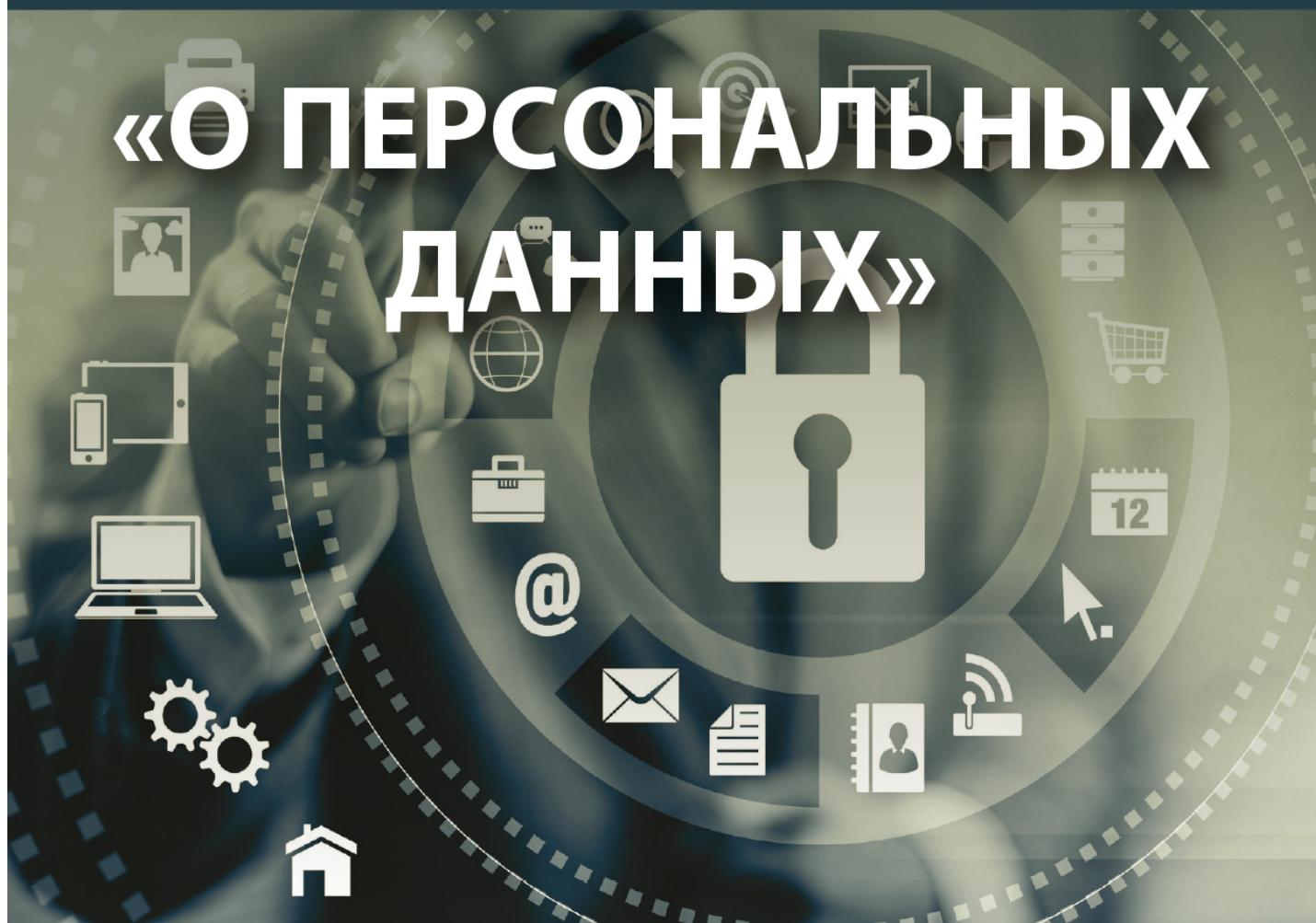


А.И. Савельев

Научно-практический постатейный комментарий  
к Федеральному закону

# «О ПЕРСОНАЛЬНЫХ ДАННЫХ»



Александр Савельев

**Научно-практический  
постатейный комментарий  
к Федеральному закону  
«О персональных данных»**

«Статут»

2017

УДК 342.7  
ББК 67.400.32

**Савельев А. И.**

Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» / А. И. Савельев — «Статут», 2017

ISBN 978-5-8354-1365-2

Настоящий научно-практический комментарий к Федеральному закону «О персональных данных» подготовлен с учетом последних изменений, внесенных в него в том числе Федеральным законом от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях». При подготовке комментария учтены положения соответствующих подзаконных актов, а также последние изменения в КоАП РФ в части административной ответственности за нарушение законодательства о персональных данных. Использована отечественная судебная практика, разъяснения Минкомсвязи России и Роскомнадзора по вопросам применения законодательства о персональных данных. Ряд положений Закона о персональных данных анализируется в сравнении с европейским законодательством, включая недавно принятый General Data Protection Regulation и правовые позиции Европейского Суда Справедливости. Комментарий рассчитан на практикующих юристов, научных работников, студентов и аспирантов, а также всех интересующихся проблематикой защиты персональных данных. Тексты нормативных правовых актов приведены по состоянию на 15 марта 2017 г.

УДК 342.7  
ББК 67.400.32

ISBN 978-5-8354-1365-2

© Савельев А. И., 2017

© Статут, 2017

## Содержание

Список сокращений	6
Введение	7
Глава 1. Общие положения	9
Статья 1. Сфера действия настоящего федерального закона	9
Статья 2. Цель настоящего федерального закона	22
Конец ознакомительного фрагмента.	28

# Савельев А.И.

## Научно-практический постатейный комментарий к Федеральному закону «О персональных данных»

### Список сокращений

*ЕСПЧ* – Европейский суд по правам человека

*Суд ЕС* – Европейский суд справедливости

*ГК РФ* – Гражданский кодекс Российской Федерации (часть первая от 30 ноября 1994 г. № 51-ФЗ; часть вторая от 26 января 1996 г. № 141-ФЗ; часть третья от 26 ноября 2001 г. № 146-ФЗ; часть четвертая от 18 декабря 2006 г. № 230-ФЗ)

*Закон об информации* – Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

*Закон о персональных данных* – Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

*Директива 1995 г.* – Директива 95/46/ЕС от 24 октября 1995 г. о защите прав физических лиц применительно к обработке персональных данных и о свободном движении таких данных

*КоАП РФ* – Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ

*Конвенция 1981 г.* – Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных». Заключена в г. Страсбурге (Франция) 28 января 1981 г.

*Минкомсвязи России* – Министерство связи и массовых коммуникаций Российской Федерации

*ОЭСР* – Организация по экономическому сотрудничеству и развитию *Регламент 2016 г.* – Регламент ЕС 2016/679 от 27 апреля 2016 г. о защите прав физических лиц применительно к обработке персональных данных, о свободном движении таких данных и об отмене Директивы 95/46/ЕС (General Data Protection Regulation, GDPR)

*Роскомнадзор* – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

*Руководящие принципы ОЭСР* – Руководящие принципы ОЭСР по защите частной жизни и трансграничного обмена персональными данными 1980 г. (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)

*ТК РФ* – Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ

*УК РФ* – Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ

*УПК РФ* – Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ

## Введение

Законодательство о персональных данных и практика его применения в Российской Федерации претерпели значительную эволюцию за последние годы. То, что ранее не вызывало особого интереса у большей части участников оборота и воспринималось ими как очередная бюрократическая формальность, сейчас превратилось в одно из наиболее обсуждаемых на самых различных площадках и самом высоком государственном уровне направлений развития законодательства. Во многом это связано с общим курсом государства на обеспечение цифрового суверенитета, в рамках которого регулирование оборота информации приобретает ключевое значение. Одним из проявлений данного курса стали нашумевшие поправки о локализации отдельных процессов обработки персональных данных российских граждан. Данные поправки спровоцировали не только шквал дискуссий и различных интерпретаций, но и необходимость переосмысления базового терминологического аппарата законодательства в контексте новых технологических реалий: понятия персональных данных, понятия оператора и лица, осуществляющего обработку персональных данных по его поручению, трансграничной передачи данных, обезличенных данных и т.п. Кроме того, особую актуальность приобрели вопросы обеспечения электронного взаимодействия оператора и субъекта персональных данных, в частности, при получении согласия на обработку таких данных, предоставлении необходимой информации о порядке ее обработки и т.п.

В связи с вышеизложенным при подготовке данного комментария были учтены не только судебная практика по вопросам применения законодательства о персональных данных, но и общедоступные разъяснения Минкомсвязи России и Роскомнадзора. При этом особое внимание уделяется определению сферы применения законодательства о персональных данных, в том числе в сети «Интернет», а также существующим интерпретациям ключевых дефиниций законодательства о персональных данных, сфере применения предусмотренных законом оснований для обработки персональных данных различных категорий и обязанностям, возлагаемым на оператора. Кроме того, в комментарии учтены недавние изменения в КоАП РФ, касающиеся увеличения ответственности операторов за нарушение законодательства о персональных данных, а также положения соответствующих нормативных-правовых актов, регламентирующих порядок осуществления контрольно-надзорной деятельности в сфере законодательства о персональных данных.

При этом следует отметить, что законодательство о персональных данных развивается не только в России, но и в Европе, где совсем недавно был принят новый Общеевропейский регламент по защите персональных данных (*General Data Protection Regulation*), который в 2018 г. сменит устаревшую, но все еще выступающую своего рода эталоном законодательного регулирования защиты персональных данных Директиву ЕС 1995 г.

