrer HTTP-запроса пользователя, позволяющие определить предпочтения пользователя; Hash-ID линии пользователя, позволяющий определить линии, абоненты которых выразили несогласие с обработкой данных.

По мнению суда, передаваемая информация является информацией о соединениях и трафике абонента, а следовательно, представляет собой сведения об абонентах.

Заявление было удовлетворено, ПАО «МГТС» привлечено к административной ответственности. Однако ответчик направил апелляционную жалобу об отмене решения суда. В итоге решение Арбитражного суда г. Москвы было оставлено без изменения.

Признание судами в качестве сведений об абоненте запросов абонента, интернет-адресов веб-страниц, посещаемых абонентом, IP-адресов абонента и др., которые позволяют идентифицировать абонента, имеет важное значение, поскольку оно является судебным толкованием норм закона. Это толкование позволяет восполнить пробел в правовом регулировании в части конкретизации данных, которые относятся к *персональным данным общего характера*.

Использование новых информационных технологий повлияло на развитие законодательства о персональных данных. Прежде всего следует назвать Федеральный закон от 13.07.2015 № 264-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации” и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации»[13]. Значение этого Закона состоит в том, что он ввел в российское законодательство «*право на забвение*». Нормы названного Закона обязывают операторов поисковых систем в Интернете прекращать выдавать ссылки на информацию о пользователях, обратившихся к ним с соответствующим требованием (ст. 10.3 Федерального закона «Об информации, информационных технологиях и о защите информации»).

Оператор поисковой системы, распространяющий в сети Интернет рекламу, направленную на привлечение внимания потребителей, находящихся на территории Российской Федерации, по требованию гражданина обязан прекратить

[13] СЗ РФ. 2015. № 29 (ч. I). Ст. 4390.

выдачу сведений об указателе страницы сайта в Интернете, позволяющих получить доступ к информации о заявителе. Это относится к информации, распространяемой с нарушением законодательства, являющейся недостоверной, а также неактуальной, утратившей значение для заявителя в силу последующих событий или действий заявителя, за исключением информации о событиях, содержащих признаки уголовно наказуемых деяний, сроки привлечения к уголовной ответственности по которым не истекли, и информации о совершении гражданином преступления, по которому не снята или не погашена судимость.

Важным средством защиты персональных данных является также *обезличивание данных о конкретном лице*. Обезличивание персональных данных — это действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. Требование об обезличивании персональных данных устанавливает Федеральный закон «О персональных данных» (п. 9 ст. 3) и конкретизируют подзаконные акты[14].

Несмотря на принятие новых законов, а также принятие государственными органами подзаконных актов, среди которых особое значение имеют акты Роскомнадзора, правовое регулирование отношений по использованию и защите персональных данных трудно признать удовлетворительным.

Основные проблемы в рассматриваемой сфере, на наш взгляд, состоят в следующем.

Во-первых, необходимо урегулировать *вопрос об ответственности* субъектов отношений по сбору, обработке, хранению и распространению персональных данных. Согласно ст. 24 Федерального закона «О персональных данных» лица, виновные в нарушении требований данного Закона, несут предусмотренную законодательством Российской Федерации ответственность.

Кодекс РФ об административных правонарушениях устанавливает административную ответственность лиц за нарушение законодательства Российской Федерации в области персональных данных (ст. 13.11), за осуществление незаконной деятельности в области защиты информации (ст. 13.13), за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14).

Отметим, что размер административного штрафа за указанные административные правонарушения весьма мал. Так, обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации, влечет наложение административного штрафа на должностных лиц — от 10 тыс. до 20 тыс. руб., а на юридических лиц — от 15 тыс. до 75 тыс. руб. (ч. 2 ст. 13.11 КоАП РФ). Разглашение информации, доступ к которой ограничен федеральным законом, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа на граждан в размере от 500 до 1 тыс. руб.; на должностных лиц — от 4 тыс. до 5 тыс. руб. Очевидно, что размер такой ответственности не соответствует материальным (и не только) последствиям разглашения персональных данных и информации с ограниченным доступом.

