

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Юридический институт
кафедра международного права

УТВЕРЖДАЮ
Заведующий кафедрой
_____ Т. Ю. Сидорова
подпись инициалы, фамилия
«_____» _____ 2020 г.

БАКАЛАВРСКАЯ РАБОТА

40.03.01.01 «Международное и иностранное право»
код – наименование направления

Защита персональных данных: сравнительный аспект России и Германии
тема

Научный руководитель	_____	к.ю.н., доцент	В. В. Терешкова
	подпись, дата	должность, ученая степень	инициалы, фамилия
Выпускник	_____	16151003	М. А. Попов
	подпись, дата	номер зачетной книжки	инициалы, фамилия

Красноярск 2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	3
Глава 1. Общая характеристика персональных данных человека по законодательству России и Германии.....	7
1.1. Понятие персональных данных по законодательству России и Германии....	7
1.2. Персональные данные как элемент права на уважение частной жизни.....	28
Глава 2. Правовой механизм защиты персональных данных человека по законодательству России и Германии.....	34
2.1. Ограничения при обработке персональных данных	34
2.2. Гарантии защиты для субъекта персональных данных	53
2.3. Ответственность оператора за нарушение законодательства	60
ЗАКЛЮЧЕНИЕ	77
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	80

ВВЕДЕНИЕ

Человек в современном мире постоянно сообщает свои персональные данные. Люди покупают товары и услуги в сети Интернет, пользуются социальными сетями, заключают договоры с фирмами, имеющими базы данных своих клиентов, обращаются в государственные органы за получением государственных услуг. Все это неизбежно приводит к сообщению своих персональных данных и их последующей обработке. Даже простое посещение веб-страниц позволяет компаниям собирать информацию о человеке (например, в форме файлов-cookies, с дачей согласия на обработку которых людям приходится регулярно сталкиваться при посещении сайтов, особенно если эти сайты направлены на европейскую аудиторию). Современные системы автоматизированной обработки персональных данных позволяют из незначительных элементов составить довольно полный портрет человека. Поэтому защита персональных данных, в том числе и в правовом аспекте, имеет важное значение.

Об актуальности свидетельствует и опубликованный 08 июня 2020 года Федеральный закон «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации»¹, который создает единую базу данных, содержащую достаточно большой пласт сведений о всех гражданах России, а также иностранных гражданах и лицах без гражданства временно или постоянно проживающих в России.

По данным статистики, опубликованной на сайте Фонда общественного мнения, половина пользователей сети Интернет в России уверены, что их персональные данные плохо защищены². Между тем, неправомерный сбор и обработка персональных данных в ряде случаев не только сами по себе наносят вред праву человека на частную жизнь, но может причинить и материальный ущерб, если персональные данные будут использованы злоумышленниками.

¹ О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации [Электронный ресурс] : федер. закон от 08.06.2020 № 168-ФЗ // Справочная правовая система «КонсультантПлюс» - Режим доступа: <http://consultant.ru/>.

² Статистика по вопросу безопасности в интернете [Электронный ресурс] : официальный сайт Фонда общественного мнения – Режим доступа: <https://fom.ru/>

Нормативно-правовым актом, который в первую очередь призван обеспечивать защиту персональных данных, является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», который на сегодняшний день действует уже в двадцатой редакции. Кроме того, отдельные нормативные положения, посвященные данному вопросу, можно найти и в других законах, например, в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и других.

Так как большое количество пользователей сети Интернет не считают, что их персональные данные защищены, и нормативное регулирование, посвященное защите персональных данных, не является стабильным и окончательно систематизированным, можно сделать вывод о наличии определенных проблем в законодательстве. Поэтому опыт других стран может оказаться полезным и для российской правовой системы.

Немецкий механизм защиты персональных данных выбран для сравнения по нескольким причинам. Во-первых, согласно статистике 75% опрошенных граждан Германии доверяют тому, что их персональные данные будут использованы только в соответствии с указанными целями их обработки³.

Во-вторых, немецкое законодательство о защите персональных данных, несмотря на его историю, можно отнести к одним из самых современных и эффективных.

Правовое регулирование в Германии имеет богатые традиции в сфере регулирования обработки персональных данных (еще в 1970 году в немецкой федеральной земле Гессен был принят первый в мире закон «О защите персональных данных»⁴, а «старый» Федеральный закон о защите данных (BDSG-alt) действовал с 1990 по 2017 и имел всего четыре редакции).

Германия является членом Европейского союза, где в 1995 году была принята Директива о защите данных (Директива 95/46/ЕС), на смену которой в

³ Inwieweit stimmen Sie den folgenden Aussagen zum Thema Datenschutz und Sicherheit im Internet zu? [Электронный ресурс] : статистика по вопросу безопасности Интернета в Германии // Режим доступа: <https://de.statista.com/>

⁴ Горелихина О.А., Шлиньков А.А. Правовая защита персональных данных в Германии / О.А. Горелихина, А.А. Шлиньков // Вопросы экономики и права. – 2012. – № 3 – С. 27.

2016 году пришел Регламент Европейского Парламента и Совета Европейского Союза о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (Регламент 2016/679, вступил в силу 25 мая 2018 года), в литературе чаще называемый «General Data Protection Regulation» или Общий Регламент. Во исполнение данного регламента в Германии в 2017 году был принят «новый» Федеральный закон о защите данных (BDSG-neu).

Согласно статистике, опубликованной на сайте Европейского парламента, уже за первые полтора года действия Общего Регламента было рассмотрено 206 326 нарушений, взыскано штрафов на общую сумму 55 955 871 евро⁵.

Объектом работы являются общественные отношения в области защиты персональных данных в России и в Германии.

Предметом работы выступают определение понятия персональных данных в международных актах и актах Европейского союза, в национальных российской и немецкой правовых системах, а также содержательная характеристика правового механизма защиты персональных данных, включая гарантии для субъектов, чьи данные подвергаются обработке, ограничения для операторов, и их ответственность за нарушения законодательства о персональных данных.

Эмпирической базой данной работы являются российские и немецкие нормативно-правовые акты, решения национальных и международных судов, в том числе практика Европейского суда по правам человека и Суда Европейского союза, нормативно-правовые акты Европейского союза, международные конвенции, научные труды российских и иностранных авторов, а также статистические данные.

Цель работы – сравнительный анализ правовых механизмов защиты персональных данных в России и в Германии.

Для достижения данной цели поставлены следующие **задачи**:

⁵First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities [Электронный ресурс] – Режим доступа: <https://www.europarl.europa.eu>

а) определить, какие персональные данные попадают под защиту в российской и немецкой правовых системах;

б) разграничить понятия защиты персональных данных и защиты частной жизни;

в) установить, как ограничивается деятельность операторов при обработке персональных данных в России и в Германии;

г) определить объем и качество предоставленных гарантий для субъектов, чьи персональные данные подвергаются обработке;

д) установить механизм привлечения к ответственности операторов за нарушение законодательства о персональных данных, а также определить органы, контролирующие их деятельность.

К **методам**, которые были использованы при написании данной работы относятся следующие: диалектический, формально-логический, формально-догматический, сравнительно-правовой.

Структура работы представлена введением, двумя главами и заключением. В первой главе дается определение понятия персональных данных в российской и в немецкой правовых системах, а также проводится его разграничение с правом на защиту частной жизни. Вторая глава посвящена непосредственно сравнительному анализу правового механизма защиты персональных данных в России и в Германии, включая, в частности, принципы защиты персональных данных, права субъектов данных, обязанности и ограничения для операторов, ответственность операторов за несоблюдение законодательства. В заключении подводятся итоги работы, формируются окончательные выводы.

Глава 1. Общая характеристика персональных данных человека по законодательству России и Германии

1.1. Понятие персональных данных по законодательству России и Германии

Персональные данные включают в себя широкий перечень информации о человеке, поэтому, как отмечается в литературе, установить одинаковый правовой режим для данной сферы невозможно⁶, как невозможно и установление исчерпывающего перечня сведений, которые можно было бы отнести к персональным данным⁷, так как сущность категории правовых данных предполагает индивидуальный и ситуативный подход⁸.

Границы отнесения той или иной информации к персональным данным различаются на уровне как доктринальных подходов, так и законодательной позиции и судебной практики.

Согласно п. 1 статьи 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (ФЗ «О персональных данных») персональными данными является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)⁹.

Подобное определение содержится и в Конвенции о защите физических лиц при автоматизированной обработке персональных данных 1981 г.¹⁰ (в целях реализации обязательств по которой и был принят ФЗ «О персональных данных»). Согласно подпункту «а» статьи 2 «персональные данные» означают

⁶ Терещенко, Л.К. Модернизация информационных отношений и информационного законодательства : монография / Л.К. Терещенко. – Москва : ИНФРА-М, 2013 – С. 15.

⁷ Петрыкина, Н.И. Правовое регулирование оборота персональных данных. Теория и практика : монография / Н.И. Петрыкина. – Москва : Статут, 2011. – С. 22.

⁸ Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». /А.И. Савельев. – Москва : Статут, 2017. – С.24

⁹ О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 № 152-ФЗ ред. от 31.12.2017 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>

¹⁰ О защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс] : конвенция от 28.01.1981 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>

любую информацию об определенном или поддающемся определению физическом лице (субъект данных).

Интересным является то, что ФЗ «О персональных данных» до 2011 года содержал примерный перечень сведений, относимых к персональным данным («фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы»), а также предусматривал такой признак персональных данных, как возможность установить лицо «на основании такой информации». В последствии законодатель отошел от этого подхода и не стал расширять понятие, данное в Конвенции 1981 года.

Согласно одной из господствующих в последние годы точек зрения в литературе, только такое «широкое» определение персональных данных позволяет достичь целей защиты прав человека, охраны неприкосновенности частной жизни, личной и семейной тайны¹¹. Понятие персональных данных недопустимо толковать ограничительно. В современном мире человек постоянно сообщает сведения о себе, иногда даже не подозревая об этом. В некоторых случаях из таких, на первый взгляд даже незначительных сведений, с помощью особых способов обработки, можно создать полный портрет человека. В дальнейшем данная информация может быть использована в коммерческих и иных целях. Поэтому в случае наличия каких-либо сомнений в отнесении конкретной информации к персональным данным, необходимо считать такую информацию персональными данными. Представляется, что подобный подход в итоге может привести к презумпции отнесения любой информации о физическом лице к персональным данным.

Отметим, что действующее в настоящий момент определение, данное в ФЗ «О персональных данных», не предполагает связи между информацией и возможностью определения конкретного лица с помощью этой информации. Оно лишь говорит о том, что информация, составляющая персональные

¹¹ Грибанов, А.А. Общий регламент о защите персональных данных (General Data Protection Regulation): идеи для совершенствования российского законодательства / А.А Грибанов // Закон. – 2018. – № 3. – С. 153.

данные, относится к некоему физическому лицу. Таким образом, единственным критерием отнесения тех или иных сведений к персональным данным является их относимость к физическому лицу. При этом, согласно нормативному определению, не имеет значение, возможно ли с помощью этой информации определить субъекта персональных данных.

Таким образом, первая концепция предлагает считать любую информацию о физическом лице персональными данными, вне зависимости от того, возможно ли с помощью этой информации определить субъекта данных.

В соответствии с другой точкой зрения, также получившей распространение в доктрине и судебной практике, определение, данное в ФЗ «О персональных данных» является слишком широким и не соответствует установленному Конституционным Судом РФ принципу формальной определенности¹². Дело в том, что зачастую правоприменитель руководствуется только текстом нормативного правового акта, и, таким образом, на практике относит к персональным данным такую информацию, которая явно не соответствует разумным ожиданиям общества и конкретных лиц¹³. Данное утверждение является спорным, так как ограничительное толкование понятия, указанного в законе, при отсутствии установленного перечня сведений, относимых к персональным данным, а также при отсутствии точного критерия или теста по установлению этих сведений, не добавляет определенности правовому регулированию и, следовательно, не соответствует принципу правовой определенности.

В этом отношении является интересной практика США, где на законодательном уровне установлен закрытый перечень сведений, которые в совокупности могут являться персональными данными. Однако, как отмечается

¹²См., например, Определение Конституционного Суда РФ от 17 июня 2013 г. № 979-О // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>

¹³ Приезжева, А.А. Федеральный закон «О персональных данных»: научно-практический комментарий. / А.А. Приезжева. – Москва : Редакция «Российской газеты», 2015. – № 11. – С.15.

в литературе, в современных условиях охватить все персональные данные закрытым перечнем вряд ли удастся¹⁴.

Сторонники ограничительного толкования понятия персональных данных считают, что для того, чтобы отнести какую-либо информацию к персональным данным, необходимо ввести еще один дополнительный признак этой информации, а именно ее необходимость и достаточность для идентификации лица¹⁵.

Корни ограничительного толкования понятия персональных данных в части сведений, которые к ним относятся, можно найти в Указе Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»¹⁶. В нем под персональными данными понимаются только такие сведения о фактах, событиях и обстоятельствах частной жизни гражданина, которые позволяют идентифицировать его личность.

Однако это не предполагает включение в круг персональных данных только той информации, которая получена из документов, удостоверяющих личность. К ее числу даже сторонники ограничительного толкования понятия персональных данных относят достаточно широкий перечень сведений.

Подтверждение этому можно найти в судебной практике. Суды и на сегодняшний день продолжают идти по пути ограничительного толкования определения понятия персональных данных, существовавшего ранее в ФЗ «О персональных данных»¹⁷. В качестве примера, что не любая информация о физическом лице будет являться его персональными данными, можно привести постановление Президиума Высшего арбитражного суда РФ от 5 октября 2010

¹⁴Фомина Л.Ю. Международные стандарты защиты персональных данных в условиях информационного общества / Л. Ю. Фомина // Международное право. – 2019. – № 4. – С. 54.

¹⁵Приезжева, А.А. Федеральный закон «О персональных данных»: научно-практический комментарий. / А.А. Приезжева. – Москва : Редакция «Российской газеты», 2015. – № 11. – 176 с.

¹⁶Об утверждении перечня сведений конфиденциального характера [Электронный ресурс] : указ Президента РФ от 06.03.97 № 188 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>

¹⁷Грибанов, А.А. Общий регламент о защите персональных данных (General Data Protection Regulation) : идеи для совершенствования российского законодательства / А.А Грибанов // Закон. – 2018. – № 3. – С. 152.

г. № 6336/10. Изложенные в нем правовые позиции применяются арбитражными судами по настоящее время.

Так, ОАО «Вымпел-Коммуникации» обратилось в суд с заявлением о признании незаконным и отмене постановления о привлечении общества к административной ответственности за то, что общество отказалось предоставить по требованию судебного пристава-исполнителя номер мобильного телефона должника. Президиум ВАС РФ удовлетворил требования заявителя в полном объеме.

Свое решение Президиум ВАС РФ мотивировал следующим образом. В соответствии со ст. 53 ФЗ «О связи»¹⁸ сведения об абонентах являются конфиденциальной информацией и защищаются на основе законодательства РФ. Сведения об абонентах-гражданах без их согласия могут передаваться в силу статьи 64 ФЗ «О связи» только государственным органам, осуществляющим оперативно-розыскную деятельность или занимающимся вопросами обеспечения безопасности Российской Федерации. Далее суд указал, что сведения об абонентах «содержат» персональные данные, то есть исходя из буквального толкования, сведения об абонентах не исчерпываются одними лишь персональными данными.

Поскольку доступ к сведениям об абонентах-гражданах и к их персональным данным является ограниченным, то на основании ст. 9 ФЗ «Об информации, информационных технологиях и о защите информации»¹⁹ соблюдение конфиденциальности такой информации является обязательным.

Анализ позиции Высшего арбитражного суда РФ позволяет сделать вывод, что персональными данными является не любая информация, относящаяся к физическому лицу. Как видим, не все сведения об абонентах будут являться персональными данными, равно как и не все персональные данные будут являться сведениями об абонентах. Однако вся эта информация

¹⁸ О связи [Электронный ресурс] : федер. закон от 07.07.2003 № 126-ФЗ ред. от 18.04.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>

¹⁹ Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ ред. от 03.04.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>

будет являться конфиденциальной, иметь ограниченный доступ и защищаться на основании законодательства РФ.

Суд сослался на действующее в тот момент в ФЗ «О персональных данных» определение понятия персональных данных, и перечислил круг информации, относящейся к персональным данным физического лица, а именно его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, имущественное, семейное, социальное положение, образование, профессия, доходы, другая информация.

В качестве примеров того, что суды РФ уже после изменений в ФЗ «О персональных данных», стали относить к персональным данным, можно привести следующие.

а) Паспортные данные гражданина. Судом установлена правомерность отказа начальника отдела МВД России в предоставлении паспортных данных граждан лицу, которое требовало их без законных оснований²⁰.

В другом деле суд также признал паспортные данные лица персональными данными. Однако в удовлетворении исковых требований к оператору персональных данных было отказано, потому что работник разгласил их в своей научной работе, а не во время трудовой деятельности²¹.

Однако в практике судов нет однозначного мнения, будут ли относиться к персональным данным сами по себе такие сведения, как серия и номер паспорта.

В одном из дел суд указал, что серия и номер паспорта относятся не к личности самого гражданина, а к бланку документа, удостоверяющего личность, поэтому не являются персональными²². В другом деле суд рассматривал иск гражданина о незаконном размещении его серии и номера

²⁰ Апелляционное определение Московского городского суда от 22 мая 2014 по делу № 33-14709 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

²¹ Апелляционное определение Московского городского суда от 16 ноября 2016 г. по делу № 33-45367/2016 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

²² Постановление Тринадцатого арбитражного апелляционного суда от 21 июня 2010 г. по делу № А56-4788/2010 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

паспорта в одном из решений на официальном сайте арбитражного суда. Суд пришел к выводу, что в соответствии с пунктом 3 описания бланка паспорта гражданина РФ²³, утвержденного постановлением Правительства РФ от 8 июля 1997 г. № 828, бланк паспорта имеет нумерацию, которая состоит из трех групп цифр и обозначает серию бланка и номер бланка паспорта, следовательно, указанная информация не относится к личности гражданина и поэтому не может являться персональными данными²⁴. Однако практика не отнесения серии и номера паспорта к персональным данным не является устоявшейся (см., например, ниже пункт «б»).

Вышеуказанные позиции представляются недостаточно обоснованными, так как несмотря на то, что серия и номер паспорта относятся к бланку документа, сам документ удостоверяет конкретную личность, неразрывно связан с ней и не может быть использован по назначению другим человеком. Кроме того, указанные сведения являются уникальными и актуальными в течение достаточно продолжительного времени, что в совокупности свидетельствует о необходимости защиты их как персональных данных.

б) Идентификационный номер налогоплательщика и страховой номер индивидуального лицевого счёта. В решении Красноярского краевого суда к персональным данным отнесены как данные документа, удостоверяющего личность гражданина, включая серию, номер, дату выдачи, наименование органа, выдавшего документ, так и сведения об идентификационном номере налогоплательщика²⁵. В качестве аргумента суд привел пункт 1.3 Инструкции о порядке обработки в органах прокуратуры Российской Федерации

²³Описания бланка паспорта гражданина РФ [Электронный ресурс] : утв. постановлением Правительства РФ от 8.07.1997 г. № 828 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

²⁴ Определение судебной коллегии по гражданским делам Московского городского суда от 29 февраля 2012 г. № 33-6709 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

²⁵ Решение Красноярского краевого суда № 7П-428/2017 от 14 сентября 2017 г. по делу № 7П-428/2017 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

персональных данных, полученных в связи с осуществлением прокурорского надзора²⁶, где подобные сведения отнесены к персональным данным граждан.

Арбитражный суд Красноярского края утвердил перечень персональных данных, которые обрабатываются в суде. В этом перечне есть и реквизиты паспорта, и идентификационный номер налогоплательщика, и страховой номер индивидуального лицевого счета²⁷.

Однако и в этом случае практика не является устоявшейся и однозначной. Так, суд указал, что идентификационный номер налогоплательщика не содержит в себе какой-либо персональной информации личного характера, которая бы относилась к конкретному физическому лицу, поскольку данный номер используется исключительно в целях налогового учета и не заменяет имя человека²⁸.