В ходе данной реформы было затронуто множество вопросов, связанных с вызовами, которые бросают новые технологии защите частной жизни граждан: распространение персональных данных в сети «Интернет» социальными сетями, использование инструментов аналитики «больших данных» и профайлинга, трансграничный характер обработки персональных данных при использовании «облачных» сервисов, информационная «перегруженность» потребителей и пр. Существует достаточно большой пласт решений Европейского Суда Справедливости по вопросам применения отдельных положений законодательства о персональных данных, где многие из указанных проблем были предметом глубокого анализа. В этой связи европейский опыт может быть особенно полезным для России, учитывая не только общность проблем, но и общность законодательства, обусловленную общими корнями – положениями Конвенции Совета Европы 1981 г. № 108 «О защите физических лиц при автоматизированной обработке персональных данных». Европейское законодательство представляет интерес

для российского читателя еще и потому, что оно носит экстерриториальный характер и распространяется не только на европейских операторов, но и на иностранных лиц, что особенно актуально, принимая во внимание трансграничный характер электронной коммерции.

В связи с вышеизложенным в настоящем комментарии осуществлено сравнение ряда положений российского законодательства с европейскими нормами: как с ныне действующими, так и с вступающими в силу в 2018 г. При этом в комментарии также приводятся и правовые позиции Европейского Суда Справедливости, которые, по мнению автора, могут быть применимы и в российских реалиях в силу сходства соответствующих правовых норм. Это позволяет обеспечить комплексный и сбалансированный подход к рассмотрению проблем применения законодательства о персональных данных в цифровой среде.

Автор выражает признательность коллегам по Консультативному Совету при Роскомнадзоре, в особенности – заместителю руководителя Роскомнадзора Антонине Аркадьевне Приезжевой и начальнику Управления по защите прав субъектов персональных данных Юрию Евгеньевичу Контемирову, без которых этот комментарий вряд ли был бы написан. Особо хотелось бы поблагодарить и другого коллегу по Консультативному Совету – доцента кафедры теории и истории государства и права СПбГУ Владислава Владимировича Архипова за ценные дискуссии и высказанное мнение по ряду вопросов, отраженных в данном комментарии.

Настоящий комментарий подготовлен в ходе проведения исследования в рамках Программы фундаментальных исследований Национального исследовательского университета «Высшая школа экономики» (НИУ ВШЭ) с использованием средств субсидии в рамках государственной поддержки ведущих университетов Российской Федерации «5-100». Высказанные в работе суждения являются личным мнением автора и могут не совпадать с официальной позицией компании IBM, НИУ ВШЭ или какой-либо иной организации.

**27 июля 2006 года № 152-ФЗ**

## **РОССИЙСКАЯ ФЕДЕРАЦИЯ ФЕДЕРАЛЬНЫЙ ЗАКОН**

### **О ПЕРСОНАЛЬНЫХ ДАННЫХ**

*Принят*

*Государственной Думой*

*8 июля 2006 года*

*Одобрено*

*Советом Федерации 14 июля 2006 года*

**(В ред. федеральных законов от 25.11.2009 № 266-ФЗ, от 27.12.2009 № 363-ФЗ, от 28.06.2010 № 123-ФЗ, от 27.07.2010 № 204-ФЗ, от 27.07.2010 № 227-ФЗ, от 29.11.2010 № 313-ФЗ, от 23.12.2010 № 359-ФЗ, от 04.06.2011 № 123-ФЗ, от 25.07.2011 № 261-ФЗ, от 05.04.2013 № 43-ФЗ, от 23.07.2013 № 205-ФЗ, от 21.12.2013 № 363-ФЗ, от 04.06.2014 № 142-ФЗ, от 21.07.2014 № 216-ФЗ, от 21.07.2014 № 242-ФЗ, от 03.07.2016 № 231-ФЗ, от 22.02.2017 № 16-ФЗ)**



## Глава 1. Общие положения

### Статья 1. Сфера действия настоящего федерального закона

1. Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее – государственные органы), органами местного самоуправления, иными муниципальными органами (далее – муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

2. Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

3) утратил силу. – Федеральный закон от 25 июля 2011 № 261-ФЗ;

4) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

5) предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом от 22 декабря 2008 года № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

1. Несмотря на название комментируемая статья определяет лишь *предметную* сферу действия комментируемого Закона, а именно отношения, на которые он распространяется, а также перечень изъятий из сферы его действия. Сфера действия данного Закона во времени определяется в его ст. 25. К сожалению, комментируемый Закон никак не конкретизирует сферу своего действия в пространстве, что особенно актуально для определения круга иностранных лиц, на которых распространяются его требования. Как следствие, территориальная сфера действия настоящего Закона определяется посредством системного толкования положений иных законов и конкретизирована в разъяснениях Минкомсвязи России, которое является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере обработки персональных данных и уполномоченным на дачу разъяснений по указанным вопро-

сам<sup>1</sup>. Данные разъяснения опубликованы на официальном сайте Минкомсвязи России<sup>2</sup> и будут предметом подробного анализа далее.

1.1. Предметная сфера действия законодательства РФ о персональных данных определена в комментируемой статье посредством указания на два основных признака правоотношений:

- 1) наличие связи таких отношений с процессами обработки персональных данных;
- 2) использование средств автоматизации или иных средств, которые по своему характеру схожи с ними и позволяют осуществлять поиск персональных данных в соответствии с заданным алгоритмом.

Первый признак имеет место всегда, когда положительно решен вопрос о квалификации выступающей объектом правоотношения информации в качестве персональных данных, поскольку существующая дефиниция обработки персональных данных охватывает любые действия, совершаемые с ними (о понятиях персональных данных и их обработки см. комментарий к ст. 3 Закона о персональных данных).

Второй признак имеет место во всех случаях автоматизированной обработки, т.е. использования средств вычислительной техники для обработки персональных данных (компьютеров, планшетов, смартфонов, «умных часов», устройств, подключенных к сети «Интернет», и т.п.). Фактически об автоматизированной обработке персональных данных можно вести речь всегда, когда такие данные выражены в цифровой форме.

Кроме того, рассматриваемый признак имеет место при осуществлении «неавтоматизированной» обработки персональных данных, удовлетворяющей в совокупности следующим условиям (далее – квази-автоматизированная обработка):

- а) поиск и (или) доступ к таким данным осуществляется в соответствии с определенным алгоритмом, что предполагает наличие систематизации соответствующих документов по конкретным критериям (например, по фамилиям в алфавитном порядке и (или) по годам);
- б) использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных осуществляются при непосредственном участии человека независимо от того, хранятся такие сведения в информационной системе персональных данных или нет<sup>3</sup>.

1.2. В отсутствие систематизации документов по определенным критериям невозможно осуществление действий с ними по определенному алгоритму, а следовательно, такие действия не могут по своему характеру соответствовать действиям, осуществляемым при автоматизированной обработке, и не подпадают под действие Закона о персональных данных. При этом следует подчеркнуть, что буквальное толкование ч. 1 комментируемой статьи позволяет сделать вывод о том, что требование о наличии алгоритма установлено в виде альтернативы применительно как к *поиску*, так и к *доступу* к соответствующим данным, а не только к поиску, как иногда указывается в литературе<sup>4</sup>. Кроме того, настоящий Закон прямо указывает на то, что речь идет о доступе к «таким данным», отсылая тем самым к предыдущей фразе, в которой речь идет о «зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных». Иными словами, *к хранению и иным видам обработки несистематизированных персональных данных без использования*

---

<sup>1</sup> См. п. 1 и 6.6 Положения о Министерстве связи и массовых коммуникаций Российской Федерации, утв. постановлением Правительства РФ от 2 июня 2008 г. № 418 «О Министерстве связи и массовых коммуникаций Российской Федерации» // СПС «КонсультантПлюс».

<sup>2</sup> <http://www.minsvyaz.ru/ru/personaldata/>.

<sup>3</sup> Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

<sup>4</sup> См.: Федеральный закон «О персональных данных»: Научно-практический комментарий / Под ред. зам. руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций А.А. Приезжевой. М., 2015. С. 8–9.

*средств автоматизации Закон о персональных данных не применяется*, даже если к таким сведениям возможен последующий доступ третьих лиц.

1.3. Примером квази-автоматизированной обработки, подпадающей под действие комментируемого Закона, являются действия оператора, связанные с ведением различного рода картотек личных дел сотрудников организации; договоров, заключенных с физическими лицами; медицинских карт пациентов в регистратурах поликлиник; журналов выдачи одно-разовых пропусков на территорию и т.п. При этом если персональные данные, содержащиеся в «бумажных» документах и систематизированные в картотеках, параллельно используются, уточняются, распространяются или уничтожаются с помощью средств вычислительной техники (например, при использовании программных продуктов по расчету зарплат и управлению персоналом), то имеет место так называемая смешанная обработка – обработка, осуществляемая оператором без использования средств автоматизации и автоматизированным способом одновременно. Данный термин хотя и не фигурирует в законе, но используется на практике контрольно-надзорными органами и судами (см.: Постановление Четвертого арбитражного апелляционного суда от 17 января 2011 г. по делу № А19-25289/2009; Апелляционное определение Владимирского областного суда от 20 января 2015 г. по делу № 33-139/2015; п. 9 Рекомендаций Роскомнадзора по заполнению формы уведомления об обработке (о намерении осуществлять обработку) персональных данных от 29 января 2016 г.). Несмотря на то что в данном случае оба средства обработки подпадают под действие Закона о персональных данных, существуют определенные отличия в правовых последствиях их осуществления, которые необходимо учитывать, например, в части наличия или отсутствия обязанности по уведомлению Роскомнадзора об обработке персональных данных (см. подробнее комментарий к ст. 22 настоящего Закона). При этом следует учитывать п. 2 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, в соответствии с которым «обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее».