Об актуальности защиты персональных данных свидетельствуют и результаты плановых проверок, которые проводит Роскомнадзор, являющийся уполномоченным органом по защите прав субъектов персональных данных. Роскомнадзор в 2018 г. провел 832 плановые проверки соблюдения законодательства о персональных данных, по результатам которых различные нарушения были выявлены в 80 % случаев[15]. В течение 2018 г. органами

[14] Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (вместе с Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ) (зарегистрирован в Минюсте России 10.09.2013 № 29935) // СПС «КонсультантПлюс».

[15] URL: https://rkn.gov.ru/docs/Otchet_o_dejatel6nosti_Upolnomochennogo_organa.pdf (дата обращения: 28.08.2019).

Роскомнадзора было составлено и направлено в суды 156 протоколов об административных правонарушениях в отношении персональных данных за такие нарушения. Из них 67 протоколов об административных нарушениях было составлено по ч. 1 ст. 13.11 КоАП РФ, предусматривающей ответственность за обработку персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных. Чуть меньше (31) было составлено протоколов об административных нарушениях по ч. 2 ст. 13.11 КоАП РФ за обработку персональных данных без получения согласия в письменной форме субъекта персональных данных.

Очевидно, что одной из причин многочисленных нарушений в сфере обработки персональных данных является мизерная сумма штрафа (максимальный размер составляет всего 75 тыс. руб.). Размер ответственности за нарушение правил обработки персональных данных, установленных Директивой ЕС, во много раз превышает размер штрафа, предусмотренного КоАП РФ.

С мая 2018 г. в Европе действуют новые правила обработки персональных данных, установленные Общим регламентом по защите данных (Регламент ЕС 2016/679 от 27.04.2016, GDPR — General Data Protection Regulation). Названный регламент имеет прямое действие в 28 странах ЕС. С его принятием утратила силу Директива о защите персональных данных 95/46/ЕС от 24.10.1995. Важной особенностью GDPR является экстерриториальный принцип действия новых европейских правил обработки персональных данных, а также усиление ответственности за нарушение правил обработки персональных данных: штрафы достигают 20 млн евро (около 1,5 млрд руб.).

Отсюда очевидна необходимость изменения российского законодательства в части значительного усиления ответственности за нарушения законодательства о персональных данных.

Кроме того, расширение сфер применения современных технологий значительно изменяет степень общественной опасности правонарушений, совершаемых в этих областях. Особенно это относится к распространению информации в информационно-телекоммуникационной сети Интернет.

В этой связи заслуживает внимания законопроект № 729516-7 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (внесен в Государственную Думу 13.06.2019). Он направлен на реализацию ч. 5 ст. 18 Федерального закона «О персональных данных», устанавливающей обязанность оператора при сборе персональных данных, в том числе посредством сети Интернет, обеспечить запись, систематизацию, накопление, хранение, уточнение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации. Неисполнение оператором обязанности по локализации баз с персональными данными создает угрозу безопасности граждан, препятствует эффективной борьбе с терроризмом и экстремизмом.

Законопроект предлагает усилить административную ответственность — дополнить ст. 13.11 КоАП РФ новой частью 8, предусматривающей ответственность за невыполнение оператором при сборе персональных данных, в том числе посредством сети Интернет, обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения, извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации. Предлагается наложение административного штрафа на граждан в размере от 30 тыс. до 50 тыс. руб.; на должностных лиц — от 200 тыс. до 500 тыс. руб.; на юридических лиц — от 2 млн до 6 млн руб. Повторное совершение данного деяния влечет наложение административного штрафа на граждан в размере от 50 тыс. до 100 тыс. руб.; на должностных лиц — от 500 тыс. до 1 млн руб.; на юридических лиц — от 6 млн до 18 млн руб.