Данные разногласия постаралось разрешить Министерство финансов РФ, прямо указав в письме, что индивидуальный номер налогоплательщика не является информацией, входящей в перечень персональных данных, и он применяется только для целей учета налогоплательщиков и в их интересах²⁹. Однако Роскомнадзор в своих разъяснениях традиционно максимально широко толкует понятие персональных данных, включая в него и вышеназванные сведения³⁰.

В ситуации отсутствия однозначного решения данной проблемы, суд должен принимать решение на основе обстоятельств каждого конкретного дела.

²⁶ Инструкция о порядке обработки в органах прокуратуры Российской Федерации персональных данных, полученных в связи с осуществлением прокурорского надзора [Электронный ресурс] : утв. приказом Генерального прокурора Российской Федерации от 22.11.2013 г. №506 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

²⁷ Об обработке персональных данных в Арбитражном суде Красноярского края [Электронный ресурс] :приказ от 05.06.2018 № 93 – Режим доступа: <https://krasnoyarsk.arbitr.ru/>.

²⁸ Апелляционное определение Санкт-Петербургского городского суда № 2-3097/2014 33-1644/2015 от 3 февраля 2015 г. по делу № 2-3097/2014[Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

²⁹ О присвоении физлицу ИНН и его применении [Электронный ресурс] : письмо Министерства финансов № 03-01-11/76554 от 25.10.2018// Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

³⁰ Разъяснения Роскомнадзора по вопросу применения законодательства о персональных данных // [Электронный ресурс] – Режим доступа: <https://rkn.gov.ru/>.

в) Сведения о пересечении государственной границы³¹. Гражданин обратился в ФМС России с требованием предоставить ему сведения о пересечении государственной границы другим лицом. ФМС России отказала предоставлять указанные сведения, сославшись на то, что эти сведения подлежат разглашению только в случаях, предусмотренных ФЗ «О персональных данных». Суд посчитал действия ФМС России правомерными.

г) Информация о трудовой деятельности³². Судом установлено, что информация о трудовой деятельности судьи, наряду с иной информацией, также относится к персональным данным и для ее раскрытия необходимо получение согласия субъекта персональных данных.

д) Адрес проживания и размер долга по оплате коммунальных платежей³³. Суд признал нарушающим требования ФЗ «О персональных данных» передачу сведений управляющей компании третьему лицу о физических лицах, имеющих задолженность по оплате коммунальных платежей, в которых сообщались адрес проживания и размер долга указанных лиц.

е) Сведения, содержащиеся в пенсионном деле гражданина³⁴. В данном деле адвокат требовал признать неправомерным отказ Управления Пенсионного фонда Российской Федерации предоставить по адвокатскому запросу пенсионное дело гражданина, которому он оказывал юридические услуги. Суд признал отказ Управления Пенсионного фонда Российской Федерации правомерным, так как адвокатский запрос не порождает для органов безусловной обязанности предоставить сведения, в любом случае предоставление адвокату информации должно не противоречить другим законам, в частности регулирующим предоставление информации.

³¹ Апелляционное определение Московского городского суда от 10.04.2014 № 33-11688 [Электронный ресурс] – Режим доступа: <https://www.mos-gorsud.ru/>.

³² Решение Верховного Суда РФ от 11.03.2013 № АКПИ13-61 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

³³ Постановление Нижегородского областного суда от 12 мая 2015 г. № 4а-288/2015 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

³⁴ Определение Приморского краевого суда № 33-11759/2014 33-470/2015 от 19 января 2015 г. [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

Однако суд не указал, какие именно сведения, содержащиеся в пенсионном деле гражданина, он посчитал персональными данными.

ж) Сведения, содержащиеся в техническом паспорте на многоквартирный дом³⁵. Гражданин обжаловал отказ отделения филиала ФГУП «Ростехинвентаризация-Федеральное БТИ» в предоставлении ему технического паспорта на весь многоквартирный дом, в котором находилась его квартира. Суд признал отказ правомерным.

Однако ситуация в этом деле похожа на указанное в предыдущем пункте решение про пенсионное дело гражданина: суд не раскрывал, какие именно сведения из технического паспорта будут являться персональными данными. Он лишь перечислил сведения, содержащиеся в техническом паспорте, а именно «фамилия, имя и отчество, паспортные данные, полное наименование юридического лица, документы, подтверждающие право собственности». Очевидно, что, наименование юридического лица, не может быть отнесено к персональным данным, потому что субъектом данных по российскому законодательству является исключительно физическое лицо.

в) Адрес электронной почты³⁶. Суд к персональным данным отнес адрес электронной почты лица, который был указан наряду с другими персональными данными. В другом деле суд указал, что адрес электронной почты в совокупности с указанным при регистрации телефонным номером относится к персональным данным³⁷. Данный вопрос является достаточно спорным³⁸. В ряде решений³⁹ суды указывают, что адрес электронной почты не относится к

³⁵ Определение Приморского краевого суда от 28 апреля 2014 г. по делу № 33-3718 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

³⁶ Апелляционное определение Санкт-Петербургского городского суда от 31.01.2017 № 33а-1151/2017 по делу № 2а-4760/2016 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>

³⁷ Апелляционное определение Новосибирского областного суда от 27 сентября 2016 г. № 33-9626/2016 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

³⁸ Жердина, С.Ю., Двенадцатова, Т.И. Защита персональных данных: первые итоги и перспективы судебных дел / С.Ю. Жердина, Т.И. Двенадцатова // Журнал «Акционерное общество» – 2017. – №11. – С. 73–79.

³⁹ См., например, решение Заельцовского районного суда г. Новосибирска № 2-1770/2018 2-1770/2018 ~ М-987/2018 М-987/2018 от 27 июня 2018 г. по делу № 2-1770/2018, Апелляционное определение Московского городского суда от 12.12.2016 по делу № 33-42101/2016

персональным данным, поскольку не позволяет идентифицировать субъекта персональных данных, а является лишь средством передачи данных.

Еще больше усложнило решение данного вопроса внесение изменений от 13 сентября 2019 г. в Постановление Правительства РФ от 30 июня 2018 г. № 772⁴⁰. Данным постановлением утвержден состав сведений, размещаемых в единой информационной системе персональных данных, к числу которых теперь добавлен и адрес электронной почты.

Интересным является Постановление Тринадцатого арбитражного апелляционного суда⁴¹. Суд постановил, что указание при регистрации на онлайн-ресурсе таких сведений, как адрес электронной почты, дата рождения и даже имя, фамилия и отчество, не попадает под действие ФЗ «О персональных данных», так как владелец данного онлайн-ресурса не проверяет правильность и точность указанных пользователем сведений. Эта информация не является персональными данными, так как не соответствует указанному в пункте 6 статьи 5 ФЗ «О персональных данных» принципу точности.

Нельзя согласиться с данным выводом суда, так как требование пункта 6 статьи 5 ФЗ «О персональных данных» направлено к оператору – он должен обеспечивать точность персональных данных. Кроме того, подобная трактовка позволяет недобросовестным лицам, осуществляющим обработку персональных данных, ссылаться на то, что они не устанавливают точность сообщаемых им данных, следовательно, они могут распоряжаться этими сведениями без ограничений, установленных ФЗ «О персональных данных». По сути, любой онлайн-ресурс не может проверить сообщаемые ему данные, поэтому вынесенное Тринадцатым арбитражным апелляционным судом

⁴⁰ 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 [Электронный ресурс] : постановление Правительства РФ от 30.06.2018 № 772 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

⁴¹ Постановление Тринадцатого арбитражного апелляционного суда от 01.06.2015 № 13АП-10709/2015 по делу № А56-75017/2014[Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

постановление по данному делу идет в разрез с существующей практикой и не соответствует законодательному регулированию.

г) IP-адрес (решение Арбитражного суда Челябинской области по делу № А76-29008/2015 от 11.02.2016⁴²). При этом в других делах, суды не признают IP-адрес персональными данными⁴³.

Отдельно необходимо затронуть вопрос отнесения изображения гражданина к персональным данным. Практика судов в данном вопросе в большей части устоявшаяся: изображение гражданина к персональным данным не относится⁴⁴. При этом, Роскомнадзор дал разъяснения⁴⁵, что изображение гражданина, содержащееся, например, в паспорте, является биометрическим персональным данным этого гражданина. Однако важным аспектом квалификации изображения гражданина как персональных данных является цель, с которой оно используется. Если целью является установление личности гражданина, как в случае с пропуском на определенный объект, то в данном случае изображение будет являться персональным данным, а если сотрудник банка сканирует паспорт гражданина с целью заключения договора, данные действия с изображением человека не будут являться обработкой данных. Также персональными данными не являются рентгеновские или флюорографические снимки до тех пор, пока они не будут использованы операторами, например, органами следствия и дознания, в целях установления личности конкретного лица.

Раскрытие в полном объеме понятия персональных данных невозможно без определения того, кто является субъектом персональных данных. В статье 3

⁴²Решение Арбитражного суда Челябинской области по делу № А76-29008/2015 от 11.02.2016 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

⁴³Постановление Тринадцатого арбитражного апелляционного суда от 01.06.2015 № 13АП-10709/2015 по делу № А56-75017/2014 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

⁴⁴Решение Октябрьского районного суда г. Красноярска № 2-3904/2019 2-3904/2019~М-966/2019 М-966/2019 от 26 августа 2019 г. по делу № 2-3904/2019, Апелляционное определение Санкт-Петербургского городского суда от 15.11.2016 № 33-22976/2016 по делу № 2-2932/2015

⁴⁵О вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки [Электронный ресурс] : разъяснения Роскомнадзора – Режим доступа: <https://rkn.gov.ru/>

ФЗ «О персональных данных» к субъекту персональных данных отнесены физические лица. Очевидно, что эта формулировка исключает юридических лиц: они не могут быть субъектами данных. Однако в таком случае возникает вопрос, попадают ли сведения об индивидуальных предпринимателях под определение понятия персональных данных. Судебная практика решает этот вопрос однозначно и логично: так как индивидуальным предпринимателем является гражданин, то есть физическое лицо, то и сведения о нем являются персональными данными этого гражданина. Так, суд обязал убрать с сайта администрации адреса места жительства индивидуальных предпринимателей, указанные в плане проведения проверок, так как признал эти сведения персональными данными⁴⁶.

Интересной представляется позиция Конституционного Суда РФ, рассматривавшего вопрос о принятии жалобы гражданина, являющегося индивидуальным предпринимателем, который хотел, чтобы из общедоступных сведений Единого государственного реестра индивидуальных предпринимателей исключили данные о его фамилии, имени, отчестве и дате рождения⁴⁷. Конституционный Суд РФ среди прочего указал, что в данном случае приоритет следует отдать публичности реестра, что обеспечивает стабильный гражданский оборот. Кроме того, ФЗ «О персональных данных» допускает в случаях, предусмотренных законом, обработку персональных данных без согласия субъекта, а Федеральный закон «О государственной регистрации юридических лиц и индивидуальных предпринимателей» как раз относится к числу таких законов.

Регулирование сферы персональных данных в Германии осуществляется многими нормативно-правовыми актами как на национальном уровне, так и на международном и уровне Европейского союза.

⁴⁶ Апелляционное определение Волгоградского областного суда от 24.04.2014 № 33-4427/2014 [Электронный ресурс] // Интернет-ресурс Судебные и нормативные акты РФ – Режим доступа: <http://www.sudact.ru/>

⁴⁷ Определение Конституционного суда РФ от 17 июля 2012 г. № 1346-О [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>

Германия, как и Россия, ратифицировала Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981 года⁴⁸, следовательно, обязана соблюдать ее положения.

Кроме того, к нормативно-правовым актам, создающим обязательные для всех правила поведения, в том числе для граждан и юридических лиц, относятся наравне с национальным немецким законодательством еще и право Европейского союза⁴⁹. Проанализировав статью 249 Договора об учреждении Европейского сообщества⁵⁰, можно сделать вывод о том, что основными источниками права Европейского союза являются регламенты, директивы и решения, при этом наивысшей юридической силой обладает регламент. Как указано в статье, он подлежит прямому применению во всех государствах-членах. В области защиты персональных данных таковым является Общий регламент о защите персональных данных (Datenschutz-Grundverordnung, более распространенным является его английское наименование: General Data Protection Regulation⁵¹). Также на уровне Европейского союза действует Хартия основных прав, статья 8 которой закрепляет право на защиту персональных данных⁵².

В связи с тем, что в Германии сложилось сильное федеративное территориальное устройство, наряду с нормативно-правовыми актами федерации по вопросу регулирования персональных данных граждан

⁴⁸О защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс] : конвенция от 28.01.1981 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>

⁴⁹Миндубаев, Р. Р. Полномочия ЕС по принятию собственных правовых актов / Р. Р. Миндубаев // Актуальные проблемы права: материалы междунар. науч. конф. /Ваш полиграфический партнер – Москва, 2011. – С. 132.

⁵⁰Договор, учреждающий Европейское Сообщество [Электронный ресурс] : от 25.03.1957 с изм. от 16.04.2003 // Право Европейского Союза – Режим доступа: <https://eulaw.ru/>

⁵¹Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронный ресурс] – Режим доступа: <https://dsgvo-gesetz.de/>

⁵² Хартия Европейского союза об основных правах [Электронный ресурс] : от 07.12.2000 // Право Европейского Союза – Режим доступа: <https://eulaw.ru/>

существуют и акты земель, например, Закон о защите персональных данных земли Баварии (Bayerisches Datenschutzgesetz⁵³).

В числе основных нормативно-правовых актов, регулирующих персональные данные в Германии, можно выделить:

а) Регламент (EU) 2016/679 «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46/ЕС»⁵⁴ (Общий Регламент о защите персональных данных / General Data Protection Regulation (англ.) / Datenschutz-Grundverordnung (нем.) (далее – «Общий Регламент»);

б) Директива (EU) 2016/680 «О защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования уголовных преступлений, ведения розыскных или судебных действий или исполнения уголовных наказаний, а также за свободное перемещение таких данных и отменяя Рамочное решение Совета 2008/977 / JHA»⁵⁵;

в) Bundesdatenschutzgesetz⁵⁶ (Федеральный закон о защите данных);

г) законодательство земель.

Общий Регламент вступил в силу 25 мая 2018 г, отменив действовавшую с 1995 года Директиву № 95/46/ЕС Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных», существенно изменив сферу персональных данных и ужесточив отдельные положения, касающиеся защиты персональных данных.

⁵³ Bayerisches Datenschutzgesetz (BayDSG) [Электронный ресурс] : от 15.05.2018 // Bayern.Recht – Режим доступа: <https://www.gesetze-bayern.de/>

⁵⁴ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронный ресурс] – Режим доступа: <https://dsgvo-gesetz.de/>

⁵⁵ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [Электронный ресурс] // EUR-Lex – Режим доступа: <https://eur-lex.europa.eu/>

⁵⁶ Bundesdatenschutzgesetz (BDSG) [Электронный ресурс] // Gesetze im Internet – Режим доступа: <https://www.gesetze-im-internet.de/>

В отличие от российской системы, где границы понятия персональных данных в настоящий момент законодательно не установлены, а выводятся из доктрины и правоприминительной практики, из текста нормативно-правовых актов ЕС и Германии можно установить, что относится к персональным данным.

Согласно пункту 1 статьи 4 Общего Регламента⁵⁷ под персональными данными понимается любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу («субъект данных»). Идентифицируемым лицом считается любое физическое лицо, которое может быть прямо или косвенно идентифицировано. Соответственно, Общий Регламент вводит такой признак персональных данных, как возможность идентификации конкретного лица с помощью этих данных. Данная характеристика персональных данных, как было указано ранее, используется также и в российской доктрине. Кроме того, в пункте 26 Преамбулы к Общему Регламенту указано, что под его защиту не попадает анонимная информация, то есть та, с помощью которой невозможно установить конкретное лицо. При этом сведения, подвергнутые псевдонимизации, подлежат защите. Стоит отметить, что понятия анонимной информации нет в ФЗ «О персональных данных»⁵⁸.

Для определения того, возможно ли идентифицировать субъекта с помощью конкретных сведений учитывается в том числе время, необходимое для идентификации, имеющиеся технологии обработки и другое⁵⁹.

Идентификация в соответствии с Общим Регламентом возможна с помощью идентификатора или особых признаков, идентифицирующих личность.

⁵⁷ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронный ресурс] – Режим доступа: <https://dsgvo-gesetz.de/>

⁵⁸ Фомина Л.Ю. Международные стандарты защиты персональных данных в условиях информационного общества / Л. Ю. Фомина // Международное право. – 2019. – № 4. – С. 58

⁵⁹ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронный ресурс] – Режим доступа: <https://dsgvo-gesetz.de/>

К идентификатору, в частности, относятся имя, идентификационный номер, данные о местоположении, онлайн-идентификатор. Под идентификационным номером может пониматься страховой номер индивидуального лицевого счета, личный идентификационный номер или номер удостоверения личности⁶⁰. В практике российских судов, как было указано выше, подобные данные зачастую не рассматриваются в качестве персональных.

Согласно п. 30 преамбулы к Общему Регламенту под онлайн-идентификатором понимаются IP-адреса, файлы cookie, а также другие идентификаторы, в т.ч. метки радиочастотной идентификации, с которыми могут быть ассоциированы физические лица.

Онлайн-идентификаторы предоставляются устройствами пользователей, приложениями, программами и протоколами. Они могут оставить следы, которые особенно при комбинации с уникальными идентификаторами и другой информацией, получаемой серверами, могут быть использованы для создания профилей физических лиц и для их идентификации⁶¹. Под созданием профиля физического лица в п. 4 ст. 4 Общего Регламента понимается любой вид автоматизированной обработки персональных данных, заключающийся в том, что персональные данные используются для оценки определенных личных аспектов, относящихся к физическому лицу, в частности для анализа или прогнозирования аспектов его работы, экономического положения, здоровья, личных предпочтений, интересов, надежности, поведения, места жительства или смены местоположения⁶².

⁶⁰ Paul Voigt, Axel von dem Bussche. EU-Datenschutz-Grundverordnung (DSGVO) : Praktikerhandbuch / Paul Voigt, Axel von dem Bussche–Berlin –Springer,2018 – С. 14.

⁶¹Грибанов, А.А. Общий регламент о защите персональных данных (GeneralDataProtectionRegulation) : идеи для совершенствования российского законодательства / А.А Грибанов // Закон. – 2018. – № 3. – С. 151.

⁶²Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронныйресурс] – Режимдоступа: <https://dsgvo-gesetz.de/>

В практике суда Европейского союза IP-адреса еще до принятия Общего Регламента признавались персональными данными⁶³. Бесспорно решался вопрос относительно статических IP-адресов, однако в отношении динамических IP-адресов (которые меняются после каждого выхода в сеть) практика не была устоявшаяся. В 2016 г в деле Брейер против Германии⁶⁴ суд ЕС признал, что динамические IP-адреса могут рассматриваться в качестве персональных данных, если имеется какая-либо дополнительная информация о лице, которая в совокупности с IP-адресом позволяет идентифицировать человека. Это совпадает с подходом, который закреплен в Общем Регламенте.

Таким образом, сами IP-адреса или файлы cookie на уровне Европейского союза рассматриваются в качестве персональных данных, особенно в случае их комбинации с уникальными идентификаторами и другой информацией. В российской правоприменительной практике IP-адреса в большинстве случаев, как было указано выше, не признаются персональными данными.

Под особенным признаком, идентифицирующим личность понимаются, в частности, такие физические, физиологические, генетические, психические, экономические, культурные и социальные факторы, которые являются выражением индивидуальности данной личности⁶⁵.

Согласно Общему Регламенту, данные, чтобы попасть под сферу действия этого акта, должны быть «персонализированными», то есть относиться к физическому лицу⁶⁶.