1.4. Если деятельность по обработке персональных данных не сопряжена с использованием автоматизированных или квази-автоматизированных средств обработки, то она в соответствии с ч. 1 комментируемой статьи не подпадает под действие Закона о персональных данных. Например, если осуществляется обработка персональных данных контрагента по «бумажному» договору при оформлении дополнительных документов к нему (актов, дополнительных соглашений, договоров уступки) без использования вычислительных средств, а также без внесения этих документов в систематизированные картотеки (Постановление Двадцатого арбитражного апелляционного суда от 12 июля 2016 г. № 20АП-3775/2016 по делу № А23-4903/2012).

По тем же причинам не подпадают под действие Закона о персональных данных устное разглашение личных сведений о физическом лице в присутствии третьих лиц (Апелляционное определение Курганского областного суда от 27 марта 2014 г. по делу № 33-929/2014) и разглашение личных данных посредством направления письма, содержащего их, в адрес третьих лиц (Кассационное определение Саратовского областного суда от 7 февраля 2012 г. по делу № 33-697). Однако если указанные действия совершались с использованием вычислительных средств, например, посредством сети «Интернет», то они по общему правилу подпадают под действие Закона о персональных данных.

1.5. В судебной практике сформировалась позиция, согласно которой действие Закона о персональных данных не распространяется на «отношения по собиранию, проверке, хранению сведений в процессе возбуждения, расследования и рассмотрения уголовных дел и сам по себе он (указанный Закон. – А.С.) не может ограничивать права участников уголовного процесса и заявителей о преступлениях на ознакомление с материалами уголовных дел и проверок сооб-

щений о преступлениях»<sup>5</sup> (Определение Конституционного Суда РФ от 29 сентября 2011 г. № 1251-О-О; Апелляционное определение Санкт-Петербургского городского суда от 1 октября 2014 г. № 33-14325/2014 по делу № 2-1111/2014). Таким образом, наличие в материалах проверки по заявлению о правонарушении персональных данных иных лиц при отсутствии в них сведений об их частной жизни и иных конфиденциальных сведений, не может ограничивать право гражданина на ознакомление с этими материалами, непосредственно затрагивающими его права и свободы (Апелляционное определение Верховного суда Республики Башкортостан от 18 мая 2016 г. № 33а-9145/2016).

1.6. Хотя Конвенция 1981 г. формально касается лишь автоматизированной обработки персональных данных, она допускает возможность распространения ее положений не только на случаи автоматизированной обработки, но и на обработку без использования средств автоматизации, что было учтено Российской Федерацией при ратификации этой Конвенции<sup>6</sup>.

Аналогичные положения содержатся и в европейском законодательстве, оперирующем понятием «система учета документов» (*filling system*), под которой понимается любой структурированный массив персональных данных, доступных в соответствии с определенными критериями, безотносительно к тому, является ли он централизованным, децентрализованным или распределенным на функциональной или географической основе. В соответствии со ст. 3 Директивы 1995 г. ее положения распространяются как на автоматизированную обработку персональных данных, так и на их обработку иными способами, при которых персональные данные являются частью системы учета документов. При этом отмечается, что «досье (файлы) или их наборы, а также их обложки, не являющиеся структурированными в соответствии с определенными критериями, ни при каких обстоятельствах не охватываются рамками настоящей Директивы» (п. 27 Преамбулы).

Примечательно, что данные положения не были затронуты реформой законодательства о персональных данных и в неизменном виде содержатся также в Регламенте 2016 г. (ст. 2, п. 15 Преамбулы). Как следствие, судебная практика отдельных европейских стран не относит к системе учета документов неструктурированные массивы документов, которые по своему характеру несопоставимы с автоматизированными средствами обработки данных, например, набор документов, который бессистемно хранится в коробках (*Smith v. Lloyds TSB Bank Plc*, [2005] EWHC 246 (Ch)), или недостаточно объемные массивы документов (например, четыре досье) (*Durant v. Financial Services Authority*, [2003] EWCA Civ. 1746).

1.7. Следует отметить, что цели обработки персональных данных по общему правилу не имеют значения для решения вопроса о распространении на нее положений Закона о персональных данных, за исключением случаев, прямо указанных в ч. 2 комментируемой статьи. Поэтому безотносительно к тому, осуществляется ли обработка данных в коммерческих, политических, научно-исследовательских, статистических и прочих целях, она подпадает под действие Закона о персональных данных.

Равным образом для определения сферы применения Закона о персональных данных не имеет значения статус субъекта, осуществляющего обработку персональных данных: в качестве такового может выступать любое лицо, обладающее правоспособностью. Часть 1 комментируемой статьи относит к указанным лицам государственные и муниципальные органы власти, юридических и физических лиц. Таким образом, российское законодательство о персональных данных имеет универсальный характер и в равной степени распространяется на частный и публичный секторы, что, правда, не означает отсутствия специальных норм в отношении последнего.

---

<sup>5</sup> Здесь и далее при цитировании судебных актов сохранены орфография и пунктуация первоисточников.

<sup>6</sup> См. ст. 2 Федерального закона от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» // СПС «КонсультантПлюс».

2. Часть 2 комментируемого Закона содержит закрытый перечень видов отношений по обработке персональных данных, которые не подпадают под его действие *независимо от того, какие средства используются при их обработке* (автоматизированная или квази-автоматизированная). Таким образом, ставить вопрос о применимости каких-либо из данных видов исключений можно лишь *после того*, как положительно решен вопрос о применимости Закона о персональных данных к соответствующим отношениям в соответствии с положениями ч. 1 комментируемой статьи.

2.1. Закон о персональных данных не распространяется на обработку персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных. Появление данного исключения в российском законодательстве является следствием оговорки, сделанной Россией при ратификации Конвенции 1981 г., о неприменении ее положений к определенным категориям автоматизированных данных<sup>7</sup>, в связи с чем это исключение не противоречит международным обязательствам Российской Федерации. Аналогичное извлечение из сферы действия законодательства о персональных данных существует и в Европейском Союзе (ст. 3 (2) Директивы 1995 г., ст. 2 (2) (с) Регламента 2016 г.).

2.2. Понятия личных и семейных нужд в комментируемом Законе не конкретизируются. Представляется, что для толкования этих понятий можно обратиться к гражданскому законодательству и законодательству о защите прав потребителей, в которых также используются указанные термины. Так, одним из условий квалификации гражданина в качестве потребителя является приобретение товаров (работ, услуг) «исключительно для личных, семейных, домашних и иных нужд, не связанных с осуществлением предпринимательской деятельности»<sup>8</sup>. Как следствие, не является потребителем гражданин, приобретающий товары (работы, услуги) или использующий их в деятельности, которую он осуществляет самостоятельно на свой риск с целью извлечения прибыли. При этом под предпринимательской деятельностью понимается «самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг лицами, зарегистрированными в этом качестве в установленном законом порядке» (п. 1 ст. 2 ГК РФ). Таким образом, если процесс обработки персональных данных физическим лицом направлен на осуществление предпринимательской деятельности, он не охватывается понятием «личных» и «семейных» нужд и подпадает под действие Закона о персональных данных. Факт получения разовой прибыли от деятельности, связанной с обработкой персональных данных физическим лицом, не должен сам по себе лишать возможности применения рассматриваемого исключения из сферы действия Закона о персональных данных, при условии, что отсутствуют нарушения прав субъектов персональных данных.

2.3. В отечественной доктрине отмечается, что понятие «личные нужды» следует понимать как «потребности, которые существуют у самого гражданина или лиц, связанных с ним личными (например, семейными) связями, и их удовлетворение никак не связано с удовлетворением потребностей неопределенного круга третьих лиц»<sup>9</sup>. Данная идея находит отражение в практике Суда ЕС. В деле *Bodil Lindqvist* Суд указал, что распространение физическим лицом персональных данных третьих лиц в сети «Интернет» не подпадает под действие исключения об обработке данных для личных нужд, поскольку такие данные становятся доступными неопределенному кругу лиц (*Bodil Lindqvist v. Åklagarkammaren i Jönköping*, ECJ, Case C-101/01. 6 November 2003, [47]). Представляется, что данный подход вполне укладывается в

---

<sup>7</sup> См. ст. 2 Федерального закона от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

<sup>8</sup> Преамбула к Закону РФ от 8 февраля 1992 г. № 2300-I «О защите прав потребителей»; ст. 1212 ГК РФ.

<sup>9</sup> Эрделевский А. Банковский вклад и права потребителей // Законность. 1998. № 4.