Думается, что такое существенное усиление административной ответственности операторов за неисполнение обязанности по локализации баз с персональными данными послужит снижению уровня нарушений в сфере сбора и обработки персональных данных граждан.

Полагаем необходимым усилить ответственность операторов и за нарушение правил, установленных ч. 1 и 2 ст. 13.11 КоАП РФ. Нуждается в соответствующем изменении также и часть 6 ст. 13.11. КоАП, устанавливающая ответственность за невыполнение оператором при обработке персональных данных обязанности по обеспечению сохранности персональных данных при хранении материальных носителей персональных данных, недопущения несанкционированного к ним доступа (в том числе уничтожение, изменение, копирование, распространение данных). В настоящее вре-

мя часть 6 ст. 13.11 КоАП РФ предусматривает наложение административного штрафа за неисполнение обязанности по обеспечению сохранности персональных данных на должностных лиц от 4 тыс. до 10 тыс. руб. Для юридических лиц максимальный размер штрафа составляет всего 50 тыс. руб. Несомненно, что такой мизерный размер штрафа не может препятствовать действиям по незаконному доступу к персональным данным, их копированию и распространению. С учетом того что основными обладателями персональных данных являются кредитные организации (банки, МФО), понятна необходимость существенного усиления ответственности операторов за нарушение законодательства о персональных данных.

Другой проблемой является соотношение *защиты персональных данных* и *публичного интереса*. По мнению Э. В. Талапиной, этот конфликт можно рассматривать как частный случай проявления общего конфликта публичного и частного права, поскольку публичный интерес предполагает специфическое ви́дение проблемы глазами самого общества. Многие государства предусматривают специальные правила, регламентирующие хранение персональных данных своих граждан. И в этом контексте все чаще возникает вопрос о праве собственности на персональные данные или, как предусмотрено во французском Законе о цифровой Республике от 7 октября 2016 г., о свободе распоряжения собственными персональными данными. В этом случае частноправовым свободам «противостоят» публично-правовые интересы локализации персональных данных, в том числе интересы национальной безопасности[16].

Весьма актуальным является решение вопроса о правах на персональные данные, которые содержатся в социальных сетях (Facebook, «ВКонтакте», Linkedin). Это сведения о фамилиях пользователей сетей, об их месте работы или учебы, месте проживания и т.п. Понятно, что эти данные первоначально были предоставлены в сеть при регистрации самими пользователями. Проблема возникает при использовании персональных данных пользователей социальной сети третьими лицами (коммерческими организациями) в своих целях. При этом разрешения на это использование данных коммерческие организации от пользователей и от социальной сети не получают и не платят за пользование данными. В некоторых случаях инициаторами рассмотрения в суде дел об использовании данных пользователей социальных сетей являются владельцы этих баз данных. Судебная практика по таким делам довольно обширна (например, определение Верховного Суда РФ от 29.01.2018 № 305-КГ17-21291 по делу № А40-5250/2017, постановление Девятого арбитражного апелляционного суда от 27.07.2017 № 09АП-31744/2017 по делу № А40-5250/17). Согласно позиции судов не являются общедоступными обрабатываемые организациями персональные данные, содержащиеся в открытых источниках (социальных сетях: «ВКонтакте», «Одноклассники», «МойМир», Instragram, Twitter; интернет-порталов «Авито» и «Авто.ру»). Соответственно, необходимо получение согласия граждан на использование их данных.

На наш взгляд, законодательное закрепление указанной позиции судов по использованию персональных данных граждан, содержащихся в базах социальных сетей, восполнило бы этот пробел.

Любое государство заинтересовано в получении максимально полной информации о гражданах, в интересах же граждан обеспечить защиту своих персональных данных. Характер правового регулирования в сфере сбора, обработки и использования персональных данных определяется позицией государства в выборе приоритета интересов. На наш взгляд, необходимо юридически обеспечить «частноправовой» подход при подготовке новых нормативных правовых актов в рассматриваемой сфере. В литературе верно отмечалось, что в нашей стране защита интересов государства осуществляется успешно, в отличие от защиты интересов личности[17].