В Общем Регламенте, так же, как и в ФЗ «О персональных данных», выделяется специальная категория персональных данных, обработка которых допустима только в прямо предусмотренных случаях. К таким данным отнесены расовая и этническая принадлежность, вероисповедание,

⁶³ Judgment of the Court (Third Chamber) 24 November 2011 in Case C-70/10 [Электронный ресурс] – Режим доступа: <http://curia.europa.eu/>

⁶⁴ Judgment of the Court (Second Chamber) 19 October 2016 [Электронный ресурс] // EUR-Lex – Режим доступа: <https://eur-lex.europa.eu/>

⁶⁵ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронный ресурс] – Режим доступа: <https://dsgvo-gesetz.de/>

⁶⁶ Paul Voigt, Axel von dem Bussche. EU-Datenschutz-Grundverordnung (DSGVO) : Praktikerhandbuch / Paul Voigt, Axel von dem Bussche – Berlin – Springer, 2018 – С. 13.

философские воззрения, политические взгляды, информация о здоровье, половой жизни и сексуальной ориентации, членство в профсоюзе, биометрические и генетические данные. В ФЗ «О персональных данных» к специальной категории персональных данных относятся, в целом, те же самые сведения, за исключением сексуальной ориентации и генетических данных. Кроме того, биометрические персональные данные по российскому законодательству отнесены не к «специальной категории данных», а вынесены в отдельную категорию.

Интересным образом решается вопрос об отнесении изображения субъекта к его персональным данным. В российском законодательстве, как уже отмечалось, данный вопрос регулируется только на уровне судебной практики и разъяснений Роскомнадзора. В пункте 14 статьи 4 Общего Регламента, изображения субъекта отнесены в числе прочих данных к биометрическим персональным данным. Однако в пункте 51 Преамбулы к Общему Регламенту поясняется, что изображения человека являются персональными данными только в том случае, если они обрабатываются с использованием специальных технических средств, делающих возможной однозначную идентификацию субъекта данных⁶⁷, что, в целом, соответствует позиции Роскомнадзора⁶⁸.

Таким образом, Общий Регламент устанавливает определенные критерии для отнесения тех или иных данных к персональным, чего нет в российском законодательстве. Однако нельзя сказать, что Общим Регламентом в этом смысле сужается широкое определение понятия персональных данных, данное в Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981 года⁶⁹. Очерчивая достаточно широкие границы понятия персональных данных, Общий Регламент сокращает

⁶⁷ Грибанов, А.А. Общий регламент о защите персональных данных (General Data Protection Regulation) : идеи для совершенствования российского законодательства / А.А. Грибанов // Закон. – 2018. – № 3. – С. 153..

⁶⁸ О вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки [Электронный ресурс] : разъяснения Роскомнадзора – Режим доступа: <https://rkn.gov.ru/>

⁶⁹ О защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс] : конвенция от 28.01.1981 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>

пространство для возможного ограничительного толкования данного положения со стороны правоприменителей, что в свою очередь ведет к большей правовой определенности.

Основным законом, регулирующим персональные данные, является «новый» Федеральный закон о защите данных⁷⁰ (BDSG-neu), который вступил в силу 25 мая 2018 года одновременно с Общим Регламентом. В связи с этим, большая часть его положений полностью совпадают с нормами Общего регламента, в том числе и касательно понятия персональных данных (параграф 46 Федерального закона о защите данных). В абзаце 5 параграфа 1 сказано, что положения этого закона не применяются в той степени, в какой непосредственное применение имеет Общий Регламент.

Немецкое законодательство о защите персональных данных под субъектом персональных данных также не подразумевает юридическое лицо. Персональными данными, в таком случае, будет являться только та информация, которая хоть и относится к юридическому лицу, но при этом тесно связана с физическим лицом (например, сведения о размере доли участника или его функции в юридическом лице)⁷¹. Тем не менее, и из этого правила есть исключение: если в юридическом лице только один участник, то не может идти речи о персональных данных, так как в таком случае невозможно разделить данные, относящиеся только к юридическому лицу, и данные, относящиеся к физическому.

Висбаденский административный суд в 2008 году постановил, что правовые положения о защите данных, соответственно, применяются и к юридическим лицам в той мере, в какой это установлено конституционным правом на информационное самоопределение⁷².

⁷⁰Bundesdatenschutzgesetz (BDSG) [Электронный ресурс] // Gesetze im Internet – Режим доступа: <https://www.gesetze-im-internet.de/>

⁷¹Paul Voigt, Axel von dem Bussche. EU-Datenschutz-Grundverordnung (DSGVO) : Praktikerhandbuch / Paul Voigt, Axel von dem Bussche – Berlin – Springer, 2018 – С. 25.

⁷² Verwaltungsgericht Wiesbaden am 18. Januar 2008 (AZ 6 E 1559/06) [Электронный ресурс] – Режим доступа: <https://openjur.de/>

Исходя из анализа российского законодательства и правоприменительной практики, можно сделать следующие выводы:

а) вопреки положениям ФЗ «О персональных данных» в правоприменительной практике понятие персональных данных и на сегодняшний день продолжает трактоваться ограничительно. Под персональными данными, согласно этой позиции, понимаются сведения о физическом лице, наличие которых достаточно для идентификации его личности;

б) к персональным данным судами зачастую относится совокупность сведений о человеке, при этом суды не указывают, какие именно данные они посчитали персональными, а какие просто содержатся в том же документе, доступ к которому является предметом спора;

в) суды действуют осторожно, приводя широкий перечень сведений, являющихся предметом конкретного разбирательства, при этом включая в него и информацию, явно несоответствующую требованиям ФЗ «О персональных данных»;

г) зачастую, чтобы судом был применен ФЗ «О персональных данных», речь в деле должна идти о совокупности фамилии, имени (отчестве) и других данных о человеке;

д) нельзя с точностью сказать, что какое-то сведение в отдельности и даже определенная совокупность сведений может быть отнесена судом к персональным данным. Все будет зависеть от обстоятельств конкретной ситуации.

В связи с формальной неопределенностью понятия персональных данных (даже не установлены примерные его границы) в этой сфере образуется широкий простор для судебного усмотрения: признание того или иного сведения о физическом лице персональным данным зависит от обстоятельств конкретного дела и является трудно предсказуемым на начальном этапе судебного разбирательства. Представляется не совсем верным отход законодателя от изначальной концепции определения примерного круга

персональных данных в тексте закона и возвращения понятия, существующего в Конвенции 1981 года. Современная ситуация ввиду огромного количества персональной информации и способов ее получения, а также возможности неконтролируемой ее передачи требует более точного регулирования в данном вопросе.

В немецком законодательстве, в отличие от российского, закрепляется такой признак персональных данных, как возможность идентификации с их помощью конкретного лица, устанавливается понятие онлайн-идентификатора, а также устанавливаются иные границы определения понятия персональных данных, что сужает пространство для судебного усмотрения и ведет к большей формальной определенности правовых норм.

Тем не менее, предполагается нецелесообразным полное ограничение права усмотрения правоприменителя в данном вопросе. Для правильного рассмотрения конкретного спора следует изначально исходить из широкого понимания персональных данных, то есть относить к ним всю информацию о человеке, однако в зависимости от обстоятельств конкретной ситуации у правоприменителя должна сохраняться возможность не применять режим защиты к определенным сведениям (или их совокупности) в интересах разумности и справедливости (например, если этих сведений окажется недостаточно даже для косвенного определения субъекта данных).

1.2. Персональные данные как элемент права на уважение частной жизни

В научной литературе и различных нормативно-правовых актах, как национальных, так и международных, употребляются различные термины, такие как «защита частной жизни»⁷³, «защита права на неприкосновенность

⁷³ Проскурякова, М.И. Персональные данные: российская и германская национальные модели конституционно-правовой защиты в сравнительной перспективе / М.И. Проскурякова // Сравнительное конституционное обозрение. – 2016 – № 6. – С. 87.

частной жизни»⁷⁴, «право на уважение частной жизни» и другие. Не вдаваясь в терминологическую дискуссию, в дальнейшем для описания правового явления, предметом защиты которого выступает частная жизнь человека, будет использован термин «защита частной жизни», по аналогии с рассматриваемым – «защита персональных данных».

В статье 8 Европейской конвенции о защите прав человека⁷⁵ установлено право каждого на уважение его личной и семейной жизни, его жилища и его корреспонденции. Европейский суд по правам человека в своей практике широко толкует понятие права на защиту частной жизни⁷⁶. Судом также подчеркивается, что невозможно дать исчерпывающее понятие самой частной жизни⁷⁷, ведь кроме прочего в содержание понятия частной жизни включается «внешний мир», который охватывает и некоторые социальные взаимодействия и профессиональную сферу деятельности лица⁷⁸.

В качестве критериев отнесения Европейским судом по правам человека той или иной деятельности к частной жизни можно выделить следующее. Во-первых, таковым выступает значимость конкретной деятельности для развития личности⁷⁹. Во-вторых, установить пределы защиты частной жизни помогает так называемый «тест на обоснованное ожидание неприкосновенности частной жизни»⁸⁰. Тест состоит из субъективной и объективной части. Субъективная

⁷⁴ Рузанова, В.Д. Проблемы соотношения защиты права на неприкосновенность частной жизни и права на защиту персональных данных / В.Д.Рузанова // Законы России: опыт, анализ, практика. – 2019. – № 9. – С. 19.

⁷⁵ Европейская конвенция о защите прав человека и основных свобод [Электронный ресурс] : принята 04.11.1950 в Риме // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

⁷⁶ Кротов, А.В. Концепция "широкого" толкования права на частную жизнь в решениях Конституционного Суда Российской Федерации / А.В. Кротов // Актуальные проблемы российского права.– 2018.– №5 (90)– С.82.

⁷⁷ Постановление Европейского Суда по правам человека по делу «Бигаева против Греции» [Bigaeva v. Greece] от 28 мая 2009 г.(жалоба № 26713/05)[Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

⁷⁸ Постановление Европейского Суда по правам человека по делу «Нимитц против Германии» [Niemietz v. Germany] от 16 декабря 1992 г. (жалоба № 13710/88) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

⁷⁹ Проскурякова, М.И. Персональные данные: российская и германская национальные модели конституционно-правовой защиты в сравнительной перспективе / М.И. Проскурякова // Сравнительное конституционное обозрение. – 2016 – № 6. – С. 87.

⁸⁰ Сыченко, Е. Прослушивание рабочего телефона, обыск служебных помещений и съемка работника на видео: практика Европейского суда по правам человека [Электронный ресурс] / Е. Сыченко //

включает в себя реальное ожидание конкретного лица на сохранение тайны его частной жизни в конкретной ситуации. Объективная часть состоит в готовности общества признать данное ожидание разумным.

Защита персональных данных согласно позиции Европейского суда по правам человека включается в право на уважение частной жизни только в случаях, когда эти данные относятся именно к частной жизни⁸¹.

На международном уровне в Резолюции Генеральной Ассамблеи ООН «Право на неприкосновенность частной жизни» рассматривается и проблема защиты персональных данных⁸².

В литературе высказывается точка зрения, рассматривающая право на защиту частной жизни как основное право, гарантирующее защиту персональных данных, ввиду большого потенциала для распространения его действия на данную сферу⁸³.

В российском законодательстве не определено понятие частной жизни гражданина. Право на неприкосновенность частной жизни, личную и семейную тайну установлено в статье 23 Конституции РФ⁸⁴, и в целом, сопоставимо с закрепленным в тексте Европейской конвенции по правам человека правом на уважение частной жизни⁸⁵. Согласно позиции Конституционного суда РФ, сформулированной в определениях № 2128-О⁸⁶, № 158-О-О⁸⁷, № 248-О⁸⁸, под

Административное право – № 1, – I квартал 2015 г. / Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

⁸¹ Проскурякова, М.И. Персональные данные: российская и германская национальные модели конституционно-правовой защиты в сравнительной перспективе / М.И. Проскурякова // Сравнительное конституционное обозрение. – 2016 – № 6. – С. 89.

⁸² Право на неприкосновенность частной жизни в цифровую эпоху [Электронный ресурс] : резолюция Генеральной Ассамблеи ООН № 73/179 от 17 декабря 2018 г. // Режим доступа: <https://undocs.org>.

⁸³ Проскурякова, М.И. Персональные данные: российская и германская национальные модели конституционно-правовой защиты в сравнительной перспективе / М.И. Проскурякова // Сравнительное конституционное обозрение. – 2016 – № 6. – С. 89.

⁸⁴ Конституция Российской Федерации [Электронный ресурс] : принята всенародным голосованием 12.12.1993 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

⁸⁵ Проскурякова, М.И. Персональные данные: российская и германская национальные модели конституционно-правовой защиты в сравнительной перспективе / М.И. Проскурякова // Сравнительное конституционное обозрение. – 2016 – № 6. – С. 90.

⁸⁶ Определение Конституционного Суда РФ от 24 декабря 2013 г. № 2128-О [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

⁸⁷ Определение Конституционного Суда РФ от 26 января 2010 года № 158-О-О [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

⁸⁸ Определение Конституционного Суда РФ от 9 июня 2005 года № 248-О [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

правом на неприкосновенность частной жизни, личную и семейную тайну понимается возможность человека контролировать информацию о себе и препятствовать разглашению сведений личного характера; причем само понятие «частная жизнь» относится только к отдельному человеку и не подлежит контролю со стороны государства и общества, если не носит противоправного характера.

Как отмечает А. И. Савельев в российской правовой системе правовое регулирование института защиты персональных данных приобрело самостоятельное значение и существует параллельно с институтом защиты частной жизни гражданина, несмотря на то, что истоки права на защиту персональных данных можно найти в праве на защиту частной жизни⁸⁹.

Похожее мнение высказывает И. А. Михайлова, что персональные данные по отдельности могут и не составлять охраняемую сферу частной жизни человека, однако в совокупности они становятся его социально-экономической характеристикой и, следовательно, подлежат защите⁹⁰.

Конституционный Суд РФ рассматривает персональные данные как один из видов охраняемой законом информации⁹¹. Так, в одном из своих определений⁹² Конституционный Суд РФ указал, что учреждение здравоохранения имеет право хранить информацию о человеке исключительно в целях реализации его права на охрану здоровья, при этом конфиденциальность информации обеспечивается врачебной тайной. Таким образом, Конституционный Суд РФ установил, что конфиденциальность персональных данных охватывается врачебной тайной, и, следовательно, право субъекта данных на удаление информации о нем не может быть реализовано.

⁸⁹ Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». / А.И. Савельев. – Москва : Статут, 2017. – С. 16.

⁹⁰ Михайлова, И.А. Персональные данные и их правовая охрана: некоторые проблемы теории и практики / И.А. Михайлова // Законы России: опыт, анализ, практика. –2017. – № 10. –С. 13.

⁹¹ Талапина, Э. В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте. / Э. В. Талапина // Труды Института государства и права РАН. – 2018. – Т.13, № 5. – С. 137.

⁹² Определение Конституционного Суда РФ от 16 июля 2013 г. № 1176-О [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

В российском законодательстве регулирование отношений по защите частной жизни и защите персональных данных происходит параллельно. ФЗ «О персональных данных» регулирует не только отношения, входящие в сферу частной жизни человека, но также и отношения по поводу публичной и общедоступной информации⁹³. Действие указанного закона распространяется только на случаи нарушений, произошедших при обработке персональных данных, то есть если право на защиту частной жизни будет нарушено другими способами, ФЗ «О персональных данных применению подлежать не будет»⁹⁴. Под действие указанного закона попадают только ситуации неправомерных действий с определенной информацией, а право на частную жизнь может быть нарушено по поводу других сведений, составляющих личную, семейную тайну.

В Основном законе ФРГ не закреплено права на защиту частной жизни, но оно охватывается правом на свободу личности⁹⁵, выведенным из решений Федерального верховного суда⁹⁶ (Bundesgerichtshof), и признанным в качестве конституционного права. В Германии право на свободу личности, в целом, предоставляет даже больший уровень гарантий, чем это предусмотрено Конвенцией в части права на частную жизнь⁹⁷.

Конституционным правом на защиту персональных данных является право на информационное самоопределение, которое также установлено в качестве такового не в тексте Основного закона, а исходит из практики Конституционного суда ФРГ, впервые упомянуто им в решении в 1983 году⁹⁸. Оно заключается в праве каждого самостоятельно принимать решение о

⁹³ Долинская, В.В. Информационные отношения в гражданском обороте / В.В. Долинская // Законы России: опыт, анализ, практика. – 2010. – № 4. – С. 5.

⁹⁴ Рузанова, В.Д. Проблемы соотношения защиты права на неприкосновенность частной жизни и права на защиту персональных данных / В.Д. Рузанова // Законы России: опыт, анализ, практика. – 2019. – № 9. – С. 20.

⁹⁵ Проскурякова, М.И. Персональные данные: российская и германская национальные модели конституционно-правовой защиты в сравнительной перспективе / М.И. Проскурякова // Сравнительное конституционное обозрение. – 2016 – № 6. – С. 91.

⁹⁶ См. BGHZ 13, 334 (338), BGHZ 26, 349 (354).

⁹⁷ Проскурякова, М.И. Персональные данные: российская и германская национальные модели конституционно-правовой защиты в сравнительной перспективе / М.И. Проскурякова // Сравнительное конституционное обозрение. – 2016 – № 6. – С. 92.

⁹⁸ BVerfG, Urteilv. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83 [Электронный ресурс] – Режим доступа: <https://dejure.org/>.

разглашении и предоставлении права использования своих персональных данных, и, в отличие от, например, австрийского правового порядка, является самостоятельным правом, а не охватывается упомянутым выше правом на свободу личности⁹⁹.

Таким образом, национальные правовые системы России и Германии, ввиду наличия отдельного правового регулирования по защите персональных данных, в том числе специальных нормативно-правовых актов, склонны разделять защиту частной жизни и защиту персональных данных, несмотря на то, что признанным является эволюционное развитие права на защиту персональных данных из права на защиту частной жизни.

С течением времени защита персональных данных стала особым институтом, отчасти совпадающим с защитой частной жизни, а отчасти регулирующим иные отношения. При этом защита частной жизни также включает и явления, не попадающие под действие актов о защите персональных данных.

В то же время, нарушение права на защиту персональных данных может одновременно являться и нарушением права на частную жизнь, гарантированного ст. 8 Европейской конвенции о защите прав человека и основных свобод и, следовательно, стать предметом международного контроля со стороны Европейского суда по правам человека.

⁹⁹ Проскурякова, М.И. Персональные данные: российская и германская национальные модели конституционно-правовой защиты в сравнительной перспективе / М.И. Проскурякова // Сравнительное конституционное обозрение. – 2016 – № 6. – С. 93.

Глава 2. Правовой механизм защиты персональных данных человека по законодательству России и Германии

2.1. Ограничения при обработке персональных данных

Согласно пункту первому Замечания Общего Порядка №16 к Международному пакту о гражданских и политических правах¹⁰⁰ (Замечание принято Комитетом ООН по Правам Человека еще в 1988 году), на государства возлагаются позитивные обязательства по принятию законодательных и иных мер для запрета произвольного и незаконного вмешательства государственных органов, юридических и физических лиц в личную и семейную жизнь человека, а также по осуществлению защиты права человека на личную и семейную жизнь. В пункте 9 указано негативное обязательство государств по воздержанию от осуществления вмешательств в личную и семейную жизнь.

В отношении обработки персональных данных государствами Генеральная Ассамблея призывала «создать новые и продолжать использовать уже имеющиеся независимые, эффективные, обеспеченные надлежащими ресурсами и беспристрастные внутренние механизмы судебного, административного и/или парламентского надзора, позволяющие обеспечивать транспарентность, сообразно обстоятельствам, и подотчетность в связи с осуществлением государствами слежения за сообщениями, их перехвата и сбора и обработки персональных данных»¹⁰¹. В этом отношении представляется важным, как будет функционировать единый федеральный информационный регистр, содержащий сведения о населении России¹⁰², закон о котором вступил в силу в июне 2020 года, и насколько на практике будет обеспечена защита содержащихся в нем персональных данных. В него планируется включить к

¹⁰⁰ Замечание общего порядка № 16 – Статья 17 (право на личную жизнь) [Электронный ресурс] : приняты Комитетом ООН по правам человека на тридцать второй сессии в 1988 г. // Режим доступа: <https://tbinternet.ohchr.org/>.