нормы российского Закона о персональных данных, который содержит положение о неприменении исключения об обработке персональных данных для личных нужд с условием о ненарушении прав субъектов персональных данных. Распространение данных в сети «Интернет», их доступность неопределенному кругу лиц означают утрату контроля над дальнейшим использованием таких данных, что в совокупности с потенциальной возможностью их последующей обработки инструментами аналитики «больших данных» определенно затрагивает права субъектов персональных данных и в ряде случаев может их нарушать (например, при публикации одним лицом совместных фотографий в отсутствие согласия других присутствующих на них лиц). Следует отметить, что Регламент 2016 г. содержит несколько иной подход, согласно которому исключение об обработке персональных данных для личных нужд может применяться и к онлайн деятельности лица, в том числе при использовании социальных сетей (п. 18 Преамбулы). Пока не очень понятно, как будет соотноситься данное положение с правовой позицией Европейского Суда Справедливости, учитывая, что положения преамбулы формально не имеют юридической силы.

Представляется, что решение о применении или неприменении исключения об обработке персональных данных для личных нужд должно приниматься с учетом всех обстоятельств конкретного случая, при этом целесообразно учитывать степень доступности содержимого интернет-ресурса, в частности, настройки приватности (при их наличии)<sup>10</sup>.

2.4. В европейской судебной практике возник вопрос о возможности применения исключения об обработке для личных нужд персональных данных применительно к случаям установки лицом для целей охраны своей собственности камеры видеонаблюдения, которая осуществляет циклическую запись на жесткий диск происходящего, например, на улице перед домом. В деле *František Ryneš* Суд ЕС признал недопустимым распространение рассматриваемого исключения на подобного рода ситуации, поскольку такая обработка данных не ограничена пределами частных владений лица, направлена за его пределы и касается данных, полученных из публичных мест (улица), в связи с чем не является их обработкой, осуществляемой исключительно для личных и семейных нужд (*František Ryneš v. Úřad pro ochranu osobních údajů*, ECJ, Case C-212/13, 11 December 2014). Тем самым была подтверждена правомерность решения национального уполномоченного органа по защите персональных данных о нарушении субъектом, установившим камеру, положений об обработке персональных данных (отсутствие согласия прохожих на обработку, непредоставление им информации о целях и иных условиях обработки, неподача уведомления об обработке в уполномоченный орган).

Фактически Суд ЕС исходил из максимально ограничительного толкования исключения об обработке для личных нужд и высказался о несовместимости личных и семейных нужд с обработкой данных из публичных мест, особенно в тех случаях, когда она осуществляется на систематической основе. Следует отметить, что согласно действующему российскому законодательству граждане и юридические лица, не уполномоченные на проведение оперативно-розыскных мероприятий, не вправе устанавливать и использовать скрытые видеокамеры (технические средства для негласного визуального наблюдения)<sup>11</sup>. В этой связи вряд ли можно рассматривать установку камер видеонаблюдения за публичными местами в качестве обработки персональных данных, осуществляемой для личных и семейных нужд.

Кроме того, возникает вопрос о правовом статусе доказательств, полученных посредством такой камеры, в случаях, когда положения законодательства о персональных данных

---

<sup>10</sup> К примеру, в практике уполномоченного органа по защите персональных данных Норвегии обработка персональных данных на странице социальной сети, доступ к которой ограничен и доступен только для зарегистрированных пользователей, подпадает под действие рассматриваемого исключения. См.: *Bygrave A. Data Privacy Law: An International Perspective*. Oxford: University Press, 2014. P. 144.

<sup>11</sup> См. ст. 6 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»; п. 2 Перечня видов специальных технических средств, утв. Постановлением Правительства РФ от 1 июля 1996 г. № 770.

были нарушены. Формально такие доказательства могут считаться полученными с нарушениями требований закона и, как следствие, недопустимыми в рамках производства по делу об административном правонарушении. Согласно ч. 3 ст. 26.2 КоАП РФ не допускается использование доказательств по делу об административном правонарушении, в том числе результатов проверки, проведенной в ходе осуществления государственного контроля (надзора) и муниципального контроля, если указанные доказательства получены с нарушением закона. Что касается уголовного процесса, то здесь все не так очевидно, поскольку ст. 75 УПК РФ признает недопустимыми доказательства, полученные с нарушением требований именно данного Кодекса, а не любого закона (ч. 1 ст. 75 УПК РФ). Однако нельзя совсем исключать ситуации, в которых нарушение требований законодательства о персональных данных в отношении участника уголовного процесса может быть «подогнано» под нарушение какого-либо требования УПК РФ.

2.5. Принимая во внимание вышеизложенные соображения, можно предположить, что под обработку персональных данных для личных и семейных нужд будут подпадать организация и использование списка контактов в телефонах или коммуникационных сервисах; хранение писем, содержащих персональные данные на компьютерных устройствах, и т.п. При этом, как представляется, использование чужих визитных карточек не подпадает под данное исключение, поскольку, с одной стороны, обычно сопряжено с профессиональной деятельностью субъекта персональных данных, а с другой – не охватывается понятием автоматизированной обработки или обработки без использования средств автоматизации и тем самым выпадает из-под действия Закона о персональных данных в силу ч. 1 комментируемой статьи, а не ее п. 1 ч. 2.

2.6. Согласно п. 2 ч. 2 настоящей статьи действие Закона о персональных данных не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации. Данное положение корреспондирует ч. 3 ст. 4 Закона об информации, согласно которой порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

В число актов указанной отрасли законодательства входят Федеральный закон от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации» (далее – Закон об архивном деле) и принятые в соответствии с ним подзаконные нормативные правовые акты, законы и иные нормативные правовые акты субъектов Российской Федерации. Субсидиарное применение законодательства о персональных данных к рассматриваемым отношениям не предусмотрено, информационному законодательству, в отличие от гражданского законодательства, не известно понятие применения закона по аналогии при наличии пробела в регулировании.

В соответствии со ст. 3 Закона об архивном деле под архивным делом понимается деятельность государственных органов, органов местного самоуправления, организаций и граждан в сфере организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов. При этом под архивным документом понимается материальный носитель с зафиксированной на нем информацией, который имеет реквизиты, позволяющие его идентифицировать, и подлежит хранению в силу значимости указанных носителя и информации для граждан, общества и государства.

Разновидностью архивных документов являются так называемые документы по личному составу, которые отражают содержание трудовых отношений работника и работодателя. Государственные органы, органы местного самоуправления, организации и индивидуальные предприниматели обязаны обеспечивать сохранность архивных документов, в том числе докумен-

тов по личному составу, в течение сроков их хранения: для документов по личному составу, созданных до 2003 г., – не менее 75 лет с момента создания; для документов, созданных после 2003 г., – не менее 50 лет с момента создания<sup>12</sup>. В отношении иных документов необходимо руководствоваться специальными перечнями<sup>13</sup>.

Неприменение закона к отношениям по обработке персональных данных при организации хранения, комплектования, учета и использования архивных документов не означает, что право граждан на частную жизнь никак не учитывается. В данном случае применяется специальная норма ч. 3 ст. 25 Закона об архивном деле, согласно которой существует ограничение на доступ к архивным документам, содержащим сведения о личной и семейной тайне гражданина, его частной жизни, а также сведения, создающие угрозу для его безопасности. Данное ограничение устанавливается на срок 75 лет со дня создания указанных документов. С письменного разрешения гражданина, а после его смерти – с письменного разрешения наследников этого гражданина ограничение на доступ к архивным документам, содержащим сведения о личной и семейной тайне гражданина, его частной жизни, а также сведения, создающие угрозу для его безопасности, может быть отменено ранее чем через 75 лет со дня создания указанных документов.

Оценивая данное исключение из сферы действия Закона о персональных данных, нельзя не отметить его достаточно спорный характер. Оно не упоминается в Законе о ратификации Конвенции 1981 г., отсутствуют схожие положения и в общеевропейском законодательстве. Напротив, Регламент 2016 г. прямо упоминает архивные цели в качестве возможных целей обработки персональных данных (п. 73, 153 Преамбулы и другие положения). Вряд ли данное изъятие можно объяснить отсутствием в законодательстве об архивной деятельности понятия «электронный архив», в связи с чем оно не может регулировать автоматизированную обработку данных<sup>14</sup>, поскольку законодательство о персональных данных распространяется в том числе и на обработку персональных данных без средств автоматизации, поэтому отсутствие понятия «электронный архив» не может само по себе препятствовать его применению. По всей видимости, включение данного положения было продиктовано желанием сохранить сложившееся регулирование в области архивного дела и не инициировать глубокую его переработку в связи с появлением нового пласта регулирования. Однако попадание в сферу архивного законодательства документов, создаваемых в процессе отношений, которые при прочих равных условиях относятся к «компетенции» законодательства о персональных данных, например, документов, содержащих сведения о трудовых правоотношениях («документов по личному составу»), может повлечь правовые коллизии и правоприменительные ошибки. Куда более логичным было бы введение отношений по обработке персональных данных в архивной деятельности в общую орбиту законодательства о персональных данных с установлением ряда специальных норм, учитывающих особенности данной сферы.

2.7. Еще одним исключением из сферы действия Закона о персональных данных являются отношения по обработке персональных данных, составляющих государственную тайну, т.е. защищаемых государством сведений в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Данное

---

<sup>12</sup> См. ст. 22.1 Закона об архивном деле.

<sup>13</sup> См. приказы Минкультуры России от 25 августа 2010 г. № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»; от 31 июля 2007 г. № 1182 «Об утверждении Перечня типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций, с указанием сроков хранения».

<sup>14</sup> Указанная точка зрения высказана представителями Роскомнадзора. См.: Федеральный закон «О персональных данных»: Научно-практический комментарий / Под ред. зам. руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций А.А. Приезжевой. М., 2015. С. 10.