В связи с этим возникает вопрос о возможности применения норм Закона РФ «О защите прав потребителей» для обеспечения интересов граждан — субъектов персональных данных. Граждане часто сталкиваются с утечкой их персональных данных и использованием последних различными организациями в своих

[16] *Талапина Э. В.* Защита персональных данных в цифровую эпоху. Российское право в европейском контексте // Труды Института государства и права РАН. 2018. Т. 13. № 5. С. 137.

[17] *Петрыкина Н. И.* Правовое регулирование оборота персональных данных. Теория и практика. М. : Статут, 2011. С. 2.

целях. Это обусловлено практикой заключения с гражданами договоров на оказание услуг (медицинских услуг, на оказание услуг в банковской сфере и др.), в соответствии с которой граждане в обязательном порядке предоставляют согласие на обработку их персональных данных. При этом гражданам, как правило, не разъясняют необходимость получения от них такого согласия, а также возможность отозвать такое согласие.

Закон РФ «О защите прав потребителей» не содержит положений о предоставлении потребителями своих персональных данных при заключении договоров. Однако это, на наш взгляд, не является препятствием для применения норм данного Закона в отношениях по сбору и обработке персональных данных граждан. Этот вывод подтверждается и судебной практикой: при рассмотрении дел об использовании персональных данных граждан суды применяют нормы Закона РФ «О защите прав потребителей».

Примером может служить постановление Арбитражного суда Северо-Западного округа от 18 июля 2016 г. № Ф07-5537/2016 по делу № А44-9647/2015. Страховое акционерное общество ВСК (Нижегородский филиал) обратилось в арбитражный суд с заявлением о признании незаконным предписания Управления Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по Новгородской области. Предписание предусматривало устранение нарушений законодательства о защите прав потребителей: условия типовых форм договоров нарушают положения ст. 16 Закона РФ от 07.02.1992 № 2300-1 «О защите прав потребителей». Предписание Управления Роспотребнадзора обязало страховое акционерное общество ВСК изменить условия договоров страхования таким образом, чтобы гражданин обладал возможностью выбора: выразить согласие или отказаться от обработки, распространения, передачи персональных данных страхователя.

Представляет интерес мотивировочная часть решения кассационной судебной инстанции. Суд отмечает, что договор страхования относится к договорам присоединения, условия договора разработаны самим страховщиком, а подписание его страхователем не может служить безусловным выражением воли и личного согласия страхователя, данным свободно и в своем интересе. При этом правовая природа договора присоединения лишает страхователя возможности до заключения договора изменить указанное условие, ограничив в той или иной мере распространение персональной информации так, как он сам это считает необходимым. Таким образом, отсутствие у потребителя права выбора возможности согласия или отказа в согласии на обработку персональных данных ущемляет права потребителей, что в силу ст. 16 Закона № 2300-1 свидетельствует об их недействительности в этой части.

Некоторые авторы выделяют и такие проблемы, требующие правового решения, как защита персональных данных и общедоступность данных, защита персональных данных и свобода и нейтральность Интернета, защита персональных данных работников и права работодателя на эти данные и др.[18]

На наш взгляд, проблема стоит несколько шире — *необходимо создать механизм, обеспечивающий комплексную защиту персональных данных граждан*, который мог бы противодействовать незаконным сбору, обработке, а также использованию персональных данных граждан. При этом полагаем необходимым обеспечить приоритет защиты прав гражданина как основополагающего принципа отношений в сфере сбора, обработки и использования персональных данных. Эта задача особенно актуальна в связи с реализацией задачи по созданию цифрового профиля.

В Государственную Думу в июле 2019 г. внесен соответствующий проект федерального закона № 747513-7 «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)». Законопроект предусматривает создание и использование цифрового профиля.