¹⁰¹ Право на неприкосновенность частной жизни в цифровую эпоху [Электронный ресурс] : резолюция Генеральной Ассамблеи ООН № 73/179 от 17 декабря 2018 г. // Режим доступа: <https://undocs.org>.

¹⁰² О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации [Электронный ресурс] : федер. закон от 08.06.2020 № 168-ФЗ // Справочная правовая система «КонсультантПлюс» - Режим доступа: <http://consultant.ru/>.

2022 – 2025 годам достаточно широкий перечень сведений о гражданах РФ и иностранных гражданах, постоянно и временно проживающих в России.

В указанной Резолюции Генеральная Ассамблея ООН призвала государства рассмотреть вопрос об улучшении мер правовой защиты для «устранения ущерба от обработки, использования, продажи или многократной перепродажи персональных данных или других видов обмена такими данными между корпорациями без свободного, явно выраженного и осознанного согласия людей». Действительно, продажа баз данных является серьезной проблемой, которая требует безотлагательных мер противодействия. Так, за первую половину 2019 г., только по данным «Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России» было обнаружено 13 тысяч объявлений о продаже (покупке) баз, содержащих персональные данные граждан¹⁰³.

В Докладе «Право на неприкосновенность частной жизни в цифровой век» Верховный комиссар ООН указал на необходимость уделять особое внимание предоставлению защиты от нарушений права на неприкосновенность частной жизни, происходящих при профилировании (создании профилей людей) и автоматизированном принятии решений, т.е. когда юридически значимое решение принимается на основе каких-то алгоритмов, без участия человека. Однако при этом недопустимо ограничение права человека на свободу выражения мнений.

Так как обработка персональных данных создает большую угрозу нарушения права на частную жизнь, государствам необходимо принимать меры по ограничению деятельности операторов по обработке персональных данных и по осуществлению контроля за ней. Для решения этих задач и во исполнение указанных выше обязательств, государства в нормативно-правовых актах закрепляют принципы обработки персональных данных, устанавливают

¹⁰³ ЦБ впервые раскрыл масштаб продаж персональных данных россиян [Электронный ресурс] // Официальный сайт РБК. – Режим доступа <https://www.rbc.ru/>.

обязанности операторов и ответственность за их нарушение, а также определяют гарантии для субъектов.

В ФЗ «О персональных данных» в статье 5 к принципам обработки персональных данных отнесены следующие¹⁰⁴:

а) обработка данных осуществляется в соответствии с законом и справедливостью;

б) обработка персональных данных осуществляется только в соответствии с конкретными целями, для которых они были получены. Также из этого принципа вытекают два других:

- недопустимо объединение разных баз данных, данные в которых были получены для различных целей;

- обработке подлежат только данные, которые отвечают целям их обработки;

в) содержание и объем персональных данных должен соответствовать целям обработки, о которых заявлялось при их получении; данные не должны быть избыточными;

г) необходимо обеспечивать точность, достаточность и в некоторых случаях актуальность персональных данных по отношению к цели;

д) хранение персональных данных должно осуществляться в форме, позволяющей идентифицировать субъекта данных, и в течении срока, не превышающего необходимый для достижения цели.

В литературе также выделяются такие понятия, как принципы защиты персональных данных и принципы качества персональных данных. К принципам защиты персональных данных относят¹⁰⁵:

а) принцип защищенности субъекта данных от вмешательства в частную жизнь и соблюдения прав субъекта персональных данных;

¹⁰⁴О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 № 152-ФЗ ред. от 31.12.2017 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁰⁵ Кафтанникова, В. М. Принципы защиты персональных данных в России и за рубежом / В. М. Кафтанникова // Вестник ЮУрГУ. Серия «Право» – 2013 –Т. 13, № 2 – С. 99.

б) принцип гарантии физической защищенности персональных данных от незаконного доступа;

в) принцип обеспечения контроля за деятельностью по обработке персональных данных и применения ответственности за нарушение требований нормативно-правовых актов;

г) принцип выделения особых категорий персональных данных, нуждающихся в дополнительной защите.

Представляется интересным мнение В. П. Иванского¹⁰⁶, что принципы защиты данных являются совокупностью принципов качества персональных данных (которые установлены статьей 5 Конвенции 1981 года) и прав субъекта данных. К ним относятся:

а) принцип законности данных, то есть персональные данные должны быть получены и обработаны в соответствии с законом;

б) принцип законности целей, то есть данные можно собирать и использовать только в соответствии с законной целью;

в) принцип адекватности и релевантности данных, который означает, что данные не должны быть избыточными для достижения цели, для которой они собираются;

г) принцип достоверности и актуальности данных, то есть данные должны быть точными и, если это необходимо, регулярно обновляемыми;

д) принцип анонимности, который означает, что данные должны храниться в форме, позволяющей идентифицировать человека только в той степени, в какой этого требует цель, для которой данные собираются.

Соблюдение вышеуказанных принципов, по мнению В.П. Иванского, позволяет достичь баланс интересов между желанием получения и использования максимально возможного количества сведений о лице и защитой частной сферы этого лица. Он также отмечает, что в данном случае, на одной чаще весов стоит право со стороны всего общества на доступ к информации, а с

¹⁰⁶Иванский В.П. Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования: монография / В.П. Иванский. – Москва : РУДН, 1999. –С. 16.

другой право конкретного лица на ограничение доступа к информации, составляющей его частную сферу¹⁰⁷.

Таким образом, и принципы качества, и принципы обработки персональных данных по своей сути совпадают и представляют собой требования в первую очередь к оператору данных, которые направлены на защиту интересов субъектов данных в процессе обработки персональных данных. Принципы защиты персональных данных включают в себя требования не только к операторам, но также и к государству по созданию условий для соблюдения прав субъектов данных.

ФЗ «О персональных данных» помимо принципов выделяет также условия обработки персональных данных. Из текста закона сложно установить, что именно понимается законодателем под условиями, так как статья 6 содержит в себе большое количество пунктов и подпунктов, относящихся к различным аспектам регулирования обработки персональных данных. Так, например, в статье, посвященной условиям обработки персональных данных, перечислены случаи, когда такая обработка допустима без согласия субъекта:

а) если обработка осуществляется для достижения целей, предусмотренных международным договором или законом;

б) если обработка осуществляется в связи с участием субъекта в судопроизводстве;

в) если обработка осуществляется в рамках исполнительного производства;

г) если обработка необходима для предоставления субъекту государственных или муниципальных услуг;

д) если обработка персональных данных необходима для заключения договора по инициативе субъекта данных либо для исполнения договора, стороной по которому является субъект данных;

¹⁰⁷ Иванский В.П. Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования: монография / В.П. Иванский. – Москва : РУДН, 1999. –С. 17.

е) если обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта, и при этом получение согласия было невозможно;

ж) если обработка необходима для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей, но только при условии, что в этом случае не будут нарушены права и свободы субъекта данных;

з) если обработка необходима для осуществления профессиональной деятельности журналиста либо средства массовой информации, но также только в случае соблюдения прав и свобод субъекта данных;

и) если обработка осуществляется для статистических и иных исследовательских целей, при этом данные должны быть обязательно обезличены;

к) если обрабатываются персональные данные, которые субъект сам сделал общедоступными;

л) если осуществляется обработка персональных данных, подлежащих в соответствии с законом опубликованию или обязательному раскрытию.

Таким образом, перечень исключений является достаточно обширным, но при этом закрытым.

Также в статье, посвященной условиям обработки персональных данных, урегулированы следующие моменты:

а) указано, что особенности обработки некоторых видов данных и биометрических данных имеют специальное регулирование;

б) установлено право оператора поручать обработку данных другому лицу с согласия субъекта, определена процедура выдачи этого поручения, установлено, кто в этом случае будет нести ответственность за нарушения.

Все это в совокупности выделено в законе как условия обработки персональных данных и указано в статье, расположенной сразу после принципов, что представляется достаточно нелогичным с точки зрения законодательной техники.

В статье 5 Общего Регламента перечислены принципы обработки персональных данных: принцип законности; принцип беспристрастности и прозрачности; принцип целевого ограничения; принцип минимизации собираемых данных; принцип точности; принцип ограничения срока хранения; принцип целостности и конфиденциальности; принцип ответственности. Стоит отметить, что структурированность и систематизация принципов в Общем Регламенте значительно превосходит ФЗ «О персональных данных», где в статье, посвященной принципам, 3 пункта посвящены только одному принципу целевого ограничения, а также отсутствуют наименования каждого принципа.

Согласно принципу законности, обработка персональных данных должна попадать под одно из указанных в Общем Регламенте оснований: наличие согласия субъекта для обработки его персональных данных в соответствии с конкретной целью; обработка нужна для заключения договора, где субъект выступает стороной; обработка необходима для выполнения обязательства в отношении оператора; обработка нужна для защиты законных интересов субъекта данных или иных лиц; обработка необходима при выполнении публичных функций в интересах общества; обработка необходима для соблюдения законных интересов оператора, кроме случаев, когда законные интересы субъекта являются более важными, в особенности, если субъектом выступает ребенок.

Всё эти основания, в целом, соответствует установленным в ФЗ «О персональных данных» условиям обработки данных, хотя в российском законодательстве установлено больше случаев отсутствия необходимости в получении согласия субъекта данных. Однако интересным представляется толкование указанных в Общем Регламенте положений, в том числе содержащееся в Преамбуле к данному акту. Подобных разъяснений российское законодательство не содержит.

Так, при обработке персональных данных для соблюдения законных интересов оператора, согласно п. 47 Преамбулы, должны приниматься во внимание разумные ожидания субъектов персональных данных, основанные на

их отношениях с оператором, которые зависят от времени и других обстоятельств сбора персональных данных, целей их обработки. Также отмечается, что законные интересы оператора могут требовать обработки персональных данных для противодействия мошенничеству и для осуществления прямого маркетинга.

Таким образом, согласно Общему Регламенту, осуществление прямого маркетинга охватывается понятием законных интересов оператора, поэтому предварительное согласие субъекта не требуется, в отличие от российского законодательства¹⁰⁸. Соблюдение прав субъекта гарантируется в данном случае тем, что он имеет право бесплатно и в любое время возражать против обработки персональных данных, после чего обработка персональных данных в этих целях должна быть прекращена.

Согласно подходу российского законодателя, при осуществлении обработки персональных данных в целях прямого маркетинга больше защищаются интересы субъекта данных, избавляя его от несогласованной с ним рекламы (по крайней мере, *de jure*), однако европейское законодательство предоставляет больше возможностей для ведения предпринимательской деятельности. Кроме того, предприниматели сами заинтересованы в том, чтобы качественно выстраивать отношения с клиентами, что является внеправовым способом ограничения злоупотреблений со стороны операторов, поэтому подход Общего Регламента представляется более взвешенным¹⁰⁹.

Еще одной отличительной особенностью Общего Регламента является форма согласия субъекта. Согласно ФЗ «О персональных данных» для обработки специальных категорий персональных данных, биометрических данных, а также для трансграничной передачи данных требуется согласие субъекта в письменной форме на бумажном носителе (либо в форме

¹⁰⁸ Грибанов, А.А. Общий регламент о защите персональных данных (General Data Protection Regulation) : идеи для совершенствования российского законодательства / А.А Грибанов // Закон. – 2018. – № 3. – С. 159.

¹⁰⁹ Грибанов, А.А. Общий регламент о защите персональных данных (General Data Protection Regulation) : идеи для совершенствования российского законодательства / А.А Грибанов // Закон. – 2018. – № 3. – С. 159.

электронного документа, подписанного хотя бы простой электронной подписью)¹¹⁰. Общий Регламент же в этой части предлагает более широкий выбор способов дачи согласия. Для обработки специальных категорий персональных данных он вводит понятие «явно выраженного согласия»¹¹¹. Явно выраженное согласие может быть дано посредством заполнения электронной формы, отправки электронного письма, загрузки скана документа с подписью субъекта или с использованием электронной подписи.

В остальных случаях согласие может быть выражено, например, посредством проставления галочек в специальных формах на сайте, выбора определенных параметров в технических настройках информационных сервисов либо иного заявления или поведения, которые с учетом контекста явно указывают на принятие субъектом персональных данных условий их обработки.

Кроме того, российское законодательство гораздо более требовательно в части установления содержания согласия. В части 4 статьи 9 ФЗ «О персональных данных»¹¹² определен перечень из 9 пунктов, которые устанавливаются, что должно быть указано в письменном согласии субъекта данных. В числе прочего, там выделяется наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора. В пункте 42 Преамбулы к Общему Регламенту сказано, что согласие должно содержать по меньшей мере лишь сведения об операторе персональных данных и целях обработки персональных данных¹¹³. Ослабление

¹¹⁰О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 № 152-ФЗ ред. от 31.12.2017 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹¹¹Грибанов, А.А. Общий регламент о защите персональных данных (General Data Protection Regulation) : идеи для совершенствования российского законодательства / А.А. Грибанов // Закон. – 2018. – № 3. – С. 156.

¹¹²О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 № 152-ФЗ ред. от 31.12.2017 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹¹³Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронный ресурс] – Режим доступа: <https://dsgvo-gesetz.de/>.

требований к содержанию согласия субъекта данных благоприятно сказались бы на российской правовой системе¹¹⁴.

Принцип беспристрастности и прозрачности означает, что персональные данные должны обрабатываться оператором таким способом, который от него ожидает разумный человек, и при этом процесс обработки должен быть открытым, что выражается, например, в указании конкретной цели обработки еще на этапе получения персональных данных¹¹⁵.

Принципами, прямо не установленными в тексте ФЗ «О персональных данных», однако которые также можно вывести из толкования его положений, являются принцип целостности и конфиденциальности и принцип ответственности.

Принцип целостности и конфиденциальности предполагает, что обработка персональных данных должна обеспечивать безопасность данных, в том числе с использованием технических и организационных мер, что должно препятствовать незаконному к ним доступу.

Принцип ответственности означает, что оператор не только несет ответственность за соблюдение всех остальных принципов, но также должен быть в состоянии продемонстрировать это, например, в политике конфиденциальности и других актах¹¹⁶.

Принцип целевого ограничения, принцип минимизации данных, принцип точности, принцип ограничения хранения, в целом, соответствуют установленным в ФЗ «О персональных данных», однако в нем они не имеют наименований.

По российскому законодательству лицо, занимающееся обработкой персональных данных, называется оператором. Согласно статье 3 ФЗ «О

¹¹⁴ Грибанов, А.А. Общий регламент о защите персональных данных (General Data Protection Regulation) : идеи для совершенствования российского законодательства / А.А. Грибанов // Закон. – 2018. – № 3. – С. 157.

¹¹⁵ Чурилов, А.Ю. Принципы Общего регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации / А.Ю. Чурилов // Вестник Омской юридической академии. – 2019. – № 1. – С. 30.

¹¹⁶ Чурилов, А.Ю. Принципы Общего регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации / А.Ю. Чурилов // Вестник Омской юридической академии. – 2019. – № 1. – С. 33.

персональных данных», под обработкой персональных данных понимается любое действие или совокупность действий, совершаемых с использованием средств автоматизации (или без таковых) с персональными данными. «Автоматизированная» означает проводимая с помощью средств вычислительной техники. В литературе отмечается, что так как ФЗ «О персональных данных» не содержит специальных требований относительно неавтоматизированной обработки данных, то к обоим этим видам обработки данных применяются одни и те же правила¹¹⁷. При этом стоит учитывать, что неавтоматизированная обработка всё-таки предполагает возможность осуществления поиска по базе данных с использованием какого-либо заданного алгоритма, а если такой возможности нет, то данная «обработка» вовсе не регулируется ФЗ «О персональных данных»¹¹⁸.

Особым видом обработки данных является трансграничная передача данных. Она означает передачу персональных данных субъекта на территорию иностранного государства. Трансграничная передача, согласно статье 12 ФЗ «О персональных данных», возможна по общему правилу без дополнительных условий в страны, являющиеся сторонами Конвенции о защите физических лиц при автоматизированной обработке данных, а также в страны, хоть и не являющиеся сторонами конвенции, но которые установлены специальным перечнем, издаваемым Роскомнадзором¹¹⁹. Закон называет все эти страны как «страны, обеспечивающие адекватную защиту данных». В другие государства оператор может осуществлять передачу данных только в следующих случаях:

- а) наличия письменного согласия субъекта;

¹¹⁷ Вуколова, Т. Законодательство о персональных данных в Германии и России. Сравнительно-правовое исследование. / Т. Вуколова // Интеллектуальная собственность. Авторское право и смежные права – 2016 – №4 – С. 25

¹¹⁸108. Приезжева, А.А. Федеральный закон «О персональных данных»: научно-практический комментарий. / А.А. Приезжева. – Москва : Редакция «Российской газеты», 2015. – № 11. – С. 8.

¹¹⁹ Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных [Электронный ресурс] : приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 15.03.2013 г. № 274 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>

б) наличия соответствующего международного договора Российской Федерации;

в) наличия соответствующего федерального закона, разрешающего это в публичных интересах;

г) исполнения договора, стороной по которому является субъект данных;

д) защиты жизни, здоровья субъекта при невозможности получения согласия.

Обязанности оператора при обработке персональных данных установлены главой 4 ФЗ «О персональных данных» и другими нормативно-правовыми актами. Все обязанности оператора можно условно разделить на имеющие публично-правовую сущность, то есть исполняемые в целях защиты публичного интереса, и обязанности, имеющие частноправовую сущность, то есть исполняемые в правоотношениях между оператором и субъектом данных.

К первой группе можно отнести следующие обязанности оператора:

а) самостоятельно устанавливать меры, необходимые для обеспечения выполнения возложенных на него обязанностей, в частности, назначать ответственного за организацию обработки персональных данных, издавать соответствующие локальные акты, применять технические меры и другое;

б) опубликовать и обеспечить возможность доступа неограниченного круга лиц к документу, определяющему политику оператора в отношении обработки персональных данных, а также опубликовать сведения о реализуемых требованиях к защите персональных данных;

в) принимать необходимые правовые, организационные и технические меры с целью предотвращения несанкционированного доступа к персональным данным. Требования к защите персональных данных устанавливаются Правительством Российской Федерации¹²⁰;

¹²⁰ Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс] : постановление Правительства РФ от 01.11.2012 № 1119 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

г) уведомлять Роскомнадзор о своем намерении осуществлять обработку персональных данных. Однако из этой обязанности установлен достаточно большой перечень исключений, например, уведомление не требуется, если обработка осуществляется в соответствии с трудовым законодательством, если персональные данные включают в себя только фамилии, имена и отчества субъектов, если данные необходимы для однократного пропуска субъекта на определенную территорию и другое.

д) уведомлять Роскомнадзор о месте нахождения базы данных, где используются персональные данные российских граждан¹²¹. На практике это приводит к тому, что оператор самостоятельно вынужден выяснить, какие информационные системы используются им при сборе данных, и где расположены их базы данных, что, в целом, приводит к выбору операторами более надежных информационных систем¹²².

Ко второй группе обязанностей можно отнести следующие:

а) коррелирующая обязанность оператора предоставлять сведения по требованию субъекта данных, касающиеся обработки персональных данных этого субъекта;

б) блокировать персональные данные на время осуществления проверки, если поступило заявление субъекта данных о неправомерной обработке его персональных данных. Если по результатам проверки подтверждается неправомерность обработки, то оператор обязан в течении трех рабочих дней устранить нарушения и обеспечить правомерность данной обработки. Если это невозможно, то в течении десяти дней он обязан уничтожить такие сведения. О всех этих действиях он обязан уведомлять субъекта данных.

в) блокировать персональные данные на время осуществления проверки, если поступило заявление субъекта данных о неточности персональных

¹²¹ О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях [Электронный ресурс] : федер. закон от 21.07.2014 г. № 242-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹²² Добрикова, Е. Особенности применения закона о локализации персональных данных на практике: рекомендации для бизнеса.[Электронный ресурс] / Е. Добрикова // Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

данных. Если по результатам проверки будет установлено, что сведения являются неточными, оператор обязан в течение семи дней исправить их и снять блокировку;

г) в случае достижения цели обработки оператор обязан прекратить обработку и в течение тридцати дней уничтожить сведения о субъекте;

д) если субъект отзывает свое согласие на обработку данных, то оператор обязан прекратить обработку и, если сведения больше не требуются для целей обработки, в течение тридцати дней уничтожить их.