исключение было предусмотрено в оговорке, сделанной при ратификации Конвенции 1981 г., о неприменении ее положений к определенным категориям автоматизированных данных<sup>15</sup>, в связи с чем это исключение не противоречит международным обязательствам Российской Федерации. Порядок отнесения сведений к государственной тайне и их правовой режим устанавливаются Законом РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне».

2.8. Четвертым и последним изъятием из сферы действия Закона о персональных данных являются отношения, связанные с предоставлением уполномоченными органами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации». Данное исключение связано с действием принципа гласности судопроизводства. Однако его практическая реализация обладает спецификой в зависимости от типа суда, который вынес судебный акт.

Так, тексты судебных актов, принятых арбитражными судами, Конституционным Судом РФ и конституционными судами субъектов РФ, по общему правилу размещаются в сети «Интернет» в полном объеме.

Как отметил Высший Арбитражный Суд РФ, опубликование судебных актов, содержащих персональные данные лиц, участвующих в производстве по делу об административном правонарушении, не может само по себе рассматриваться как наносящее ущерб безопасности таких лиц, членов их семей, их близких, а также их чести и достоинству. При этом содержание персональных данных в судебных актах арбитражных судов не препятствует их размещению в сети «Интернет» в полном объеме. В случае необходимости сохранения коммерческой или иной охраняемой законом тайны разбирательство дел об административных правонарушениях осуществляется в закрытом судебном заседании при удовлетворении судом соответствующего ходатайства лица, участвующего в деле<sup>16</sup>.

При размещении в сети «Интернет» текстов судебных актов, принятых судами общей юрисдикции, по общему правилу в целях обеспечения безопасности участников судебного процесса из указанных актов исключаются персональные данные, кроме фамилий и инициалов истца, ответчика, третьего лица, гражданского истца, гражданского ответчика, осужденного, оправданного либо лица, в отношении которого ведется производство по делу об административном правонарушении, секретаря судебного заседания, рассматривавших (рассматривавшего) дело судей (судьи), а также прокурора, адвоката и представителя, если они участвовали в судебном разбирательстве. Вместо исключенных персональных данных используются инициалы, псевдонимы или другие обозначения, не позволяющие идентифицировать участников судебного процесса (ч. 3 ст. 15 Федерального закона от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»). При этом некоторые судебные решения в целях защиты прав граждан на неприкосновенность частной жизни, личной и семейной тайны, их чести и деловой репутации не подлежат публикации в сети «Интернет» (например, решения по делам, возникающим из семейно-правовых отношений, в том числе по делам об усыновлении (удочерении) ребенка, другим делам, затрагивающим права и законные интересы несовершеннолетних; по делам о преступлениях против половой неприкосновенности и половой свободы личности; об ограничении дееспособности гражданина или о признании его недееспособным; о принудительной госпитализации гражданина в психиатрический стационар и принудительном психиатрическом освидетельствовании; о внесении исправлений или изменений в запись актов гражданского состояния). Правда, следует отметить, что на практике опубликованные в сети «Интернет» судебные решения обычно

---

<sup>15</sup> См. п. «б» ст. 1 Федерального закона от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

<sup>16</sup> См. п. 17 постановления Пленума ВАС РФ от 8 октября 2012 г. № 61 «Об обеспечении гласности в арбитражном процессе».

не содержат фамилий и инициалов участников процесса вопреки требованиям ч. 5 ст. 15 вышеуказанного Закона. Во многом это связано с тем, что перед публикацией судебные акты проходят процедуру деперсонификации в автоматизированном режиме с использованием соответствующего модуля сопряжения подсистемы «Интернет-портал» с базой данных подсистемы «Банк судебных решений (судебная практика)» ГАС «Правосудие»<sup>17</sup>.

3. Обратимся к сфере действия Закона о персональных данных в пространстве. Как отмечалось ранее, ни комментируемая статья, ни иные положения Закона о персональных данных не содержат каких-либо положений, регламентирующих данный вопрос. В то же время ясное представление понимания сферы применения законодательства о персональных данных по территории и кругу лиц является необходимым условием обеспечения правовой определенности для всех участников отношений, регулируемых законодательством о персональных данных: субъектов персональных данных, использующих интернет-ресурсы в своей повседневной деятельности; операторов персональных данных, использующих инструментарий сети «Интернет» для осуществления своей деятельности; уполномоченных органов по контролю и надзору за соблюдением законодательства о персональных данных. В этой связи необходимо отметить следующее.

3.1. Гражданство или местожительства субъекта персональных данных, сведения о котором обрабатываются, не имеют значения при решении вопроса о применимости российского законодательства о персональных данных. Такой подход соответствует целям Конвенции 1981 г., которая согласно ст. 1 «состоит в обеспечении на территории каждой Стороны для каждого физического лица, *независимо от его гражданства или местожительства*, уважения его прав и основных свобод, и в частности его права на неприкосновенность частной жизни, в отношении автоматизированной обработки касающихся его персональных данных» (курсив мой. – А.С.).

3.2. Требования Закона о персональных данных распространяются на лиц, осуществляющих обработку персональных данных, которые являются гражданами РФ и юридическими лицами, созданными по законодательству РФ, в силу того, что юрисдикция Российской Федерации по общему правилу распространяется на всех граждан государства, безотносительно к их фактическому местоположению (так называемая личная юрисдикция)<sup>18</sup>. Кроме того, поскольку понятия физического и юридического лица, упомянутые в комментируемой статье, включают в себя, так как прямо не указано иное, и иностранных лиц, которым в соответствии со ст. 2 ГК РФ предоставляется национальный режим, можно сделать вывод, что Закон о персональных данных может распространяться и на иностранных физических и юридических лиц, на официальном сайте суда общей юрисдикции, утв. Постановлением Президиума Совета судей РФ от 27 января 2011 г. № 253.

осуществляющих обработку персональных данных. Если иностранное лицо физически присутствует на территории России в форме представительства или иного обособленного подразделения, то это является достаточным условием для распространения на него положений российского законодательства, как минимум, в части деятельности, осуществляемой через такое обособленное подразделение, и соответственно обработки персональных данных, производимой в связи с деятельностью, осуществляемой посредством такого обособленного подразделения. Если лицо, обрабатывающее персональные данные, не имеет физического присутствия на территории России, Закон о персональных данных может применяться к нему в случае установления факта *«виртуального» его присутствия* на территории Российской Федерации.

---

<sup>17</sup> См.: Регламент организации размещения сведений о находящихся в суде делах и текстов судебных актов в информационно-телекоммуникационной сети «Интернет»

<sup>18</sup> Международное право: Учебник / Б.М. Ашавский, М.М. Бирюков, В.Д. Бордюнов и др.; отв. ред. С.А. Егоров. М.: Статут, 2015.

Концепция «виртуального» присутствия связана с осуществлением лицом деятельности в информационно-телекоммуникационной сети «Интернет», которая в силу своего трансграничного, децентрализованного и виртуального характера не позволяет четко обозначить географические границы осуществления такой деятельности. Одной лишь доступности интернет-сайта на территории Российской Федерации недостаточно для вывода, что на него распространяется законодательство Российской Федерации, в том числе о персональных данных, поскольку в таком случае сфера его применения носила бы по существу всемирный характер и делала бы практически невозможным контроль за исполнением им российского законодательства.

Принимая во внимание указанные обстоятельства, Минкомсвязи России конкретизировало условия, при наличии которых Закон о персональных данных распространяется на иностранных лиц<sup>19</sup>. В их основе лежит критерий направленности деятельности, который используется в международном частном праве, а также в европейской практике<sup>20</sup>. Так, согласно ст. 1212 ГК РФ выбор права, подлежащего применению к договору, стороной которого является потребитель, не может повлечь за собой лишение такого лица защиты его прав, предоставляемой императивными нормами права страны места жительства потребителя, если контрагент потребителя любыми способами направляет свою деятельность на территорию этой страны. Кроме того, критерий направленности деятельности получил отражение и в информационном законодательстве применительно к «праву быть забытым». В соответствии со ст. 10.3 Закона об информации соответствующие обязанности по удалению ссылок на информацию о заявителе возлагаются на операторов поисковых систем, которые распространяют в сети «Интернет» «рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации».

Для определения направленности деятельности в указанных разъяснениях выделены два базовых и ряд дополнительных факторов (критериев), которые были подготовлены с учетом европейского опыта толкования положений о направленной деятельности (*Joined cases: Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG (C-585/08) and Hotel Alpenhof GesmbH v. Oliver Heller (C-144/09)*, 7 December 2010).

#### Базовые критерии

1) Использование географического доменного имени, связанного с РФ (.ru, .рф., .su) или ее отдельными регионами (например, .moscow, .москва).

Данный критерий основан на презумпции, согласно которой регистрация и фактическое использование доменного имени в указанных зонах являются проявлением намерения владельца интернет-ресурса осуществлять свою деятельность «с прицелом» на Россию, что обусловлено сильной географической привязкой данных доменов к ее территории. В качестве исключения можно рассматривать регистрацию доменного имени *без его последующего фактического использования*, когда такая регистрация осуществляется в защитных целях для предотвращения захвата такого доменного имени конкурентами или *киберсквоттерами*.