Цифровой профиль является совокупностью сведений о гражданах и юридических лицах, содержащихся в информационных системах государственных органов, органов местного самоуправления и организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, а также в единой системе идентификации и аутентификации.

С помощью инфраструктуры цифрового профиля может обеспечиваться:

— идентификация и аутентификация физических и юридических лиц;

[18] *Талапина Э. В.* Указ. соч. С. 139.

— доступ к цифровому профилю и предоставление сведений, входящих в цифровой профиль, в электронной форме физическим и юридическим лицам;
— предоставление и обновление по запросу государственных органов, органов местного самоуправления, организаций, осуществляющих публичные полномочия, сведений о физическом или юридическом лице, содержащихся в цифровом профиле;
— хранение сведений о гражданах и юридических лицах, в том числе результатов предоставления государственных и муниципальных услуг в электронной форме.

Важной новеллой законопроекта является положение, предусматривающее получение и отзы́в согласия на обработку персональных данных граждан и сведений о юридических лицах в случаях, если эти сведения были получены с использованием инфраструктуры цифрового профиля. Действующее законодательство о персональных данных не регламентирует порядок получения и отзы́ва согласия на обработку персональных данных граждан, оно лишь предусматривает возможность отзы́ва согласия. Согласно законопроекту субъект персональных данных отзывает такое согласие в инфраструктуре цифрового профиля в форме электронного документа, в том числе подписанного усиленной квалифицированной электронной подписью или простой электронной подписью, ключ которой был получен при обращении за получением государственных и муниципальных услуг в электронной форме.

Рассматриваемый законопроект устанавливает правила дистанционной идентификации и аутентификации лиц, носящей юридически значимый характер и порождающей правовые последствия, в случае если правоотношения складываются в сферах, не относящихся к предоставлению государственных услуг и осуществлению государственных функций. Законопроект содержит определения таких понятий, как «идентификация», «аутентификация», «цифровой профиль», вводит правовой институт цифрового профиля с его более детальным регулированием, а также предоставляет Правительству РФ полномочия по определению порядка получения и предоставления сведений с использованием цифрового профиля.

БИБЛИОГРАФИЯ

1. *Михайлов А. В.* Проблемы становления цифровой экономики и вопросы развития предпринимательского права // Актуальные проблемы российского права. — 2018. — № 11.
2. *Петрыкина Н. И.* Правовое регулирование оборота персональных данных. Теория и практика. — М. : Статут, 2011.
3. *Савельев А. И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». — М. : Статут, 2017.
4. *Талапина Э. В.* Защита персональных данных в цифровую эпоху. Российское право в европейском контексте // Труды Института государства и права РАН. — 2018. — Т. 13. — № 5.

Материал поступил в редакцию 29 августа 2019 г.

REFERENCES

1. Mikhailov AV. Problemy stanovleniya tsifrovoy ekonomiki i voprosy razvitiya predprinimatelskogo prava [Problems of formation of digital economy and issues of development of business law]. *Aktualnye problemy rossiyskogo prava*. 2018;11. (In Russ.)
2. Petrykina NI. Pravovoe regulirovanie oborota personalnykh dannykh. Teoriya i praktika [Legal regulation of personal data turnover. Theory and practice]. Moacow: Statut Publishing; 2011. (In Russ.)
3. Saveliev AI. Nauchno-prakticheskiy postateynyy kommentariy k Federalnomu zakonu «O personalnykh dannykh» [Scientific and practical annotated commentary to the Federal Law “On personal data”]. Moscow: Statut Publishing; 2017. (In Russ.)
4. Talapina EV. Zashchita personalnykh dannykh v tsifrovuyu epokhu. Rossiyskoe pravo v evropeyskom kontekste [Protecting personal data in the digital age. Russian Law in the European context]. *Proceedings of the RAS Institute of State and Law*. 2018;13(5). (In Russ.)