е) в случае правомерности требования субъекта оператор поисковой системы обязан прекратить выдачу сведений об указателе страницы сайта в сети Интернет (реализация «права на забвение»)¹²³.

Интересной представляется относительно новая обязанность операторов, действующая с 1 сентября 2015 года, которая была установлена Федеральным законом от 21 июля 2014 г. № 242-ФЗ¹²⁴. Данный закон часто называют «законом о локализации персональных данных»¹²⁵. Он внес изменения в ФЗ «Об информации, информационных технологиях и о защите информации», а также в ФЗ «О персональных данных». Новая обязанность операторов персональных данных заключается в том, что они должны осуществлять ряд действий по обработке персональных данных (а именно запись, систематизацию, накопление, хранение, уточнение, обновление, изменение и извлечение данных) только с использованием баз данных, территориально находящихся в России. Соответственно, остальные действия по обработке, то есть сбор, использование, передачу, обезличивание, блокирование, удаление,

¹²³Об информации, информационных технологиях и о защите информации [Электронный ресурс] :федер. закон от 27.07.2006 № 149-ФЗ ред. от 03.04.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹²⁴О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях [Электронный ресурс] :федер. закон от 21.07.2014 г. № 242-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹²⁵Добрикова, Е. Особенности применения закона о локализации персональных данных на практике: рекомендации для бизнеса. [Электронный ресурс] / Е. Добрикова // Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

уничтожение персональных данных, оператор может осуществлять не на территории России.

Данное нововведение распространяется только на операторов, осуществляющих деятельность в России¹²⁶. Об осуществлении деятельности в России может говорить, в частности, использование доменного имени сайта, связанного с Россией (.ru, .рф и другие), наличие русскоязычной версии сайта, возможность исполнения на территории России заключенного на сайте договора или использования на сайте русскоязычной рекламы и другое.

На основании «закона о локализации персональных данных» в августе 2016 года решением суда был заблокирован сервис LinkedIn, так как по запросам представителей Роскомнадзора LinkedIn не стал предоставлять сведений о том, где находятся его базы данных¹²⁷. Помимо нарушений требований о локализации баз данных, был установлен еще ряд нарушений. После этого, законность блокировки была подтверждена апелляционным определением Московского городского суда¹²⁸.

По сравнению с российским законодательством Общий Регламент более детально разграничивает понятия «оператор персональных данных» (согласно терминологии Общего Регламента в немецкоязычном переводе он называется «Verantwortlicher», т.е. «ответственный») и непосредственно «обработчик персональных данных» (в немецкоязычной версии Общего Регламента он назван как «Auftragsverarbeiter»). Полномочия обработчика персональных данных по ФЗ «О персональных данных» можно установить путем системного толкования. В Общем Регламенте не только даны определения оператора и обработчика, но и установлена разница в функциях и обязанностях, а также в ответственности за нарушение обязанностей.

¹²⁶О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях [Электронный ресурс] : комментарий к Федеральному закону от 21 июля 2014 г. № 242-ФЗ // официальный сайт Роскомнадзора. – Режим доступа: <https://pd.rkn.gov.ru/>.

¹²⁷ Решение Таганского районного суда №2-3491/2016[Электронный ресурс] // официальный сайт московского городского суда. – Режим доступа: <https://www.mos-gorsud.ru/>.

¹²⁸ Решение Московского городского суда по делу №33-15365 [Электронный ресурс] // официальный сайт московского городского суда. – Режим доступа: <https://www.mos-gorsud.ru/>.

Согласно Общему Регламенту, оператор определяет цели и способы обработки персональных данных, в то время как самой обработкой персональных данных занимается непосредственно обработчик¹²⁹. Однако это не препятствует совпадению функций оператора и обработчика в одном лице.

По общему правилу, согласно пункту 1 статьи 3, Общий Регламент применяется к операторам и обработчикам, если местом их деятельности является Европейский союз, при этом не имеет значения, где именно происходит обработка¹³⁰. Под его действие может попадать и оператор, не имеющий своего присутствия в Европейском союзе, например, находящийся на территории Российской Федерации.

Общий Регламент распространяет свою юрисдикцию и за пределы Европейского союза¹³¹. Это может произойти в двух случаях:

а) если деятельность оператора связана с оказанием услуг или предоставлением товаров субъектам данных, находящимся в Европейском союзе. Критериями в данном случае могут выступать использование на сайте языка или предоставление возможности оплачивать товар или услугу в валюте, обычно используемых в одном или нескольких государствах-членах Европейского союза; возможность заказывать товары и услуги на этом языке; упоминание в качестве потребителей лиц, которые находятся в Евросоюзе (пункт 23 Преамбулы Общего Регламента).

б) если деятельность оператора связана с мониторингом действий субъектов данных, находящихся в Европейском союзе. Причем под мониторингом может пониматься даже использование сайтом файлов cookie в отношении гражданина Европейского союза¹³².

¹²⁹Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронный ресурс] – Режим доступа: <https://dsgvo-gesetz.de/>.

¹³⁰Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронный ресурс] – Режим доступа: <https://dsgvo-gesetz.de/>.

¹³¹Долинская В.В. Защита прав в сфере персональных данных в России и ЕС / В.В. Долинская // Законы России: опыт, анализ, практика. – 2019. – № 9. – С. 28.

¹³²Долинская В.В. Защита прав в сфере персональных данных в России и ЕС / В.В. Долинская // Законы России: опыт, анализ, практика. – 2019. – № 9. – С. 28.

Таким образом, несмотря на действие Общего Регламента в рамках Европейского союза, он может применяться и в отношении операторов данных, находящихся в государстве за его пределами.

В Общем Регламенте установлены следующие обязанности оператора¹³³:

а) принимать в зависимости от целей, объема и контекста обработки, от различной степени вероятности рисков нарушения прав субъекта данных соответствующие технические и организационные меры по защите персональных данных. К таким мерам относятся, например, псевдонимизация и шифрование данных, минимизация количества собираемых данных, тестирование эффективности применяемых мер и другое;

б) оператор должен обеспечить обработку только тех персональных данных, которые нужны для достижения цели обработки. Для этого он ограничивает объем персональных данных, степень их обработки, срок хранения и возможность доступа к ним других лиц (по общему правилу запрещено предоставлять доступ неограниченному кругу лиц);

в) если оператор не имеет своего присутствия в Европейском союзе, однако тем не менее попадает по действие Общего Регламента (этот случай описан выше), то он обязан в письменной форме назначить представителя в соответствующем государстве Европейского союза, при этом, представитель должен непосредственно присутствовать в этом государстве. Эта обязанность не распространяется на операторов, являющихся публичным учреждением или проводящих нерегулярную обработку персональных данных, если она не создает риск для защиты прав субъектов данных;

г) непосредственный обработчик персональных данных не может обрабатывать персональные данные вопреки указаниям оператора. Кроме того, он не может передавать свои полномочия другим лицам без разрешения

¹³³Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронный ресурс] – Режим доступа: <https://dsgvo-gesetz.de/>.

оператора. При этом, оператор также должен обеспечивать соблюдение этих требований;

д) оператор (или непосредственный обработчик), если штат его сотрудников насчитывает больше, чем 250 человек, обязан вести регистр всех совершаемых по обработке действий и предоставлять его в установленных случаях в надзорный орган. Регистр включает в том числе сведения об операторе, о целях обработки, о категориях субъектов и персональных данных, о категориях получателей персональных данных и другое. При определенных обстоятельствах данный регистр обязана вести и компания с меньшим количеством сотрудников.

е) оператор обязан до начала обработки провести оценку влияния планируемых операций на защиту персональных данных, если существует вероятность большого риска нарушения прав субъектов в ходе такой обработки. Если оценка показывает, что риски, действительно, будут высокими, а при этом оператором не установлено достаточных механизмов по их снижению, он обязан произвести предварительную консультацию с надзорным органом;

ж) оператор обязан предоставлять субъекту данных определенную информацию при сборе его персональных данных, отраженную в политике обработки персональных данных. Перечень этих сведений, по сравнению с российским законодательством, не такой обширный и не предполагает предоставления большого количества детализированной информации, что, однако, не сказывается на качестве механизма защиты персональных данных, установленного Общим Регламентом¹³⁴.

Интересным представляется регулирование отношений по уведомлению надзорного органа. По российскому законодательству оператор обязан уведомить орган о намерении начать обработку. Общий Регламент отказался от

¹³⁴ Грибанов, А.А. Общий регламент о защите персональных данных (General Data Protection Regulation) : идеи для совершенствования российского законодательства / А.А Грибанов // Закон. – 2018. – № 3. – С. 160.

такого подхода. В пункте 89 Преамбулы сказано, что обязанность по уведомлению надзорного органа увеличивает административную и финансовую нагрузку на организации, и не всегда положительно сказывается на защите прав субъекта данных. Поэтому нормы Общего Регламента сфокусированы на создании процедур и механизмов, регулирующих законность операций с персональными данными, создающими высокие риски нарушения прав субъектов в силу своих характера, сферы применения, контекста и целей.

Как отмечается в литературе, обязанность оператора по уведомлению надзорного органа о начале обработки не является эффективным средством обеспечения защиты прав субъектов¹³⁵. Во-первых, в связи с тем, что обработкой персональных данных занимается практически каждая организация, данная мера лишена практического смысла. Во-вторых, многие организации игнорируют указанное требование. В-третьих, надзорный орган (в частности, Роскомнадзор) не обладает ресурсами по оценке возможных рисков при рассмотрении каждого полученного им уведомления оператора. Таким образом, подход Общего Регламента представляется более прогрессивным.

При этом в Общем Регламенте предусмотрена обязанность оператора по уведомлению надзорного органа о нарушении защиты данных (здесь термин «защита» употреблен в контексте информационной безопасности). Речь идет в первую очередь о неправомерном доступе к данным со стороны третьих лиц. В случае обнаружения подобного «взлома» системы, оператор обязан в течении 72 часов сообщить об этом в соответствующее надзорное учреждение (а в некоторых случаях даже уведомить и субъекта данных). Подобной обязанности в российском законодательстве не установлено.

Согласно положениям Федерального закона о защите данных (BDSG), оператору предоставлены дополнительные права, а также уточнены некоторые

¹³⁵Грибанов, А.А. Общий регламент о защите персональных данных (GeneralDataProtectionRegulation) : идеи для совершенствования российского законодательства / А.А Грибанов // Закон. – 2018. – № 3. – С. 160.

обязанности, по сравнению с теми, которые предусматривает Общий Регламент. К ним можно отнести следующие¹³⁶:

а) оператор наделен дополнительно правом на отказ от предоставления сведений надзорному органу, которые создают угрозу его уголовного или иного преследования. Это является так называемым в немецком праве *Auskunftsverweigerungsrecht*, то есть правом на отказ от дачи показаний, предоставленное любому лицу, в частности, свидетелю;

б) оператор обязан не препятствовать доступу уполномоченного сотрудника надзорного органа на свою территорию (земельный участок и место осуществления предпринимательской деятельности), а также ко всем устройствам и оборудованию, участвующим в обработке персональных данных.

Таким образом, свобода деятельности операторов по обработке персональных данных достаточно сильно ограничена путем установления на законодательном уровне запретов и обязанностей. При этом, действующее в России законодательство устанавливает даже более жесткие требования, регулирует в том числе и отдельные незначительные моменты, что в конечном итоге не улучшает действие механизма защиты персональных данных, но приводит к трудностям в работе операторов, являющихся, как правило, предпринимателями. Подход Общего Регламента представляется более современным и прогрессивным, не содержащим большого количества избыточного регулирования, но при этом обеспечивающий надлежащую защиту субъектам данных.

2.2. Гарантии защиты для субъекта персональных данных

В пункте 30 доклада Верховного комиссара ООН по правам человека «Право на неприкосновенность частной жизни в цифровой век»¹³⁷ установлены

¹³⁶ Paul Voigt, Axel von dem Bussche. *EU-Datenschutz-Grundverordnung (DSGVO) : Praktikerhandbuch* / Paul Voigt, Axel von dem Bussche – Berlin – Springer, 2018 – С. 267.

¹³⁷ Право на неприкосновенность частной жизни в цифровой век [Электронный ресурс] : доклад Верховного комиссара Организации Объединенных Наций по правам человека от 3 августа 2018 г. // Режим доступа: <https://documents-dds-ny.un.org>.

минимальные гарантии для субъектов персональных данных. К таковым отнесены: право субъекта знать об обработке, право иметь доступ к хранимым данным, право исправлять неточные или устаревшие данные, право исправлять или уничтожать незаконно хранящиеся данные.

Эти права практически не отличаются от закрепленных в статье 8 Конвенции 1981 года¹³⁸ дополнительных гарантий субъекта данных, которые, по мнению В. П. Иванского, являются одновременно и правами субъекта персональных данных¹³⁹:

а) право человека иметь информацию о наличии собранных о нем персональных данных, о цели, для которой они собирались и кем они собирались (с указанием места жительства либо адреса регистрации юридического лица);

б) право получать указанную выше информацию по запросу в разумные сроки, а также получать ее без запроса через определенные интервалы времени;

в) право получать доступ к своим персональным данным;

г) право требовать исправления или уничтожение недостоверных сведений, а также сведений, полученных с нарушением закона;

д) право на судебную защиту нарушенных прав в сфере обработки персональных данных.

На основании анализа главы 3 ФЗ «О персональных данных»¹⁴⁰ можно выделить следующие права субъекта персональных данных, установленные этим нормативно-правовым актом:

а) право на доступ к своим персональным данным;

б) право субъекта на дачу согласия на обработку, а также право требовать от оператора прекратить обработку его персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической

¹³⁸О защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс] : конвенция от 28.01.1981 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹³⁹Иванский В.П. Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования: монография / В.П. Иванский. – Москва : РУДН, 1999. – С. 17.

¹⁴⁰О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 № 152-ФЗ ред. от 31.12.2017 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

агитации. Причем ФЗ «О персональных данных», в отличие от Общего Регламента, устанавливает для обработки персональных данных в этих целях (к которым относится в том числе и прямой маркетинг) обязательное наличие предварительного согласия субъекта данных¹⁴¹.

в) право на дачу согласия на принятие решения, порождающего юридически значимые последствия на основании автоматизированной обработки персональных данных, а также право возражать против такого принятия решения;

г) право на обжалование действий или бездействий оператора в уполномоченный орган (таковым является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)¹⁴²) или в суд.

В целом, российское законодательство здесь использует основные идеи, заложенные в Конвенции, но при этом добавляет отдельные нюансы правового регулирования, конкретизирует ее положения.

В литературе в качестве наиболее общего права, принадлежащего субъекту данных, также выделяется право на защиту персональных данных¹⁴³, в содержание которого включается два элемента:

а) исключение каких-либо действий с персональными данными субъекта без его согласия на то;

б) обеспечение возможности субъектов данных контролировать действия операторов, производимых с их персональными данными.

Однако существующее регулирование говорит о существенном ограничении права на защиту персональных данных в таком его понимании, поэтому практическое значение данная его характеристика не имеет.

¹⁴¹Грибанов, А.А. Общий регламент о защите персональных данных (GeneralDataProtectionRegulation) : идеи для совершенствования российского законодательства / А.А Грибанов // Закон. – 2018. – № 3. – С. 156.

¹⁴²О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] : постановление Правительства РФ от 16.03.2009 № 228 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁴³Федосин, А.С. Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации : автореф. ... дис. канд. юрид. наук :12.00.14 / Федосин Алексей Сергеевич – Москва, 2009 – С. 9.

Еще одним важным правом субъекта персональных данных в цифровую эпоху является называемое в литературе «право на забвение», которое позволяет лицу требовать удаления информации о себе из поисковой системы¹⁴⁴. О. С. Соколова отмечает, что право на забвение следует из права на защиту чести, достоинства и деловой репутации, установленного ст. 152 ГК РФ.

Отметим, что о праве на забвение впервые было упомянуто в решении Суда Европейского союза в деле *Google v. Spain*¹⁴⁵ в 2014 году. Поисковая система Google выдавала в результатах поиска адрес страницы, которая содержала устаревшую информацию о гражданине. Поисковая система была признана Судом оператором персональных данных, а также указано, что субъект данных имеет право при определенных условиях требовать удаления из результатов поиска страницы с информацией о себе. Данное решение создало прецедент, который инициировал изменение законодательства о персональных данных в различных государствах, в том числе и в России.

Так, в Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»¹⁴⁶ в июле 2015 года были внесены изменения¹⁴⁷, которыми введена статья 10.3. Эта статья устанавливает процедуру реализации права на забвение¹⁴⁸.

В литературе положительно оценивается введение в ФЗ «Об информации, информационных технологиях и о защите информации» понятия поисковой системы¹⁴⁹, под которой понимается информационная система,

¹⁴⁴ Соколова, О.С. Защита персональных данных посредством права на забвение / О.С. Соколова // Современное право. –2016.–№ 9. – С. 71.

¹⁴⁵ Judgment of the Court (Grand Chamber), 13 May 2014. *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. [Электронный ресурс]– Режим доступа: <https://eur-lex.europa.eu/>.

¹⁴⁶ Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ ред. от 03.04.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁴⁷ О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации [Электронный ресурс] : федер. закон от 13.07.2015 № 264-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁴⁸ Талапина, Э. В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте. / Э. В. Талапина // Труды Института государства и права РАН. – 2018. – Т.13, № 5. – С. 134.

¹⁴⁹ Соколова, О.С. Защита персональных данных посредством права на забвение / О.С. Соколова // Современное право. –2016.–№ 9. – С. 71.

осуществляющая по запросу пользователя поиск в сети Интернет информации, и предоставляющая ему сведения об указатели страницы сайта, принадлежащего иному лицу, для доступа к запрашиваемой информации¹⁵⁰. Информационные системы, используемые для осуществления государственных и муниципальных функций, к поисковым не относятся.

Так, для того, чтобы поисковая система перестала выдавать определенную информацию о субъекте данных, субъект должен обратиться к оператору с требованием об удалении этих данных. При этом заявитель должен находиться на территории Российской Федерации, а основанием удаления должна служить недостоверность или неактуальность информации, утратившей значение для субъекта в силу последующих событий или действий субъекта¹⁵¹. Подобным способом нельзя удалить информацию, содержащую признаки уголовно-наказуемых деяний и сведения о совершенном преступлении (если еще не погашена судимость).

В литературе отмечается, что механизм реализации права на забвение имеет ряд недостатков. Во-первых, оператор не имеет средств для оценки недостоверности опубликованной о субъекте информации, и, опасаясь санкций со стороны государства, вынужден удовлетворять требования об удалении основываясь только на словах заявителя. Во-вторых, закон предписывает удалять не ссылку из поисковой системы, а саму информацию. Технически это осуществить представляется достаточно сложным.

Права субъекта персональных данных в Германии установлены в первую очередь главе 3 Общего Регламента. Отдельные положения конкретизированы в национальном немецком законодательстве, если такую возможность прямо предусматривает Регламент.

В Общем Регламенте содержатся следующие права субъекта данных.

а) Право субъекта данных на получение от оператора информации:

¹⁵⁰ Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ ред. от 03.04.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁵¹ Соколова, О.С. Защита персональных данных посредством права на забвение / О.С. Соколова // Современное право. –2016.–№ 9. – С. 71.

- обрабатываются ли относящиеся к нему персональные данные;
- какова цель обработки;
- каким категориям получателей будут раскрыты его персональные данные;
- если это возможно, срок их хранения;
- присутствует ли автоматизированный процесс принятия решения в отношении субъекта данных на основании осуществленной обработки.

Стоит отметить, что перечень сведений, которые субъект вправе требовать от оператора несколько шире того, который установлен в ФЗ «О персональных данных». Кроме того, в Общем Регламенте указано дополнительное требование: сведения должны быть предоставлены в детальной, доступной, понятной и простой для понимания форме с использованием простого и ясного стиля речи¹⁵². Российский законодатель ограничился лишь требованием доступности¹⁵³.