Схожий критерий применения российского законодательства в сети «Интернет» используется Федеральной антимонопольной службой РФ для определения сферы применения в сети «Интернет» законодательства о рекламе<sup>21</sup>. Наличие зарегистрированного доменного имени в зоне «.ru» признается достаточным для установления юрисдикции российских судов и в отечественной судебной-арбитражной практике (см., например, Постановление Суда по интеллек-

---

<sup>19</sup> <http://minsvyaz.ru/ru/personaldata/>

<sup>20</sup> См. ст. 3 (2) Регламента 2016 г.; ст. 15(1)(с) Регламента ЕС № 44/2001 от 22 декабря 2000 г. «О юрисдикции, признании и исполнении судебных решений по гражданским и торговым делам»; ст. 6 Регламента ЕС № 593/2008 от 17 июня 2008 г. «О праве, применимом к договорным отношениям».

<sup>21</sup> Письмо ФАС России от 3 августа 2012 г. № АК/24981 «О рекламе алкогольной продукции в Интернете и печатных СМИ»

туальным правам от 2 октября 2014 г. № С01-856/2014 по делу № А40-102183/2013, в котором говорится: «Поскольку доменное имя, о запрете администрирования которого ответчиком просит истец, зарегистрировано в доменной зоне «.ru», рассматриваемый спор относится к компетенции арбитражных судов Российской Федерации»).

Критерий использования географического доменного имени, связанного с территорией России, носит самодостаточный характер и может применяться вне зависимости от наличия иных критериев. В частности, данному критерию будет удовлетворять использование такого доменного имени для целей переадресации на иной интернет-ресурс, который может располагаться под функциональным доменом типа «.com». Например, в случае использования доменного имени «abc.ru», с которого осуществляется переадресация на «abc.com».

2) Наличие русскоязычной версии интернет-ресурса (в совокупности с одним из вторичных критериев, указанных ниже).

Использование русского языка на интернет-ресурсе является сильным аргументом в пользу присутствия направленности деятельности такого сайта на территорию РФ безотносительно к его доменному имени (т.е. данный критерий применим и к случаям, когда интернет-сайт использует функциональный домен типа .com, .org). При этом во внимание должна приниматься именно целенаправленная локализация интернет-сайта, осуществленная самим владельцем или иным привлеченным им лицом, применение систем автоматического перевода не должно приниматься во внимание. Однако необходимо учитывать, что использование русского языка во многих, но не во всех случаях свидетельствует о направленности на территорию РФ. Например, если из содержания сайта очевидно, что в качестве целевой аудитории могут выступать граждане Белоруссии, Казахстана, русскоязычное население Европы, Канады или других стран. В этой связи базовый критерий использования русского языка подлежит применению при наличии как минимум одного из дополнительных (вторичных) критериев.

#### Вторичные критерии

1) возможность заключения и исполнения договора с российским резидентом, в частности, осуществление доставки товара или цифрового контента на территорию России;

2) возможность осуществления расчетов в российских рублях;

3) использование контекстной или баннерной рекламы на русском языке, включающей ссылку на соответствующий интернет-ресурс;

4) иные обстоятельства, которые явно свидетельствуют о намерении владельца интернет-сайта включить российский рынок в свою бизнес-стратегию. Например, к ним может быть отнесено наличие на интернет-ресурсе способов обратной связи, касающихся территории РФ, например, номера телефона, на который можно бесплатно позвонить с территории России (общегосударственного бесплатного номера (8-800...), или телефона с кодом российского города. Факты приобретения владельцем интернет-сайта соответствующих услуг связи, готовность оформлять документацию с отечественным оператором связи и нести расходы по оплате услуг, подобных использованию номера 8-800... и т.д., говорят о высокой заинтересованности владельца в российских потребителях.

Следует отметить, что схожие по существу критерии направленности деятельности также приведены в комментариях, размещенных на официальном сайте Роскомнадзора<sup>22</sup>.

3.3. Вышеуказанные критерии были применены на практике при рассмотрении спора о внесении интернет-сайта социальной сети *LinkedIn* в Реестр нарушителей прав субъектов персональных данных и блокировании доступа к нему на территории РФ в связи с нарушением

---

<sup>22</sup> См.: Комментарий к Федеральному закону от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях». С. 15. URL: <https://pd.rkn.gov.ru/library/p195/>. К сожалению, этот документ не содержит указания на авторов данного комментария.

обязанности по локализации отдельных процессов обработки персональных данных в соответствии с ч. 5 ст. 18 Закона о персональных данных (см. комментарий к ней). Удовлетворяя указанное требование, суд указал на то, что «о направленности интернет-сайта [www.linkedin.com](http://www.linkedin.com) на территорию РФ свидетельствует наличие русскоязычной версии интернет-сайта. При этом интернет-сайт допускает возможность использования рекламы на русском языке, что дополнительно свидетельствует о включении российской аудитории в сферу бизнес-интересов владельца сайта» (Определение Московского городского суда от 10 ноября 2016 г. по делу № 33-38783/2016). Как видно, суд руководствовался вторым базовым критерием в совокупности с дополнительным критерием в виде наличия рекламы на русском языке. К этому следует добавить, что пользовательские соглашения указанного сервиса были доступны и на русском языке, а также что наличие факта использования географического доменного имени «[linkedin.ru](http://linkedin.ru)», с которого осуществлялась переадресация на сайт «[linkedin.com](http://linkedin.com)», позволяло говорить о применении и первого базового критерия направленности деятельности на территорию России.

3.4. Критерий направленной деятельности как условие распространения законодательства о персональных данных на иностранное лицо, не имеющее присутствия на территории страны – члена Европейского Союза, пришел на смену критерию местонахождения оборудования, содержащемуся в ст. 4 (1) Директивы 1995 г.<sup>23</sup>, и был имплементирован в европейское законодательство Регламентом 2016 г., в соответствии со ст. 3 (2) которого указанный Регламент распространяется на процессы обработки персональных данных, связанные с:

а) предложением товаров или услуг безотносительно к наличию встречной обязанности по их оплате лицам, проживающим на территории Европейского Союза, или б) мониторингом поведения таких лиц в той мере, в какой такое поведение имеет место на территории Европейского Союза (этот критерий касается различного рода интернет-сервисов, которые осуществляют сбор пользовательских данных в целях их последующего использования для предоставления таргетированной рекламы).

Таким образом, европейское законодательство о персональных данных приобретает в значительной степени экстерриториальный характер, в связи с чем в литературе отмечается, что единственным легальным способом не соблюдать положения Регламента 2016 г. является решение о неведении бизнеса в странах Европейского Союза<sup>24</sup>.

Из всего сказанного следует, что российский подход к определению территориальной сферы действия Закона о персональных данных находится в русле развития европейского законодательства и отражает специфику регулирования юрисдикционных аспектов отношений в сети «Интернет». Остается выразить надежду, что он рано или поздно перерастет рамки разъяснений правоприменительных органов, данных по результатам систематического толкования иных законодательных положений и доктрины, и будет формализован на уровне закона.

<sup>23</sup> В соответствии со ст. 4 (1)(c) Директивы 1995 г. государство – участник ЕС применяет свое национальное законодательство о персональных данных, если «оператор учрежден не на территории ЕС и в целях обработки персональных данных использует оборудование, расположенное на территории такого государства – участника ЕС (если только такое оборудование не используется исключительно для целей транзита по территории Сообщества)». Данный подход был признан неудовлетворительным, поскольку: 1) достаточно много споров вызывает понятие «оборудование»; 2) распространение облачных сервисов со свойственным им динамическим распределением вычислительных мощностей в зависимости от конкретных потребностей заказчика и распределенным хранением данных в различных дата-центрах вызывает существенные трудности в применении этого критерия; 3) он создает условия для обхода обременительных требований Европейского Союза посредством искусственного подчинения правоотношения правопорядку другого государства, на территории которого находятся соответствующие мощности. См.: Opinion 8/2010 On Applicable Law. Article 29 Data Protection Working Party. 16 December 2010.

<sup>24</sup> Calder Alan. EU General Data Protection Regulation (GDPR) an Implementation and Compliance Guide. IT Governance Publishing. 2016. Kindle Edition (Kindle Locations 3-5).

## Статья 2. Цель настоящего федерального закона

**Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.**

1. Комментируемая статья обозначает цели, преследуемые законодательством о персональных данных, конкретизируя их через призму обеспечения реализации конституционных прав на неприкосновенность частной жизни, личную и семейную тайну, а также защиту иных прав и свобод человека и гражданина при обработке его персональных данных. Формулировка данной статьи представляет собой практически дословный перевод положения ст. 1 (1) Директивы 1995 г., а также весьма схожа с формулировкой ст. 1 Конвенции 1981 г. Фактически в центре законодательства о персональных данных стоит английское понятие «*privacy*» (фр. *la vie privée*; нем. *die Privatsphäre*), наиболее адекватным эквивалентом которого в русском языке и является понятие «неприкосновенность частной жизни».

Право на неприкосновенность частной жизни, личную и семейную тайну предусмотрено в ст. 23 и 24 Конституции РФ. Согласно позиции Конституционного Суда РФ право на неприкосновенность частной жизни, личную и семейную тайну означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера; в понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если не носит противоправный характер (Определение Конституционного Суда РФ от 24 декабря 2013 г. № 2128-О). Представляется, что более емко данные положения выразил М.В. Баглай, который понимает под частной жизнью «своеобразный суверенитет личности, означающий неприкосновенность его «среды обитания»»<sup>25</sup>.