б) Право потребовать исправление, удаление персональных данных, а также ограничения их использования.

Право потребовать исправление означает возможность субъекта дополнить в соответствии с целями обработки недостающие персональные данные.

Право на удаление (включая право на забвение) рассматривается, в отличие от российского законодательства, не только в контексте удаления информации из поисковой системы. Согласно Общему Регламенту субъект имеет право требовать удаления его персональных данных в следующих случаях:

- достигнута цель обработки персональных данных;

¹⁵²Paul Voigt, Axel von dem Bussche. EU-Datenschutz-Grundverordnung (DSGVO) : Praktikerhandbuch / Paul Voigt, Axel von dem Bussche – Berlin – Springer, 2018 – С. 187.

¹⁵³О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 № 152-ФЗ ред. от 31.12.2017 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

- субъект данных отзывает свое согласие на обработку или возражает против обработки, и при этом отсутствуют другие основания, позволяющие оператору сохранить персональные данные;
- персональные данные обрабатывались с нарушением закона;
- такая обязанность для оператора установлена иными актами Европейского союза или национальным правом.

В самом Общем Регламенте не закреплено понятие «удаление», однако это сделано в Федеральном законе о защите данных. Под удалением понимается «стирание, сокрытие» («Unkenntlichmachen») хранимых персональных данных. Толкование данного понятия позволит установить техническую процедуру для осуществления права на удаление¹⁵⁴. При этом, речь не идет о глобальном исчезновении данных, а только об удалении конкретных данных у конкретного оператора.

Право на удаление персональной информации по требованию субъекта не так структурировано в ФЗ «О персональных данных». Например, субъект имеет право согласно пункту 2 статьи 9 отозвать свое согласие на обработку персональных данных, при этом обязанность оператора по удалению сведений в этом случае установлена лишь в пункте 5 статьи 21.

Уникальным, по сравнению с российским законодательством, является право субъекта данных (его законного представителя) требовать удаления его персональных данных в случае, если в момент дачи согласия на обработку он являлся ребенком. Причем в регламенте установлено, что подобное согласие изначально может давать только лицо, достигшее, как минимум, 16 лет либо его законный представитель.

в) Субъект данных имеет право в любое время в силу своей особенной ситуации подать возражение против обработки, и оператор обязан прекратить подобную обработку, если отсутствуют иные законные основания, либо если она осуществлялась в целях прямого маркетинга. Особенная ситуация может

¹⁵⁴Sven Hunzinger. Das Löschen im Datenschutzrecht / Sven Hunzinger–Baden-Baden :Nomos, 2018.–С.14.

вытекать, в частности, из других конституционных прав гражданина, из семейной ситуации или из соображений соблюдения коммерческой тайны¹⁵⁵.

Согласно Федеральному закону о защите данных¹⁵⁶ указанное право субъекта данных может быть ограничено в том случае, если обработка осуществлялась в соответствии с научной, исторической исследовательской или статистической деятельностью, либо в целях соблюдения публичных интересов при формировании архивов.

г) Право не попадать под действие юридически значимого для субъекта решения, принятого исключительно путем автоматического принятия на основе автоматизированной обработки. Исключениями являются обработка в целях заключения договора или прямое согласие субъекта на принятие такого рода решений. Согласно ФЗ «О персональных данных» подобными исключениями являются только наличие согласия или прямо установленное в федеральном законе правило.

Таким образом, на законодательном уровне в России в развитие основных идей, заложенных в Конвенции 1981 года, установлены широкие гарантии субъектов персональных данных. При этом, российский законодатель старается вносить изменения в действующее правовое регулирование в соответствии с европейской правоприминительной практикой.

Однако немецкое регулирование в совокупности с положениями Общего Регламента детализирует и улучшает механизмы осуществления того или иного права субъекта данных, предоставляя больший уровень правовых гарантий.

2.3. Ответственность оператора за нарушение законодательства

За нарушение российского законодательства о персональных данных предусмотрена административная, уголовная, гражданско-правовая и

¹⁵⁵Paul Voigt, Axel von dem Bussche. EU-Datenschutz-Grundverordnung (DSGVO) : Praktikerhandbuch / Paul Voigt, Axel von dem Bussche – Berlin – Springer, 2018 – С. 236.

¹⁵⁶Bundesdatenschutzgesetz (BDSG) [Электронный ресурс] // Gesetze im Internet – Режим доступа: <https://www.gesetze-im-internet.de/>.

дисциплинарная ответственность¹⁵⁷. Нарушение может быть установлено в результате обращения субъекта данных в суд либо в уполномоченный орган, так и выявлено в ходе плановых проверок, проводимых Роскомнадзором или иными органами.

Органами, осуществляющими контроль и надзор в сфере персональных данных, являются:

а) Роскомнадзор (согласно пункту 5.1(1) Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций¹⁵⁸);

б) Прокуратура РФ как орган, осуществляющий надзор за соблюдением Конституции Российской Федерации и исполнением законов во всех сферах жизни¹⁵⁹;

в) Федеральная служба безопасности, которая является уполномоченным органом в области обеспечения безопасности¹⁶⁰;

г) Федеральная служба по техническому и экспортному контролю (ФСТЭК России)¹⁶¹, которая является уполномоченным органом в области противодействия техническим разведкам и технической защиты информации;

д) Другие органы.

Меры ответственности за нарушение законодательства в сфере персональных данных разбросаны по разным отраслевым правовым источникам и слабо поддаются систематизации¹⁶². В целом, наличие мер ответственности положительно оценивается в качестве средства,

¹⁵⁷ Долинская В.В. Защита прав в сфере персональных данных в России и ЕС / В.В. Долинская // Законы России: опыт, анализ, практика. – 2019. – № 9. – С. 26.

¹⁵⁸ О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] : постановление Правительства РФ от 16.03.2009 № 228 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁵⁹ О прокуратуре Российской Федерации [Электронный ресурс] : федер. закон от 17.01.1992 № 2202-1// Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁶⁰ О Федеральной службе безопасности [Электронный ресурс] : федер. закон от 03.04.1995 г. № 40-ФЗ// Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁶¹ Вопросы Федеральной службы по техническому и экспортному контролю [Электронный ресурс] : указ Президента РФ от 16.08.2004 г. № 1085 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁶² Долинская В.В. Защита прав в сфере персональных данных в России и ЕС / В.В. Долинская // Законы России: опыт, анализ, практика. – 2019. – № 9. – С. 27.

предотвращающего нарушение законодательства в области персональных данных¹⁶³.

Как отмечается в литературе, в российской правовой системе превалирует административная ответственность за нарушение подобных норм¹⁶⁴. Этой сфере напрямую посвящена статья 13.11 Кодекса об административных правонарушениях (КоАП)¹⁶⁵, которая охватывает большинство нарушений, которые может совершить лицо при обработке персональных данных. За различные нарушения, согласно частям данной статьи, может быть назначен штраф от одной тысячи до восемнадцати миллионов рублей.

Помимо этих, можно выделить также правонарушения, предусмотренные статьями 13.6 КоАП (использование средств связи или несертифицированных средств кодирования (шифрования), не прошедших процедуру подтверждения их соответствия установленным требованиям), 13.12 КоАП (нарушение правил защиты информации), 13.13 КоАП (незаконная деятельность в области защиты информации), 13.22 КоАП (нарушение порядка объявления выходных данных), 20.23 КоАП (нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации), 20.24 КоАП (незаконное использование специальных технических средств, предназначенных для негласного получения информации, в частной детективной или охранной деятельности) и другие¹⁶⁶.

В Уголовном Кодексе РФ¹⁶⁷ (УК РФ) наиболее релевантной является статья 137 УК РФ, которая устанавливает ответственность за незаконное собирание или распространение сведений о частной жизни лица, составляющих

¹⁶³Болотин, В. С., Маслѐха, М. А. Механизм защиты права на неприкосновенность частной жизни при обработке персональных данных в информационных системах / В. С. Болотин, М. А. Маслѐха. // Вестник государственного и муниципального управления. – 2012. – №3. – С. 101.

¹⁶⁴Долинская В.В. Защита прав в сфере персональных данных в России и ЕС / В.В. Долинская // Законы России: опыт, анализ, практика. – 2019. – № 9. – С. 27.

¹⁶⁵Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс] :федер. законот 30.12.2001 № 195-ФЗ// Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁶⁶Долинская В.В. Защита прав в сфере персональных данных в России и ЕС / В.В. Долинская // Законы России: опыт, анализ, практика. – 2019. – № 9. – С. 27.

¹⁶⁷ Уголовный кодекс Российской Федерации [Электронныйресурс] :федер. закон от 13.06.1996 № 63-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>

его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Однако по данной статье возможно привлечение к ответственности только в случае собирания информации о субъекте данных, которая будет не только относиться к персональным данным человека, но и попадать под режим охраны частной жизни, что, как отмечается в литературе, требует дополнительного изучения законных оснований вмешательства в частную жизнь в каждом конкретном случае¹⁶⁸. Некоторые авторы отмечают, что операторов практически невозможно привлечь к ответственности по статье 137 УК РФ, поэтому предлагают ввести в УК РФ статью 137.1, устанавливающую ответственность за нарушение правил обращения именно с персональными данными¹⁶⁹.

Примечательным в части гражданско-правовой ответственности является то, что ФЗ «О персональных данных» в статье 24 устанавливает наряду с возмещением имущественного вреда возможность компенсации морального вреда, причиненного субъекту персональных данных.

Применение на практике механизма привлечения оператора к ответственности за нарушение законодательства о персональных данных вызывает большое количество споров в национальных судах РФ.

Для формирования правоприменительной практики имеют значение позиции, выработанные Верховным судом РФ в следующих делах.

а) По иску Роскомнадзора была прекращена деятельность газеты, которая распространяла персональные данные граждан без получения от них согласия¹⁷⁰. В мотивировочной части решения суд обратился к Закону Российской Федерации «О средствах массовой информации»¹⁷¹ и указал, что

¹⁶⁸Павлинов А. А. Уголовная ответственность за нарушение неприкосновенности частной жизни / А.А. Павлинов // Пробелы в российском законодательстве. – 2013. – №6. – С. 190.

¹⁶⁹Кадников, Б.Н. Уголовно-правовая охрана неприкосновенности частной жизни : научно-практическое пособие / под ред. Н.Г. Кадникова. – Москва : Юриспруденция, 2011. – С. 69.

¹⁷⁰Определение Верховного Суда РФ от 24.06.2015 № 18-АПГ15-7[Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁷¹О средствах массовой информации [Электронный ресурс]: закон РФ от 27.12.1991 № 2124-1// Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

согласно статье 4 данного закона недопустимо распространение сведений, составляющих охраняемую законом тайну. Кроме того, согласно абзацу 3 статьи 16 данного закона, основанием для прекращения судом деятельности средства массовой информации являются неоднократные в течение двенадцати месяцев нарушения редакцией требований статьи 4, которые и были установлены в ходе рассмотрения этого дела. Также судом высказана позиция, что при отсутствии согласия субъекта данных на распространение его персональных данных, редакция газеты (и любого средства массовой информации) должна обеспечивать конфиденциальность данных сведений, и как возможный вариант обеспечения такой конфиденциальности, судом предложено использование механизма обезличивания данных.

В дополнение стоит отметить, что в соответствии со статьей 3 ФЗ «О персональных данных» под обезличиванием понимаются действия оператора с персональными данными, в результате которых становится невозможно установить принадлежность данных к конкретному субъекту без использования дополнительных сведений. Данный механизм обеспечивает действенную защиту данных и активно используется, в том числе и в европейских правовых порядках.

б) Судом установлена правомерность требований кассира в магазине о предъявлении паспорта для оформления возврата товара и денежных средств¹⁷².

Процесс был инициирован органами прокуратуры после проведения проверки на предмет нарушений в сфере законодательства о персональных данных; проверка была начата после обращения гражданина, который посчитал недопустимым требование кассира о заполнении заявления с указанием паспортных данных при возврате товара.

Суд указал, что требование об указании паспортных данных лица для возврата товара и получения уплаченных денежных средств не является избыточным, так как согласно Положению о порядке ведения кассовых

¹⁷² Постановление Верховного суда РФ от 15 июня 2016 г. № 25-АД15-3 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

операций с банкнотами и монетой Банка России на территории Российской Федерации¹⁷³ выдача наличных денежных средств из кассы магазина возможна только при предъявлении получателем документа, удостоверяющего личность. Таким образом, для этой ситуации установлено специальное правило, которым и следует руководствоваться.

в) Федеральная антимонопольная служба после рассмотрения заявления гражданина обратилась в организацию с требованием предоставить сведения о владельце телефонного номера, с которого производилась рекламная рассылка. Организация отказала, сославшись на требования закона о персональных данных, за что была привлечена к ответственности по статье 19.8 КоАП (непредставление сведений в федеральный антимонопольный орган). Суды всех инстанций признали данное привлечение к ответственности незаконным, а действия организации правомерными, однако Верховный суд отменил все акты нижестоящих судов, и постановил о законности привлечения к ответственности¹⁷⁴.

Аргументы нижестоящих судов заключались в том, что Федеральная антимонопольная служба не относится к органам, уполномоченным осуществлять оперативно-розыскную деятельность, следовательно, и для получения персональных данных без согласия лица у нее нет законных оснований.

Верховный суд указал, что так как Федеральная антимонопольная служба осуществляет функции государственного контроля и надзора, выявляет и пресекает правонарушения, а также возбуждает и рассматривает дела, то она может получать в рамках своей деятельности необходимые сведения о физических лицах.

¹⁷³Положение о порядке ведения кассовых операций с банкнотами и монетой Банка России на территории Российской Федерации [Электронный ресурс] :утв. Банком России от 12.11.2011 № 373-П (утратило силу) // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁷⁴Постановление Верховного суда РФ от 13 августа 2015 г. № 302-АД15-5169 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

На наш взгляд, Верховный суд необоснованно расширил полномочия Федеральной антимонопольной службы, создал прецедент для возможности неконтролируемого и избыточного получения персональных данных граждан государственными органами, так как вышеуказанными полномочиями обладает большое количество органов, осуществляющих деятельность в различных сферах. Это в конечном счете не ведет к соблюдению принципов демократии и правового государства.

Еще одним средством защиты субъектов данных может выступать обращение в Европейский суд по правам человека, в котором было рассмотрено большое количество дел, посвященных проблеме соблюдения законодательства о персональных данных со стороны государства.

Стоит отметить, что значимость решений Европейского суда по правам человека заключается в возможности ссылаться на позиции, изложенные в них, при рассмотрении дела в национальных российских судах. Правовой основой для этого служит, во-первых, часть 4 статьи 15 Конституции РФ¹⁷⁵, где сказано, что международные договоры Российской Федерации являются составной частью ее правовой системы. Во-вторых, Федеральный закон «О ратификации Конвенции о защите прав человека и основных свобод и Протоколов к ней»¹⁷⁶, который устанавливает юрисдикцию Европейского суда по правам человека в качестве обязательной по вопросам толкования и применения Конвенции о защите прав человека и основных свобод.

В-третьих, об этом неоднократно высказывался Пленум Верховного суда Российской Федерации. Так, в Постановлении от 10.10.2003 № 5 «О применении судами общей юрисдикции общепризнанных принципов и норм международного права и международных договоров Российской Федерации»¹⁷⁷

¹⁷⁵ Конституция Российской Федерации [Электронный ресурс] : принята всенародным голосованием 12.12.1993 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁷⁶ О ратификации Конвенции о защите прав человека и основных свобод и Протоколов к ней [Электронный ресурс]: федер. закон от 30.02.1998 № 54-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁷⁷ О применении судами общей юрисдикции общепризнанных принципов и норм международного права и международных договоров Российской Федерации [Электронный ресурс] : постановление Пленума

указано, что применение национальными судами Конвенции о защите прав человека и основных свобод должно осуществляться с учетом практики Европейского суда по правам человека. В Постановлении от 27.06.2013 № 21 «О применении судами общей юрисдикции Конвенции о защите прав человека и основных свобод от 4 ноября 1950 года и Протоколов к ней»¹⁷⁸ Пленум указал, что правовые позиции Европейского суда по правам человека, которые содержатся в окончательных постановлениях Суда, принятых в отношении Российской Федерации, являются обязательными для российских судов и учитываются при применении национального законодательства, а правовые позиции, которые приняты в отношении других государств учитываются российским судом, если обстоятельства рассматриваемого ими дела являются аналогичными обстоятельствам, ставшим предметом анализа и выводов Европейского суда по правам человека.

В практике Европейского суда по правам человека были дела, касающиеся нарушения законодательства о персональных данных, где государством-ответчиком выступала Российская Федерация.

В Постановлении по делу Шимоволос против России¹⁷⁹ гражданин, который являлся правозащитным активистом, без его согласия был внесен в правоохранительную базу данных, позволяющую контролировать его передвижение (при покупке им билета на поезд или самолет в правоохранительные органы приходило автоматическое уведомление).

Европейский суд установил, что имеется вмешательство в частную жизнь со стороны государства, и что данное вмешательство не предусмотрено законом. В пункте 68 Постановления указано, что база данных, в которую был внесен гражданин, создана ведомственным приказом, который опубликован не

Верховного суда от 10.10.2003 № 5// Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁷⁸О применении судами общей юрисдикции Конвенции о защите прав человека и основных свобод от 4 ноября 1950 года и Протоколов к ней [Электронный ресурс] : постановление Пленума Верховного суда от 27.06.2013 № 21 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁷⁹ Постановление Европейского Суда по правам человека по делу «Шимоволос против России» от 21.06.2011 (жалоба № 30194/09) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

был. Также не был закреплен и необходимый минимум гарантий для того, чтобы избежать неправильное применение закона, а именно: характер, объем и длительность возможных мер; основания необходимые для их применения; органы, компетентные осуществлять надзор за правильным применением данных мер; вид средства правовой защиты, предусмотренный национальным законодательством. На основании этого судом сделан вывод о нарушении статьи 8 Конвенции о защите прав человека и основных свобод.

В деле Иващенко против России¹⁸⁰ журналист подвергся досмотру на границе Российской Федерации, в результате чего сотрудниками таможенной службы было скопировано двадцать шесть гигабайт информации с личного ноутбука заявителя, в том числе личная переписка, текстовые материалы и фотографии, включая и персональные данные. Таможенный орган ссылаясь на положения тогда еще действовавшего Таможенного кодекса Таможенного союза, позволяющий в определенных случаях проводить отбор проб товаров.

Европейский суд установил нарушение статьи 8 Конвенции о защите прав человека и основных свобод, т.к. законодательство РФ и правоприменительная практика не обеспечивают должный уровень адекватных и эффективных гарантий защиты граждан. Кроме того, копирование информации с цифрового носителя не может попадать под понятие отбора проб.

В деле «Роман Захаров против России»¹⁸¹ заявитель жаловался на возможность тайного прослушивания его мобильного телефона при отсутствии необходимых правовых гарантий.

Европейский суд по правам человека в пункте 229 Постановления указал, что введение системы тайного наблюдения должно обладать предсказуемостью, однако это не должно означать, что гражданин обязан иметь возможность предвидеть, когда власти станут прослушивать его телефонные

¹⁸⁰ Постановление Европейского Суда по правам человека по делу «Иващенко против России» от 13.05.2018 (жалоба № 61064/10) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁸¹ Постановление Европейского Суда по правам человека по делу «Роман Захаров против России» от 04.12.2015 (жалоба № 47143/06) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

разговоры, чтобы он смог соответствующим образом изменить свое поведение. С целью недопущения произвола со стороны властей, должны быть на законодательном уровне установлены четкие и подробные правила применения той или иной системы тайного наблюдения, детально прописаны обстоятельства и условия, при которых государство может прибегнуть к конкретной мере тайного наблюдения.

Суд также отметил, что российское законодательство не устанавливает достаточных и необходимых гарантий для предотвращения произвольного вмешательства со стороны властей при применении мер тайного наблюдения. Кроме того, в национальном законодательстве предусмотрено сохранение не относящейся к делу информации. Также оно не содержит четких критериев, при которых после окончания судебного процесса избыточная информация должна быть удалена. У органов власти существуют широкие дискреционные полномочия по установлению скрытого наблюдения, и отсутствует механизм должного контроля и надзора за этой деятельностью, как и отсутствует обязанность по уведомлению лица по установке за ним скрытого наблюдения в какой бы то ни было момент расследования или после его завершения.

Европейский суд по правам человека установил нарушение статьи 8 Конвенции о защите прав человека и основных свобод даже несмотря на то, что доказательств применения непосредственно к заявителю меры по прослушиванию его телефонных переговоров установлено не было.

Подобную позицию Европейский суд повторил в делах «Зубков и другие против России»¹⁸², «Москалев против России»¹⁸³.

В Европейском суде по правам человека по делам о защите персональных данных ответчиками выступали и государства Европейского союза, в том числе и Германия.

¹⁸² Постановление Европейского Суда по правам человека по делу «Зубков и другие против Российской Федерации» от 07.11.2017 (жалоба № 29431/05) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁸³ Постановление Европейского Суда по правам человека по делу «Константин Москалев против Российской Федерации» от 07.11.2017 (жалоба № 59589/10) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

В деле «S. и Марпер против Соединенного Королевства»¹⁸⁴ полиция после прекращения уголовного преследования в отношении заявителей отказалась по их просьбе уничтожить полученные в ходе разбирательства их ДНК и отпечатки пальцев. Европейский суд по правам человека признал это нарушением статьи 8 Европейской конвенции по защите прав человека, так как обвиняемые были оправданы. Также Европейский суд по правам человека со ссылкой на дело «Леандер против Швеции» указал, что даже само по себе хранение личной информации человека является вмешательством государства в осуществление его прав. Однако при соблюдении таких требований, как законность, преследование правомерных целей для защиты прав и свобод других лиц и общества, незначительность вмешательства, сбор и хранение ДНК и отпечатков пальцев человека может быть признан допустимым¹⁸⁵.

В деле «P.G. and J.H. против Соединенного Королевства»¹⁸⁶ с помощью скрытых подслушивающих устройств были получены образы голоса заявителя в его квартире, а затем таким же образом записан его разговор во время допроса. Экспертами были сопоставлены два образа голоса и установлено, что он принадлежит одному и тому же человеку. Впоследствии данные доказательства были использованы и в рамках судебного рассмотрения дела. Европейский суд по правам человека признал, что в данном случае имеется нарушение статьи 8 Европейской конвенции, так как это тем не менее является обработкой персональных данных человека и должно соответствовать всем установленным требованиям, предъявляемым к процедуре получения персональных данных.

¹⁸⁴Постановление Европейского Суда по правам человека по делу «S. и Марпер против Соединенного Королевства» [S. And Marper v. The United Kingdom] от 04.12.2008(жалобы № 30562/04 и № 30566/04).[Электронный ресурс] – Режим доступа: <http://www.echr.ru/>.

¹⁸⁵Постановление Европейского Суда по правам человека по делу «Ван дер Хейден против Нидерландов» [Vander Heijden v. Netherlands] от 3 апреля 2012 г. (жалоба № 42857/05) [Электронный ресурс] // Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

¹⁸⁶Постановление Европейского Суда по правам человека по делу «P.G. and J.H. v. The United Kingdom» от 25.09.2001(жалоба № 44787/98) [Электронный ресурс] // Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

Таким же образом Судом было усмотрено нарушение Конвенции по защите прав человека в деле «Веттер против Франции»¹⁸⁷, где образцы голоса были получены так же в ходе скрытого прослушивания квартиры, где часто бывал заявитель.

В деле «Узун против Германии»¹⁸⁸ использование системы слежения посредством GPS со стороны государства было признано правомерным, так как были соблюдены требования законности, соблюден принцип пропорциональности, который означает, что вмешательство допустимо только в особых прямо установленных случаях и осуществляется в связи с невозможностью использования других средств. В данном деле заявителем были уничтожены все установленные ранее полицией устройства, он перестал пользоваться мобильной связью. Кроме того, по национальному законодательству Германии подобный способ слежения может быть установлен только в отношении подозреваемых в совершении тяжкого уголовного преступления. Все эти требования законодательства были установлены Европейским судом по правам человека в данном деле.

В деле «Коплэнд против Соединенного Королевства»¹⁸⁹ работодателем (публичная организация, находящаяся под контролем государства) была установлена слежка за рабочим компьютером, а именно мониторинг посещенных сайтов и просматривание электронных писем, а также прослушивание рабочего телефона, с целью определения, не используются ли указанные средства в личных целях в рабочее время. Европейский суд по правам человека установил, что все вышеперечисленное также включается в понятие частной жизни и подлежит защите, так как заявитель не был уведомлен о подобной слежке и имел полное право полагать, что за его действиями с

¹⁸⁷ Постановление Европейского Суда по правам человека по делу «Vetter v. France» от 31.05.2005 (жалоба № 59842/00) [Электронный ресурс] // Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

¹⁸⁸ Постановление Европейского Суда по правам человека по делу «Узун против Германии» [Uzun v. Germany] от 02.09.2010 (жалоба № 35623/05) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁸⁹ Постановление Европейского Суда по правам человека по делу «Коплэнд против Соединенного Королевства» [Copland v. The United Kingdom] от 03.04.2007 (жалоба № 62617/00) [Электронный ресурс] // Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

рабочего компьютера не будет осуществляться подобный контроль, и о них никому не станет известно.

Практическое знание имеет позиция Европейского суда по правам человека, выраженная в деле «Centrum för rättvisa v. Sweden»¹⁹⁰, особенно в сравнении с рассмотренным выше решением по делу «Роман Захаров против России»¹⁹¹. Судом рассматривалась жалоба юридического лица на неправомерность существующего в Швеции механизма массового перехвата электронных сигналов для целей правоохранительной деятельности. Европейский суд по правам человека установил, что шведским законодательством в данной сфере установлены достаточные и адекватные гарантии, препятствующие произвольному сбору данных о гражданах, например, данные меры применяются только после детального изучения судом вопроса о возможности их использования. Кроме того, в Швеции существуют специальные и независимые органы, осуществляющие надзор за законностью применения системы перехвата электронных сигналов, которые могут рассматривать и жалобы граждан.

В деле «Benedik v. Slovenia»¹⁹² Европейским судом по правам человека было установлено нарушение статьи 8 Конвенции, так как правоохранительными органами были запрошены у интернет-провайдера сведения о динамическом IP-адресе гражданина без наличия соответствующей санкции суда. При этом, решение Суда не было принято единогласно, так как судья Ф. Вехабович не посчитал сведения об IP-адресе персональными данными¹⁹³. Тем не менее, по мнению Европейского суда по правам человека, в Словении отсутствуют положения о защите от произвольного вмешательства со

¹⁹⁰ Постановление Европейского Суда по правам человека по делу [Centrum för rättvisa v. Sweden] от 19.06.2018 (жалоба № 35252/08) [Электронный ресурс] – Режим доступа: <https://hudoc.echr.coe.int/>.

¹⁹¹ Постановление Европейского Суда по правам человека по делу «Роман Захаров против России» от 04.12.2015 (жалоба № 47143/06) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

¹⁹² Постановление Европейского Суда по правам человека по делу «Benedik v. Slovenia» от 24.07.2018 (жалоба № 62357/14) [Электронный ресурс] – Режим доступа: <https://hudoc.echr.coe.int/>.

¹⁹³ Оганесян, Т. Д. Защита персональных данных: позиции международных судов / Т. Д. Оганесян // Российское правосудие. – 2019 – №6 – С. 52.

стороны правоохранительных органов в частную сферу граждан, а также органы независимого надзора за этой деятельностью.

В государствах-членах Европейского союза, в том числе в Германии, сложилась сложная многоуровневая система надзорных органов в сфере защиты персональных данных, в которую входят как национальные органы, так и органы Европейского союза.

Согласно статье 55 Общего регламента, каждый национальный надзорный орган уполномочен на территории своего государства осуществлять все полномочия, предоставленные ему данным нормативно-правовым актом¹⁹⁴. Однако в реалиях Европейского союза нередкой является ситуация, когда уполномоченными оказываются сразу несколько надзорных органов разных стран¹⁹⁵. Это создает определенные проблемы, так как в разных государствах может складываться различная правоприменительная практика по тому или иному вопросу. Для предотвращения раздвоения компетенции в Европейском союзе установлен так называемый принцип «One-stop-shop» (механизм единого окна), который применительно к данной теме означает, что оператор, в случае трансграничной обработки, взаимодействует только с национальным органом по своему основному месту предпринимательской деятельности, а уже этот орган (называемый «federführende Aufsichtsbehörde», то есть «ведущее надзорное учреждение»), взаимодействует с соответствующим национальным органом другого государства.

Надзор за соблюдением законодательства о персональных данных на национальном уровне Германии осуществляет федеральный уполномоченный по защите данных и свободы слова (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit). В одном из последних своих заявлений он указал на опасность использования сервиса для видеоконференций «Zoom», так как он не

¹⁹⁴Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронный ресурс] – Режим доступа: <https://dsgvo-gesetz.de/>.

¹⁹⁵Paul Voigt, Axel von dem Bussche. EU-Datenschutz-Grundverordnung (DSGVO) : Praktikerhandbuch / Paul Voigt, Axel von dem Bussche – Berlin – Springer, 2018 – С. 259.

использует технологию сквозного шифрования, что приводит к незащищенности разговора во время хранения его на сервере¹⁹⁶.

Так как Германия является федеральным государством, уполномоченные по защите данных существуют в каждой федеральной земле. Это приводит к тому, что принцип «One-stop-shop» также реализуется на национальном уровне, что закреплено в статье 42 Федерального закона о защите данных¹⁹⁷.

Из анализа главы VIII Общего регламента следует вывод о том, что данным нормативно-правовым актом также предусмотрено два порядка для подачи жалобы субъектом данных: административный (в национальный надзорный орган) и судебный. При этом отдельно оговорена гарантия для субъекта на возможность обжалования решения надзорного органа в судебном порядке¹⁹⁸.

При установлении факта нарушения, к операторам применяются меры ответственности в виде штрафа, размер которых значительно превышает тот, который установлен в российском законодательстве. Так, согласно статье 83 Общего регламента на оператора может быть наложен штраф в размере до 10 000 000 Евро или в размере не более 2% от общего годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше. За отдельные правонарушения возможно наложение штрафа до 20 000 000 Евро или не более 4% от общего годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма больше¹⁹⁹. При этом в каждом отдельном случае при определении размера штрафа надлежит учитывать степень вины оператора; меры, принятые им для предотвращения ущерба; ранее совершенные оператором нарушения; степень сотрудничества им с надзорным

¹⁹⁶ Datenschutz-Beauftragter warnt vor Videokonferenz-Anbieter Zoom [Электронный ресурс] : новости на Welt.de – Режим доступа: <https://www.welt.de/>.

¹⁹⁷ Paul Voigt, Axel von dem Bussche. EU-Datenschutz-Grundverordnung (DSGVO) : Praktikerhandbuch / Paul Voigt, Axel von dem Bussche – Berlin – Springer, 2018 – С. 259.

¹⁹⁸ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронный ресурс] – Режим доступа: <https://dsgvo-gesetz.de/>.

¹⁹⁹ Долинская В.В. Защита прав в сфере персональных данных в России и ЕС / В.В. Долинская // Законы России: опыт, анализ, практика. – 2019. – № 9. – С. 24.

органом; категории персональных данных, затронутых нарушением; уведомлял ли оператор орган о нарушении и другое.

В Федеральном законе о защите данных введены дополнительные штрафы²⁰⁰:

а) за неправомерную передачу большого количества не общедоступных персональных данных третьим лицам виновному лицу может быть назначено лишение свободы на срок до трех лет или штраф. При этом данная норма не ограничена по субъектному составу и распространяется на любое лицо;

б) если лицо из корыстных побуждений или с намерением причинить вред неправомерно получило доступ (или обрабатывало) не общедоступные персональные данные, то к нему может быть применено наказание в виде лишения свободы на срок до двух лет либо штраф. Расследование по данному преступлению, как и по указанному выше в пункте «а», начинается только по жалобе потерпевшего, оператора или надзорного органа;

в) дополнительный состав, предполагающий ответственность в размере до 50 000 Евро, предусмотрен за нарушение обязанности оператора по защите персональных данных в сфере потребительского кредитования.

На уровне Европейского союза также создан особый независимый орган, осуществляющий контроль за соблюдением законодательства о защите персональных данных – Европейский совет по защите данных (Europäischer Datenschutzausschuss), в который входят главы национальных надзорных органов от каждой страны Европейского союза, а также Европейский инспектор по защите персональных данных²⁰¹. Компетенция Европейского совета по защите данных указана в статье 70 Общего регламента и включает в себя в том числе контроль за соблюдением регламента, консультации Европейской комиссии по различным вопросам, издание руководящих указаний, рекомендаций, стандартов передовой практики, дача заключений

²⁰⁰Paul Voigt, Axel von dem Bussche. EU-Datenschutz-Grundverordnung (DSGVO) : Praktikerhandbuch / Paul Voigt, Axel von dem Bussche – Berlin – Springer, 2018 – С. 281.

²⁰¹Paul Voigt, Axel von dem Bussche. EU-Datenschutz-Grundverordnung (DSGVO) : Praktikerhandbuch / Paul Voigt, Axel von dem Bussche – Berlin – Springer, 2018 – С. 281.

национальным надзорным органам по вопросам принятия ими определенных решений и другое²⁰².

Следует отметить, что Общий регламент предполагает применение мер ответственности также к национальному сертифицирующему или надзорному органу за нарушение возложенных на них обязанностей по защите персональных данных²⁰³.

Также органом, который может рассматривать жалобы субъектов данных на нарушение законодательства о персональных данных со стороны государства в Германии является Европейский суд по правам человека, некоторые дела которого рассмотрены выше.

Таким образом, применение мер ответственности является важным элементом механизма защиты персональных данных, который позволяет восстановить нарушенные права, а также действует превентивно, предотвращая возможные новые правонарушения. Исходя из размера устанавливаемых штрафов можно сделать вывод, что как Россия, так и страны Европейского союза серьезно относятся к проблеме нарушения законодательства о персональных данных.

Помимо национальных органов, рассматривающих жалобы субъектов на нарушение законодательства о персональных данных, существуют и международные органы. Нарушения со стороны государства могут стать в том числе и предметом рассмотрения жалобы Европейским судом по правам человека, о чем свидетельствует богатая практика по этому вопросу.

²⁰²Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронный ресурс] – Режим доступа: <https://dsgvo-gesetz.de/>.

²⁰³Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронный ресурс] – Режим доступа: <https://dsgvo-gesetz.de/>.

ЗАКЛЮЧЕНИЕ

В результате написания данной работы были сделаны следующие выводы.

Общественные отношения по защите персональных данных регулируются различными актами как на международном, так и на национальном российском и немецком уровнях.

С вступлением в силу Общего Регламента и «нового» Федерального закона о защите данных эта сфера в Германии стала более систематизирована и получила строгое вертикальное деление: Общий Регламент имеет верховенство и прямое действие, однако в прямо предусмотренных в Регламенте случаях нормы Федерального закона о защите данных ограничивают или дополняют установленные в нем правила.

Российское законодательство о персональных данных представлено различными нормативно-правовыми актами, наиболее систематизированным из которых является ФЗ «О персональных данных».

В России на сегодняшний день на законодательном уровне не существует точного определения понятия персональных данных, не установлено критериев отнесения той или иной информации к персональной. Это влечет за собой отсутствие единства судебной практики и наличие противоречивых позиций в доктрине. В Германии границы понятия персональных данных установлены в Общем Регламенте путем перечисления примерных сведений, относящихся к ним, а также с помощью толкования, данного в Преамбуле к этому нормативно-правовому акту.

На наш взгляд, представляется логичным отнесение к персональным данным всей информации о человеке, то есть максимально широкое толкование данного понятия. Споры в этой части могут возникать лишь при анализе таких специфических сведений, как, например, IP-адрес. При этом механизм защиты персональных данных должен применяться только в отношении той информации, которая в данной ситуации не только позволяет прямо или косвенно идентифицировать конкретное физическое лицо, но и создает

реальную угрозу возможности такой идентификации при определенных условиях. В частности, сбор любых сведений о физическом лице органами государственной власти должен охватываться нормативным регулированием о защите персональных данных ввиду наличия большого потенциала последующей идентификации этого лица путем сопоставления различных сведений из разных государственных баз данных.

Защита персональных данных и в России, и в Германии, является отдельной сферой правового регулирования, хотя и тесно связанной с правом на защиту частной жизни. При этом, в определенных ситуациях, в случае нарушения права на защиту персональных данных, может применяться механизм защиты права на частную жизнь, включая и возможность обращения в Европейский суд по правам человека с жалобой на нарушение статьи 8 Конвенции.

Отличительной особенностью сферы защиты персональных данных является ее «транснациональный» характер, то есть для того, чтобы попасть под регулирование нормативно-правового акта, действующего на определенной территории, необязательно физически присутствовать на данной территории. Оператор персональных данных, находящийся в Германии, но осуществляющий деятельность по обработке персональных данных российских граждан, вынужден обращаться к нормам ФЗ «О персональных данных», равно как и российский оператор должен осуществлять обработку персональных данных граждан Германии в соответствии с Общим Регламентом и Федеральным законом о защите данных. Все это накладывает определенные обременения на предпринимателей, которые вынуждены соблюдать установленные правила, в том числе по причине установления в законодательстве этих стран достаточно больших штрафов. Однако нахождение правонарушителя в другом государстве создает определенные трудности в привлечении к ответственности, ввиду его физической удаленности от надзорных и других правоприменительных органов.

Так как правовое регулирование обработки персональных данных призвано защищать частную сферу человека, что является важной составляющей любого демократического общества и правового государства, обременения предпринимателей (и других операторов) и размер штрафов представляются отвечающими принципам разумности.

Характеризуя принципы обработки персональных данных, права субъектов и обязанности операторов по законодательству России и Германии можно сказать, что, в целом, российское правовое регулирование соответствует европейскому. Об этом свидетельствует схожесть принципов обработки данных и гарантий, предоставляемых субъектам. Отличия заключаются в отдельных обязанностях операторов, а также в механизме реализации конкретных прав субъектов персональных данных.

Кроме того, Общий Регламент и Федеральный закон о защите данных (BDSG) имеют содержательно более логичную и стройную структуру; они перерабатывают и переосмысливают всё существовавшее ранее регулирование в данной сфере, и, тем самым, устанавливают определенные стандарты в области защиты персональных данных, опыт использования которых можно применять для совершенствования российского законодательства.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно-правовые акты

1. Вопросы Федеральной службы по техническому и экспортному контролю [Электронный ресурс] : указ Президента РФ от 16.08.2004 г. № 1085 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.
2. Договор, учреждающий Европейское Сообщество [Электронный ресурс] : от 25.03.1957 с изм. от 16.04.2003 // Право Европейского Союза – Режим доступа: <https://eulaw.ru/>.
3. Европейская конвенция о защите прав человека и основных свобод [Электронный ресурс] : принята 04.11.1950 в Риме // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.
4. Замечание общего порядка № 16 – Статья 17 (право на личную жизнь) [Электронный ресурс] : приняты Комитетом ООН по правам человека на тридцать второй сессии в 1988 г. // Режим доступа: <https://tbinternet.ohchr.org/>.
5. Инструкция о порядке обработки в органах прокуратуры Российской Федерации персональных данных, полученных в связи с осуществлением прокурорского надзора [Электронный ресурс] : утв. приказом Генерального прокурора Российской Федерации от 22.11.2013 г. №506 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.
6. Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс] : федер. закон от 30.12.2001 № 195-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.
7. Конституция Российской Федерации [Электронный ресурс] : принята всенародным голосованием 12.12.1993 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

8. О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях [Электронный ресурс] :федер. закон от 21.07.2014 г. № 242-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

9. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации [Электронный ресурс] :федер. закон от 13.07.2015 № 264-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

10. О вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки [Электронный ресурс] : разъяснения Роскомнадзора – Режим доступа: <https://rkn.gov.ru/>.