2. В результате реформы гражданского законодательства в числе поправок в часть первую ГК РФ появилась ст. 152.2, посвященная охране частной жизни гражданина, согласно которой «если иное прямо не предусмотрено законом, не допускаются без согласия гражданина сбор, хранение, распространение и использование любой информации о его частной жизни, в частности сведений о его происхождении, о месте его пребывания или жительства, о личной и семейной жизни». При этом указанная статья предусматривает ряд исключений из данного правила: публичный интерес, общедоступность соответствующей информации, ее раскрытие по воле гражданина. Понятие частной жизни ГК РФ не раскрывает.

3. Поскольку право на уважение частной и семейной жизни также предусмотрено в ст. 8 Европейской конвенции о защите прав человека и основных свобод 1950 г., стороной которой является Российская Федерация<sup>26</sup>, при толковании понятий частной жизни, личной и семейной тайны необходимо учитывать практику ЕСПЧ по данному вопросу. В этой связи необходимо отметить следующие ее отличительные черты:

1) ЕСПЧ рассматривает положения Конвенции 1950 г. как «живой инструмент, который должен толковаться с учетом реалий сегодняшнего дня» (Постановление ЕСПЧ от 25 апреля 1978 г. по делу *Тайлер против Соединенного Королевства*, жалоба № 5856/72), в связи с чем ст. 8 достаточно легко применяется ЕСПЧ к современным технологиям (электронной почте, GPS-технологиям, видеонаблюдению и пр.)<sup>27</sup>;

---

<sup>25</sup> Баглай М.В. Конституционное право Российской Федерации. М., 2005. С. 185.

<sup>26</sup> Конвенция вступила в силу для Российской Федерации 5 мая 1998 г.

<sup>27</sup> См. подробнее: Ефремов А.А. Новые информационные технологии в практике Европейского суда по правам человека // Прецеденты Европейского суда по правам человека. 2016. № 6. С. 10–15.

2) согласно позиции ЕСПЧ дать исчерпывающее определение понятию «privacy» («личная жизнь») невозможно и нецелесообразно, однако одно вполне очевидно: данное понятие толкуется ЕСПЧ весьма широко по сравнению с классическим американским пониманием термина «приватность» (*privacy*) как «права быть оставленным в покое» (*right to be left alone*)<sup>28</sup>. Ключевой идеей, заложенной в основу понятия «личная жизнь», является идея личной автономии. Так, понятие «личная жизнь» охватывает физическую и моральную стороны жизни индивида, включая сексуальную жизнь (Постановление ЕСПЧ от 26 марта 1985 г. по делу *X и Y против Нидерландов*, жалоба № 8978/80); физическую и психологическую неприкосновенность индивида при оказании ему медицинской помощи или психиатрическом обследовании (постановления ЕСПЧ от 22 июля 2003 г. по делу *И.Ф. (Y.F.) против Турции*, жалоба № 24209/94; от 27 ноября 2003 г. по делу *Ворва (Worwa) против Польши*, жалоба № 26624/95); право индивида знать свое происхождение (Постановление ЕСПЧ от 13 февраля 2003 г. по делу *Одьевр (Odievre) против Франции*, жалоба № 42326/98); вопросы публикации фотографий повседневной жизни индивида (Постановление ЕСПЧ от 24 июня 2004 г. по делу *Фон Ганновер (Принцесса Ганноверская) (Von Hannover) против Германии*, жалоба № 59320/00) и ряд других вопросов<sup>29</sup>;

3) согласно позиции ЕСПЧ право на личную жизнь распространяется не только на свободу от воздействия извне на личную сферу индивида, но и на отношения с другими людьми, включая в том числе «возможность устанавливать и поддерживать отношения с другими людьми в профессиональном и деловом плане, как и в любом другом» (Постановление ЕСПЧ от 16 декабря 1992 г. по делу *Нимитц (Niemietz) против Германии*, жалоба № 13710/88);

4) ЕСПЧ подчеркивает, что право на частную жизнь хотя главным образом и состоит в защите личности от произвольного вмешательства органов государственной власти, но не ограничивается обязанностью государства воздерживаться от такового вмешательства. Оно также предполагает, что государство должно принимать меры, направленные на обеспечение уважения частной жизни даже в сфере отношений лиц между собой (Постановление ЕСПЧ от 24 июня 2004 г. по делу *Фон Ганновер (Принцесса Ганноверская) (Von Hannover) против Германии*, жалоба № 59320/00). Тем самым имплементация государством специальных законодательных норм, регламентирующих как вертикальные отношения между государством и индивидом, так и горизонтальные отношения между частными лицами – операторами и субъектами персональных данных по поводу личной информации, вполне укладывается в обязанности государства по обеспечению права на частную жизнь в понимании ЕСПЧ.

Таким образом, право на неприкосновенность частной жизни представляет собой комплекс целого ряда правомочий, обеспечивающих свободу реализации личности, содержание которых эволюционирует с развитием общества, технологий и морали (право на тайну переписки, телефонных переговоров, личную неприкосновенность, сексуальное самоопределение, защиту чести и достоинства и пр.).

В качестве примеров, признанных ЕСПЧ вмешательством в личную жизнь, которые нарушали требования Конвенции 1950 г., можно привести ситуации, в которых осуществляется слежка за индивидом как посредством контроля его коммуникаций и телефонных переговоров, в том числе с использованием системы тайного прослушивания вроде СОПМ (Постановление ЕСПЧ от 4 декабря 2015 г. по делу *Роман Захаров (Roman Zakharov) против Российской Федерации*, жалоба № 47143/06), так и посредством спутниковых систем навигации (Постановление ЕСПЧ от 2 сентября 2010 г. по делу *Узун против Германии*, жалоба № 35623/05). В качестве иных примеров нарушения права на частную жизнь ЕСПЧ привел опубликование

<sup>28</sup> Warren S., Brandeis L. The Right to Privacy // Harvard Law Review. 1890. No. IV. P. 193.

<sup>29</sup> См. подробнее: Рожкова М.А., Афанасьев Д.В., Тай Ю.В. Порядок рассмотрения жалоб в Европейском суде по правам человека. М.: Статут, 2013. Серия «Практика Европейского суда по правам человека: комментарии, судебные прецеденты». Кн. 2 // СПС «КонсультантПлюс».

видеозаписей наблюдения в общественных местах (Постановление ЕСПЧ от 28 января 2003 г. по делу *Пек (Peck) против Соединенного Королевства*, жалоба № 44647/98), нерегламентированный контроль работодателя за использованием средств коммуникаций (служебного телефона, электронной почты, интернета) работниками (Постановление ЕСПЧ от 3 апреля 2007 г. по делу *Копланд (Copland) против Соединенного Королевства*, жалоба № 62617/00).

4. Рассмотрение законодательства о персональных данных в качестве результата эволюции права на неприкосновенность частной жизни, личную и семейную тайну не означает, что право на защиту персональных данных должно рассматриваться исключительно как модернизированная манифестация этого права. Анализ положений законодательства о персональных данных позволяет сделать вывод, что регулируемые им отношения, с одной стороны, не в полной мере охватывают ситуации, которые подпадают под действие права на неприкосновенность частной жизни, а с другой – явно выходят за его рамки. Тем самым право на защиту персональных данных приобрело во многом самостоятельное значение. Графически соотношение права на защиту персональных данных и права на неприкосновенность частной жизни можно обозначить следующим образом:

Во-первых, как следует из ст. 1 Закона о персональных данных, он не регулирует отношения, связанные с обработкой данных, которые могут составлять личную или семейную тайну, если такая обработка не осуществляется с использованием средств автоматизации или систематизированных картотек персональных данных. Однако при этом лицо не лишено возможности защищать свои права в порядке, установленном гл. 8 ГК РФ. Согласно ст. 151.1 и 152.2 данного Кодекса по общему правилу распространение сведений (в том числе в виде фотографий), информирующих о частной (личной) либо семейной жизни гражданина без его согласия, является нарушением права на неприкосновенность частной жизни, безотносительно к применению автоматизированных или «квази-автоматизированных» средств обработки (Апелляционное определение Санкт-Петербургского городского суда от 24 июня 2015 г. № 33-10102/2015 по делу № 2-1450/2014). В рамках реализации прав, предоставляемых ГК РФ, гражданин вправе требовать в судебном порядке удалить соответствующую информацию с материальных носителей; пресечь и запретить дальнейшее ее распространение, а также использовать иные средства защиты, указанные в п. 2 ст. 150 ГК РФ.

Во-вторых, законодательство о персональных данных регулирует более широкий круг информационных отношений, включая отношения по поводу публичной и общедоступной информации, которая не может являться личной или семейной тайной в силу своей природы (например, информация лица о себе и о своем опыте работы в определенной сфере, размещенная им в специализированной социальной сети с целью поиска работы). Обработка подобного рода сведений не может рассматриваться как вторжение в личную сферу гражданина или как нарушение права на неприкосновенность его частной жизни, поскольку лицо само вывело указанные данные из-под режима личной тайны, сделав их общедоступными. Также вряд ли можно рассматривать в качестве вторжения в личную или семейную сферу лица, к примеру, действия работодателя по обработке данных о зарплате своего работника – субъекта персональных данных, однако данные действия все же регулируются нормами законодательства о персональных данных. По сути, законодательство о персональных данных предоставляет субъекту совокупность *специальных прав по управлению такими данными* и контролю за порядком их использования (право получения доступа к информации об их обработке, право на уточнение таких данных, прекращение их обработки и пр.), исполнение которых обеспечивается возложением на оператора ряда обязанностей.