11. О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации [Электронный ресурс] :федер. закон от 08.06.2020 № 168-ФЗ // Справочная правовая система «КонсультантПлюс» - Режим доступа: <http://consultant.ru/>.

12. О защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс] : конвенция от 28.01.1981 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

13. О персональных данных [Электронный ресурс] :федер. закон от 27.07.2006 № 152-ФЗ ред. от 31.12.2017 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

14. О применении судами общей юрисдикции Конвенции о защите прав человека и основных свобод от 4 ноября 1950 года и Протоколов к ней [Электронный ресурс] : постановление Пленума Верховного суда от 27.06.2013 № 21 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

15. О применении судами общей юрисдикции общепризнанных принципов и норм международного права и международных договоров Российской Федерации [Электронный ресурс] : постановление Пленума Верховного суда от 10.10.2003 № 5 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

16. О присвоении физлицу ИНН и его применении [Электронный ресурс] : письмо Министерства финансов № 03-01-11/76554 от 25.10.2018 // Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

17. О прокуратуре Российской Федерации [Электронный ресурс] : федер. закон от 17.01.1992 № 2202-1 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

18. О ратификации Конвенции о защите прав человека и основных свобод и Протоколов к ней [Электронный ресурс] : федер. закон от 30.02.1998 № 54-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

19. О связи [Электронный ресурс] : федер. закон от 07.07.2003 № 126-ФЗ ред. от 18.04.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

20. О средствах массовой информации [Электронный ресурс] : закон РФ от 27.12.1991 № 2124-1 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

21. О Федеральной службе безопасности [Электронный ресурс] : федер. закон от 03.04.1995 г. № 40-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

22. О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] : постановление Правительства РФ от 16.03.2009 № 228 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

23. Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ ред.

от 03.04.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

24. Об обработке персональных данных в Арбитражном суде Красноярского края [Электронный ресурс] : приказ от 05.06.2018 № 93 – Режим доступа: <https://krasnoyarsk.arbitr.ru/>.

25. 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 [Электронный ресурс] : постановление Правительства РФ от 30.06.2018 № 772 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

26. Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных [Электронный ресурс] : приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 15.03.2013 г. № 274 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

27. Об утверждении перечня сведений конфиденциального характера [Электронный ресурс] : указ Президента РФ от 06.03.97 № 188 // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

28. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс] : постановление Правительства РФ от 01.11.2012 № 1119 // Справочная

правовая система «КонсультантПлюс». – Режим доступа:
<http://www.consultant.ru/>.

29. Описание бланка паспорта гражданина РФ [Электронный ресурс] : утв. постановлением Правительства РФ от 8.07.1997 г. № 828 // Справочная правовая система «КонсультантПлюс». – Режим доступа:
<http://www.consultant.ru/>.

30. Положение о порядке ведения кассовых операций с банкнотами и монетой Банка России на территории Российской Федерации [Электронный ресурс] : утв. Банком России от 12.11.2011 № 373-П (утратило силу) // Справочная правовая система «КонсультантПлюс». – Режим доступа:
<http://www.consultant.ru/>.

31. Право на неприкосновенность частной жизни в цифровой век [Электронный ресурс] : доклад Верховного комиссара Организации Объединенных Наций по правам человека от 3 августа 2018 г. // Режим доступа:
<https://documents-dds-ny.un.org>.

32. Право на неприкосновенность частной жизни в цифровую эпоху [Электронный ресурс] : резолюция Генеральной Ассамблеи ООН № 73/179 от 17 декабря 2018 г. // Режим доступа: <https://undocs.org>.

33. Разъяснения Роскомнадзора по вопросу применения законодательства о персональных данных // [Электронный ресурс] – Режим доступа: <https://rkn.gov.ru/>.

34. Уголовный кодекс Российской Федерации [Электронный ресурс] : федер. закон от 13.06.1996 № 63-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

35. Хартия Европейского союза об основных правах [Электронный ресурс] : от 07.12.2000 // Право Европейского Союза – Режим доступа:
<https://eulaw.ru/>.

36. Bayerisches Datenschutzgesetz (BayDSG) [Электронный ресурс] : от 15.05.2018 // Bayern.Recht – Режим доступа: <https://www.gesetze-bayern.de/>.

37. Bundesdatenschutzgesetz (BDSG) [Электронный ресурс] // Gesetze im Internet – Режим доступа: <https://www.gesetze-im-internet.de/>.

38. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [Электронный ресурс] // EUR-Lex– Режим доступа: <https://eur-lex.europa.eu/>.

39. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Электронный ресурс] – Режим доступа: <https://dsgvo-gesetz.de/>.

Акты российских, немецких и международных судов

40. Апелляционное определение Волгоградского областного суда от 24.04.2014 № 33-4427/2014 [Электронный ресурс] // Интернет-ресурс Судебные и нормативные акты РФ – Режим доступа: <http://www.sudact.ru/>.

41. Апелляционное определение Московского городского суда от 10.04.2014 № 33-11688 [Электронный ресурс] – Режим доступа: <https://www.mos-gorsud.ru/>.

42. Апелляционное определение Московского городского суда от 12.12.2016 по делу № 33-42101/2016 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

43. Апелляционное определение Московского городского суда от 16 ноября 2016 г. по делу № 33-45367/2016 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

44. Апелляционное определение Московского городского суда от 22 мая 2014 по делу № 33-14709 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

45. Апелляционное определение Новосибирского областного суда от 27 сентября 2016 г. № 33-9626/2016 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

46. Апелляционное определение Санкт-Петербургского городского суда № 2-3097/2014 33-1644/2015 от 3 февраля 2015 г. по делу № 2-3097/2014 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

47. Апелляционное определение Санкт-Петербургского городского суда от 31.01.2017 № 33а-1151/2017 по делу № 2а-4760/2016 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

48. Апелляционное определение Санкт-Петербургского городского суда от 15.11.2016 № 33-22976/2016 по делу № 2-2932/2015 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

49. Определение Конституционного Суда РФ от 17 июня 2013 г. № 979-О // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

50. Определение Конституционного Суда РФ от 16 июля 2013 г. № 1176-О [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

51. Определение Конституционного суда РФ от 17 июля 2012 г. № 1346-О [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

52. Определение Конституционного Суда РФ от 24 декабря 2013 г. № 2128-О [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

53. Определение Конституционного Суда РФ от 26 января 2010 года № 158-О-О [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

54. Определение Конституционного Суда РФ от 9 июня 2005 года № 248-О [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

55. Определение Приморского краевого суда № 33-11759/2014 33-470/2015 от 19 января 2015 г. [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

56. Определение Приморского краевого суда от 28 апреля 2014 г. по делу № 33-3718 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

57. Определение судебной коллегии по гражданским делам Московского городского суда от 29 февраля 2012 г. № 33-6709 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

58. Определения Верховного Суда РФ от 24.06.2015 № 18-АПГ15-7 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

59. Постановление Верховного суда РФ от 13 августа 2015 г. № 302-АД15-5169 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

60. Постановление Верховного суда РФ от 15 июня 2016 г. № 25-АД15-3 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

61. Постановление девятнадцатого арбитражного апелляционного суда от 29 апреля 2015 г. по делу № А36-5713/2014 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

62. Постановление Европейского Суда по правам человека по делу [Centrumförrättvisav. Sweden] от 19.06.2018 (жалоба № 35252/08) [Электронный ресурс] – Режим доступа: <https://hudoc.echr.coe.int/>.

63. Постановление Европейского Суда по правам человека по делу «Benedikv. Slovenia» от 24.07.2018 (жалоба № 62357/14) [Электронный ресурс] – Режим доступа: <https://hudoc.echr.coe.int/>.

64. Постановление Европейского Суда по правам человека по делу «P.G. and J.H. v. The United Kingdom» от 25.09.2001 (жалоба № 44787/98) [Электронный ресурс] // Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

65. Постановление Европейского Суда по правам человека по делу «S. и Марпер против Соединенного Королевства» [S. and Marper v. The United Kingdom] от 04.12.2008 (жалобы № 30562/04 и № 30566/04). [Электронный ресурс] – Режим доступа: <http://www.echr.ru/>.

66. Постановление Европейского Суда по правам человека по делу «Vetter v. France» от 31.05.2005 (жалоба № 59842/00) [Электронный ресурс] // Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

67. Постановление Европейского Суда по правам человека по делу «Бигаева против Греции» [Bigaev v. Greece] от 28 мая 2009 г. (жалоба № 26713/05) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

68. Постановление Европейского Суда по правам человека по делу «Ван дер Хейден против Нидерландов» [VanderHeijden v. Netherlands] от 3 апреля 2012 г. (жалоба № 42857/05) [Электронный ресурс] // Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

69. Постановление Европейского Суда по правам человека по делу «Зубков и другие против Российской Федерации» от 07.11.2017 (жалоба № 29431/05) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

70. Постановление Европейского Суда по правам человека по делу «Иващенко против России» от 13.05.2018 (жалоба № 61064/10) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

71. Постановление Европейского Суда по правам человека по делу «Константин Москалев против Российской Федерации» от 07.11.2017 (жалоба № 59589/10) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

72. Постановление Европейского Суда по правам человека по делу «Копланд против Соединенного Королевства» [Copland v. the United Kingdom] от 03.04.2007 (жалоба № 62617/00) [Электронный ресурс] // Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

73. Постановление Европейского Суда по правам человека по делу «Нимитц против Германии» [Niemietz v. Germany] от 16 декабря 1992 г. (жалоба № 13710/88) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

74. Постановление Европейского Суда по правам человека по делу «Роман Захаров против России» от 04.12.2015 (жалоба № 47143/06) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

75. Постановление Европейского Суда по правам человека по делу «Узун против Германии» [Uzun v. Germany] от 02.09.2010 (жалоба № 35623/05) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

76. Постановление Европейского Суда по правам человека по делу «Шимоволос против России» от 21.06.2011 (жалоба № 30194/09) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

77. Постановление Нижегородского областного суда от 12 мая 2015 г. № 4а-288/2015 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

78. Постановление Президиума Высшего арбитражного суда РФ от 5 октября 2010 г. № 6336/10 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

79. Постановление Тринадцатого арбитражного апелляционного суда от 01.06.2015 № 13АП-10709/2015 по делу № А56-75017/2014 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

80. Постановление Тринадцатого арбитражного апелляционного суда от 01.06.2015 № 13АП-10709/2015 по делу № А56-75017/2014 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

81. Постановление Тринадцатого арбитражного апелляционного суда от 21 июня 2010 г. по делу № А56-4788/2010 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

82. Решение арбитражного суда республики Татарстан от 20 мая 2019 г. по делу № А65-4973/2019 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

83. Решение Арбитражного суда Челябинской области по делу № А76-29008/2015 от 11.02.2016 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

84. Решение Верховного Суда РФ от 11.03.2013 № АКПИ13-61 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

85. Решение Заельцовского районного суда г. Новосибирска № 2-1770/2018 2-1770/2018 ~ М-987/2018 М-987/2018 от 27 июня 2018 г. по делу №

2-1770/2018 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

86. Решение Красноярского краевого суда № 7П-428/2017 от 14 сентября 2017 г. по делу № 7П-428/2017 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

87. Решение Московского городского суда по делу №33-15365 [Электронный ресурс] // официальный сайт московского городского суда. – Режим доступа: <https://www.mos-gorsud.ru/>.

88. Решение Октябрьского районного суда г. Красноярска № 2-3904/2019 2-3904/2019~М-966/2019 М-966/2019 от 26 августа 2019 г. по делу № 2-3904/2019 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru/>.

89. Решение Таганского районного суда №2-3491/2016 [Электронный ресурс] // официальный сайт московского городского суда. – Режим доступа: <https://www.mos-gorsud.ru/>.

90. BVerfG, Urteilv. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83 [Электронный ресурс] – Режим доступа: <https://dejure.org/>.

91. BGHZ 13, 334 (338) [Электронный ресурс] – Режим доступа: <https://www.servat.unibe.ch/>.

92. BGHZ 26, 349 (354) [Электронный ресурс] – Режим доступа: <https://www.servat.unibe.ch/>.

93. Judgment of the Court (Third Chamber) 24 November 2011 in Case C-70/10 [Электронныйресурс] – Режимдоступа: <http://curia.europa.eu/>.

94. Judgment of the Court (Second Chamber) 19 October 2016 [Электронныйресурс] // EUR-Lex – Режимдоступа: <https://eur-lex.europa.eu/>.

95. Judgment of the Court (Grand Chamber), 13 May 2014. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. [Электронный ресурс] – Режим доступа: <https://eur-lex.europa.eu/>.

96. Verwaltungsgericht Wiesbaden am 18. Januar 2008 (AZ 6 E 1559/06) [Электронный ресурс] – Режим доступа: <https://openjur.de/>.

Научная литература

97. Болотин, В. С., Маслѐха, М. А. Механизм защиты права на неприкосновенность частной жизни при обработке персональных данных в информационных системах / В. С. Болотин, М. А. Маслѐха. // Вестник государственного и муниципального управления. – 2012. – №3. – С. 99–103.

98. Вуколова, Т. Законодательство о персональных данных в Германии и России. Сравнительно-правовое исследование. / Т. Вуколова // Интеллектуальная собственность. Авторское право и смежные права – 2016 – №4 – С. 15–30.

99. Горелихина О.А., Шлиньков А.А. Правовая защита персональных данных в Германии / О.А. Горелихина, А.А. Шлиньков // Вопросы экономики и права. – 2012. – № 3 – С. 27-32.

100. Грибанов, А.А. Общий регламент о защите персональных данных (GeneralDataProtectionRegulation) : идеи для совершенствования российского законодательства / А.А. Грибанов // Закон. – 2018. – № 3. – С. 149–162.

101. Добрикова, Е. Особенности применения закона о локализации персональных данных на практике: рекомендации для бизнеса. [Электронный ресурс] / Е. Добрикова // Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

102. Долинская В.В. Защита прав в сфере персональных данных в России и ЕС / В.В. Долинская // Законы России: опыт, анализ, практика. – 2019. – № 9. – С. 22–29.

103. Долинская, В.В. Информационные отношения в гражданском обороте / В.В. Долинская // Законы России: опыт, анализ, практика. – 2010. – № 4. – С. 3–14.

104. Жердина, С.Ю., Двенадцатова, Т.И. Защита персональных данных: первые итоги и перспективы судебных дел / С.Ю. Жердина, Т.И. Двенадцатова // Журнал «Акционерное общество» – 2017. – №11. – С. 73–79.

105. Иванский В.П. Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования: монография / В.П. Иванский. – Москва : РУДН, 1999. – 276 с.

106. Кадников, Б.Н. Уголовно-правовая охрана неприкосновенности частной жизни : научно-практическое пособие / под ред. Н.Г. Кадникова. – Москва : Юриспруденция, 2011. – 120 с.

107. Кафтанникова, В. М. Принципы защиты персональных данных в России и за рубежом / В. М. Кафтанникова // Вестник ЮУрГУ. Серия «Право» – 2013 – Т. 13, № 2 – С. 99–100.

108. Миндубаев, Р. Р. Полномочия ЕС по принятию собственных правовых актов / Р. Р. Миндубаев // Актуальные проблемы права: материалы междунар. науч. конф. / Ваш полиграфический партнер – Москва, 2011. – С. 132–135.

109. Михайлова, И.А. Персональные данные и их правовая охрана: некоторые проблемы теории и практики / И.А. Михайлова // Законы России: опыт, анализ, практика. – 2017. – № 10. – С. 11–18.

110. О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях [Электронный ресурс] : комментарий к Федеральному закону от 21 июля 2014 г. № 242-ФЗ // официальный сайт Роскомнадзора. – Режим доступа: <https://pd.rkn.gov.ru/>.

111. Оганесян, Т. Д. Защита персональных данных: позиции международных судов / Т. Д. Оганесян // Российское правосудие. – 2019 – № 6 – С. 47–56.

112. Павлинов А. А. Уголовная ответственность за нарушение неприкосновенности частной жизни / А.А. Павлинов // Пробелы в российском законодательстве. – 2013. – №6. – С. 187–191.

113. Петрыкина, Н.И. Правовое регулирование оборота персональных данных. Теория и практика : монография / Н.И. Петрыкина. – Москва : Статут, 2011. – 138 с.

114. Приезжева, А.А. Федеральный закон «О персональных данных»: научно-практический комментарий. / А.А. Приезжева. – Москва : Редакция «Российской газеты», 2015. – № 11. – 176 с.

115. Проскурякова, М.И. Персональные данные: российская и германская национальные модели конституционно-правовой защиты в сравнительной перспективе / М.И. Проскурякова // Сравнительное конституционное обозрение. – 2016 – № 6. – С. 84–98.

116. Рузанова, В.Д. Проблемы соотношения защиты права на неприкосновенность частной жизни и права на защиту персональных данных / В.Д. Рузанова // Законы России: опыт, анализ, практика. – 2019. – № 9. – С. 17–22.

117. Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». / А.И. Савельев. – Москва : Статут, 2017. – 320 с.

118. Соколова, О.С. Защита персональных данных посредством права на забвение / О.С. Соколова // Современное право. – 2016. – № 9. – С. 69–72.

119. Сыченко, Е. Прослушивание рабочего телефона, обыск служебных помещений и съемка работника на видео: практика Европейского суда по правам человека [Электронный ресурс] / Е. Сыченко // Административное право – № 1, – I квартал 2015 г. / Справочная правовая система «Гарант». – Режим доступа: <http://www.garant.ru/>.

120. Талапина, Э. В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте. / Э. В. Талапина // Труды Института государства и права РАН. – 2018. – Т.13, № 5. – С.117–150.

121. Терещенко, Л.К. Модернизация информационных отношений и информационного законодательства : монография / Л.К Терещенко. – Москва : ИНФРА-М, 2013 – 227 с.

122. Федосин, А.С. Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации :автореф. ... дис. канд. юрид. наук : 12.00.14 / Федосин Алексей Сергеевич – Москва, 2009 – 28 с.

123. Фомина, Л.Ю. Международные стандарты защиты персональных данных в условиях информационного общества / Л. Ю. Фомина // Международное право. – 2019. – № 4. – С. 50 – 59.

124. Чурилов, А.Ю. Принципы Общего регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации / А.Ю. Чурилов// Вестник Омской юридической академии. – 2019. – № 1. – С. 29–35.

125. Paul Voigt, Axel von dem Bussche. EU-Datenschutz-Grundverordnung (DSGVO) :Praktikerhandbuch / Paul Voigt, Axel von dem Bussche – Berlin – Springer, 2018 – 538 с.

126. Sven Hunzinger. Das Löschen im Datenschutzrecht / Sven Hunzinger – Baden-Baden : Nomos, 2018. – 332 с.

Иные источники

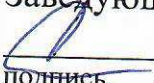

127. Статистика по вопросу безопасности в интернете [Электронный ресурс] : официальный сайт Фонда общественного мнения – Режим доступа: <https://fom.ru/>.

128. ЦБ впервые раскрыл масштаб продаж персональных данных россиян [Электронный ресурс] // Официальный сайт РБК. – Режим доступа <https://www.rbc.ru/>.

129. Datenschutz-Beauftragterwarntvor Videokonferenz-AnbieterZoom [Электронныйресурс] :новостинаWelt.de – Режимдоступа: <https://www.welt.de/>

130. Inwieweit stimmen Sie den folgenden Aussagen zum Thema Datenschutz und Sicherheit im Internet zu? [Электронный ресурс] : статистика по вопросу безопасности Интернета в Германии // Режим доступа: <https://de.statista.com/>.

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Юридический институт
кафедра международного права

УТВЕРЖДАЮ
Заведующий кафедрой

подпись Т. Ю. Сидорова
инициалы, фамилия
«  » 2020 г.

БАКАЛАВРСКАЯ РАБОТА

40.03.01.01 «Международное и иностранное право»
код – наименование направления

Защита персональных данных: сравнительный аспект России и Германии
тема

Научный руководитель


подпись,
дата

К.Ю.Н., доцент
должность, ученая
степень

В. В. Терешкова
инициалы, фамилия

Выпускник


подпись,
дата

16151003
номер зачетной
книжки

М. А. Попов
инициалы, фамилия

Красноярск 2020