В-третьих, право на неприкосновенность частной жизни, личную и семейную тайну исходит из необходимости обеспечения максимальной конфиденциальности таких данных, пребывания их в «тумане» для окружающих. Одной из основных задач законодательства о защите персональных данных является обеспечение прозрачности осуществляемых процессов обра-



ботки персональных данных для субъекта персональных данных, в том числе *предоставление ему возможности контроля* над их обработкой: в определенной степени определять кому, когда и в каком объеме могут быть предоставлены персональные данные, если иное не предусмотрено законом.

В-четвертых, права субъекта, вытекающие из законодательства о защите персональных данных, имеют «относительный» характер и могут быть реализованы только в отношении специального субъекта – оператора персональных данных. Лицо, которое осуществляет обработку персональных данных по поручению оператора, не несет ответственность непосредственно перед субъектом (ч. 5 ст. 6 Закона о персональных данных). Право на неприкосновенность частной жизни, личную и семейную тайну по общему правилу имеет абсолютный характер и действует *erga omnes* (против всех). В частности, это проявляется в порядке защиты данного права как личного нематериального блага, предусмотренном гл. 8 ГК РФ.

Следует подчеркнуть, что в Европейском Союзе право на неприкосновенность частной жизни и право на защиту персональных данных разделены и закреплены в различных статьях Хартии Европейского Союза об основных правах (ст. 7 и 8 соответственно)<sup>30</sup>. Регламент 2016 г. в качестве своей цели предусматривает уже не защиту «права на неприкосновенность частной жизни» (*right to privacy*), а «защиту фундаментальных прав и свобод человека, в том числе права на защиту персональных данных» (ст. 1).

Таким образом, право на защиту персональных данных и право на неприкосновенность частной жизни, личную и семейную тайну не являются тождественными, они имеют отличия как в части объема и природы подпадающей под охрану информации, так и в части принципов, лежащих в основе регулирования. С определенной долей условности можно констатировать, что право на неприкосновенность частной жизни, личную и семейную тайну защищает *частную информационную сферу* гражданина, в то время как право на защиту персональных данных направлено на защиту *личной информационной сферы* гражданина. Как следствие, правовой режим защиты персональных данных, установленный Законом о персональных данных, и правовой режим защиты неприкосновенности частной жизни, установленный ГК РФ, носят параллельный характер. Тот факт, что гражданин может не иметь возможности защитить свои права в рамках норм ст. 152.1 или 152.2 ГК РФ, не означает, что он лишен такой возможности в рамках Закона о персональных данных, и наоборот.

В отечественной судебной практике также можно встретить подобный дифференцированный подход. Так, суд указал, что «спорные правоотношения, а именно сбор в отношении заявителя персональных данных и распоряжение ими, не подпадают под сферу регулирования Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», заявитель не лишен возможности защиты своих прав в порядке, установленном главой 8 Гражданского кодекса Российской Федерации» (Апелляционное определение Санкт-Петербургского городского суда от 24 июня 2015 г. № 33-10102/2015 по делу № 2-1450/2014).

5. Формулировка комментируемой статьи формально не ограничивает цели Закона о персональных данных лишь защитой прав на неприкосновенность частной жизни, личную и семейную тайну, упоминая их не иначе, как *в числе защищаемых прав и свобод* человека и гражданина при обработке его персональных данных. К иным правам и свободам человека, связанным с обработкой персональных данных, можно отнести, в частности, право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ч. 2 ст. 23 Конституции РФ); право лица требовать от органов государственной власти и органов местного самоуправления, их должностных лиц обеспечения возможности ознакомления с доку-

---

<sup>30</sup> Charter of Fundamental Rights of the European Union. 2000/C 364/01. URL: [www.europarl.europa.eu/charter/pdf/text\\_en.pdf](http://www.europarl.europa.eu/charter/pdf/text_en.pdf). Данный документ был принят в 2000 г. и вступил в силу в 2009 г.

ментами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом (ч. 2 ст. 24 Конституции РФ).

6. Сведéние всех целей законодательства о персональных данных исключительно к защите конституционных прав человека и гражданина при обработке его персональных данных является существенным «упрощением» природы существующих правоотношений по поводу персональных данных и игнорирует необходимость учета и защиты прав и законных интересов иных участников отношений в указанной области – общества, государства и бизнеса.

Так, общество заинтересовано в обеспечении реализации его членами конституционных прав на свободу слова и свободу поиска, получения и распространения информации любым законным способом (ст. 29 Конституции РФ), в том числе прав на получение информации от государственных органов; на свободу литературного, художественного, научного, технического и других видов творчества (ст. 44 Конституции РФ), и ряда других конституционных прав. Во многом именно этими соображениями объясняется наличие специальных оснований для обработки персональных данных без согласия субъекта для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности (п. 7 ч. 1 ст. 6 Закона о персональных данных).

Государство заинтересовано в сборе и обработке персональных данных с целью обеспечения реализации своих публичных функций, в том числе обеспечения безопасности своих граждан и национального суверенитета. Указанными целями продиктованы такие положения Закона о персональных данных, как, например, положение о возможности обработки специальных («чувствительных») категорий данных без согласия субъекта, если такая обработка осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, противодействии терроризму, транспортной безопасности, противодействии коррупции, об оперативно-розыскной деятельности (п. 7 ч. 2 ст. 10). Во многом именно соображениями национальной безопасности можно объяснить введение обязанности операторов по локализации отдельных процессов обработки персональных данных российских граждан (ч. 5 ст. 18 Закона о персональных данных).

Коммерческий сектор заинтересован в сборе и обработке персональных данных с целью создания новых бизнес-моделей, персонализации предоставляемых товаров и услуг, максимально эффективного использования новых инновационных технологий в конкурентной борьбе. Учет данных интересов иллюстрируют, в частности, положения о трансграничной передаче данных, возможности обработки персональных данных без согласия их субъекта для целей заключения или исполнения договора, а также для осуществления прав и законных интересов оператора (п. 5, 7 ч. 1 ст. 6 Закона о персональных данных). В некоторых случаях законодательство о персональных данных может быть использовано и для целей экономического протекционизма, что признавалось еще при разработке Руководящих принципов ОЭСР<sup>31</sup>. Положения о локализации отдельных процессов обработки персональных данных, недавно имплементированные в Закон о персональных данных (ч. 5 ст. 18), вполне могут рассматриваться как имеющие своей целью, помимо прочего, поддержку отечественного рынка дата-центров.

Таким образом, *законодательство о персональных данных не только направлено на защиту неприкосновенности частной жизни физических лиц, оно также имеет важные экономические, социальные и политические функции, в связи с чем должно учитывать права и законные интересы всех участников отношений и обеспечивать баланс между ними.*

---

<sup>31</sup> Как отметил Майкл Кирби, глава рабочей группы по разработке Руководящих принципов ОЭСР, «существует опасение, что национальное законодательство о защите неприкосновенности частной жизни будет на самом деле использоваться для целей экономического протекционизма» (Kirby M. Legal Aspects of Transborder Data Flows // International Computer Law Adviser. 1991. No. 5. P. 4 ff).

Данное обстоятельство подчеркивается в ряде международных документов. Так, например, в Руководящих принципах ОЭСР указано на необходимость нахождения баланса между противоречивыми интересами – защитой неприкосновенности частной жизни, с одной стороны, и уважением права на свободный обмен информацией, с другой стороны, – для полномасштабного использования потенциала современных технологий обработки данных в той мере, в которой это представляется желательным<sup>32</sup>. При этом ОЭСР прямо признает, что «существует внутренний конфликт между защитой персональных данных и свободным обменом этими данными... интересы, связанные с защитой неприкосновенности частной жизни, может быть трудно отделить от прочих интересов, относящихся к торговле, культуре, национальному суверенитету и пр.»<sup>33</sup>.

Директива 1995 г. прямо называет в числе своих целей не только защиту права на неприкосновенность частной жизни, но и обеспечение свободного движения данных. Именно соображениями необходимости гармонизации законодательств стран – членов ЕС в области защиты персональных данных для целей построения единого европейского рынка и было во многом обусловлено ее принятие<sup>34</sup>. Аналогичные соображения лежали и в основе принятия Регламента 2016 г., направленного не на гармонизацию, а на унификацию законодательства в указанной сфере. Это лишний раз подтверждает тот факт, что законодательство о персональных данных нельзя рассматривать в отрыве от экономической составляющей, которая присутствовала с самого момента его становления. Как указал Европейский Суд Справедливости, «право на защиту персональных данных не является абсолютным правом и должно рассматриваться в контексте выполняемых им функций в обществе»<sup>35</sup>.

---

<sup>32</sup> Explanatory Memorandum to OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980. § 3. URL: <https://goo.gl/bAksLQ>

<sup>33</sup> Ibid. § 11 (h).

<sup>34</sup> *Orla Lynskey*. The Foundations of EU Data Protection Law. 2015. Oxford University Press. P. 47 ff. При этом подготовительные материалы свидетельствуют о намерении Европейской Комиссии использовать данное законодательство для стимулирования развития европейской IT-индустрии. См.: *Bygrave A.* Data Privacy Law: An International Perspective. Oxford: University Press. 2014. P. 125.

<sup>35</sup> *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*. ECJ, Joined Cases C-92/09 and C-93/09. 9 November 2010.

## **Конец ознакомительного фрагмента.**

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.