Российская Газета

УЧРЕДИТЕЛЬ ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральный закон «О персональных данных»: научно-практический комментарий

Под редакцией
заместителя руководителя
Федеральной службы
по надзору в сфере связи,
информационных технологий
и массовых коммуникаций
А.А. Приезжевой

2015

БИБЛИОТЕЧКА РОССИЙСКОЙ ГАЗЕТЫ
ВЫПУСК № 11

БИБЛИОТЕЧКА «РОССИЙСКОЙ ГАЗЕТЫ»

Федеральный закон «О персональных данных»: научно-практический комментарий

Под редакцией заместителя руководителя
Федеральной службы по надзору в сфере связи,
информационных технологий
и массовых коммуникаций
А.А. Приезжевой

Выпуск № 11
2015

Федеральный закон «О персональных данных»: научно-практический комментарий. Под редакцией заместителя руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций А.А. Приезжевой. — М.: Редакция «Российской газеты», 2015. Вып. 11. — 176 с.

В издании анализируются теоретические вопросы обработки персональных данных, рассматриваются достоинства и недостатки Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и приводятся практические примеры его применения.

Комментарий подготовлен на основе действующего законодательства РФ, международно-правовых актов и судебной практики.

Издание предназначено прежде всего для операторов и субъектов персональных данных; может быть использовано в научной и преподавательской деятельности.

Предисловие

В условиях стремительного развития информационно-телекоммуникационных технологий, существенно упростивших и ускоривших процесс обработки колоссальных объемов информации, вопросы защиты частной жизни, предметом которой выступают персональные данные, приобрели особое значение. Сегодня в центре внимания многих международных диалогов, связанных с электронной коммерцией и миграционными процессами, стоят вопросы защиты прав субъектов персональных данных. Неконтролируемое распространение личной информации может причинить существенный вред правам и законным интересам граждан. Так, создание глобального информационного пространства (электронное правительство, цифровые рынки, электронные деньги, электронные услуги) позволяет утверждать, что границы между абстрактной категорией «информация» и носителем этой информации стерты. Виртуальный мир в современных реалиях может представлять угрозу личности, собственности, общественному порядку и государственной безопасности.

В настоящее время объективной реальностью является необходимость обеспечения безопасности персональных данных, поскольку информация о человеке превратилась в дорогой товар. Опыт работы Роскомнадзора в сфере защиты прав субъектов персональных данных свидетельствует о возрастающей потребности общества в безопасном обороте данных, востребованности со стороны граждан в защите их прав как субъектов персональных данных.

Комментарий призван помочь гражданам и организациям в применении Федерального закона «О персональных данных». Он носит научно-практический характер, и в нем наряду со специально-юридическим толкованием законодательных норм, имеющим прикладное значение, даны разъяснения доктринального характера, приведены примеры из правоприменительной практики уполномоченного органа по защите прав субъектов персональных данных.

Ценность комментария состоит в том, что он написан специалистами, работающими в уполномоченном органе по защите прав субъектов персональных данных. В связи с этим читатель сможет получить представление о подходе регулятора к решению ряда практических проблем.

Сведения об авторах

Гафурова Альфия Хасибулловна — заместитель начальника Управления по защите прав субъектов персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Доротенко Елена Владимировна — юрисконсульт ФГУП «Главный радиочастотный центр».

Контемиров Юрий Евгеньевич — начальник Управления по защите прав субъектов персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

ФЕДЕРАЛЬНЫЙ ЗАКОН
«О ПЕРСОНАЛЬНЫХ ДАННЫХ»

Принят Государственной Думой
8 июля 2006 года

Одобрен Советом Федерации
14 июля 2006 года

Подписан Президентом РФ 27 июля 2006 года № 152-ФЗ

(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)

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. *(часть первая в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

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 25.07.2011 № 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». *(п. 5 введен Федеральным законом от 28.06.2010 № 123-ФЗ)*

1. Положения ст. 1 комментируемого закона определяют сферу его действия применительно к общественным отношениям, связанным с обработкой персональных данных.

Так, согласно ч. 1 анализируемой статьи требования закона распространяются при обработке персональных данных как федеральными органами государственной власти, так и органами государственной власти субъектов РФ, органами местного самоуправления, муниципальными органами, юридическими и физическими лицами, при этом законодатель определяет способы обработки персональных данных, при использовании которых вышеуказанные участники общественных отношений попадают под сферу влияния закона. Речь идет об использовании средств автоматизации, включая информационно-телекоммуникационные сети, или без использования таковых, если обработка персональных данных без использования таких средств соответствует характеру действий, которые совершаются с персональными данными с использованием средств автоматизации. Далее в рассматриваемой части законодатель сужает сферу действия закона посредством уточнения, что именно можно считать неавтоматизированной обработкой, а именно: возможность осуществления поиска персональных данных в соответствии с заданным алгоритмом.

Следует отметить, что вопрос о распространении требований комментируемого закона к неавтоматизированной обработке персональных данных вызывает у участников рассматриваемых правоотношений дискуссии. Это связано прежде всего с тем, что нередки случаи, когда алгоритм поиска персональных данных при использовании бумажного оборота данных отсутствует, и тогда делается вывод о нераспространении требований законодательства о персональных данных на указанный вид обработки. При этом зачастую может не учитываться фактор наличия доступа к таким персональным данным, а этот способ неавтоматизированной обработки персональных данных отнесен в том числе законодателем к сфере действия комментируемого закона.

☑ Например, в п. 1 ст. 89 Федерального закона от 26.12.1995 № 208-ФЗ «Об акционерных обществах» установлен перечень документов, которые общество обязано хранить. Этот перечень не является закрытым. В нем непосредственно указано, что общество обязано хранить и иные документы, предусмотренные названным законом; уставом общества; внутренними документами общества; решениями общего собрания акционеров, совета директоров (наблюдательного совета) общества, органов управления общества; правовыми актами РФ. При этом

хранение документов акционерного общества не предусматривает алгоритма поиска персональных данных. Вместе с тем в силу ст. 91 Федерального закона «Об акционерных обществах» общество обязано обеспечить акционерам доступ к документам, предусмотренным п. 1 ст. 89. Таким образом, хранение документов без соответствующих алгоритмов поиска персональных данных осуществляется наряду с обязанностью предоставления доступа к указанным документам, в связи с чем такая неавтоматизированная обработка будет производиться в соответствии с требованиями комментируемого закона.

2. Если ч. 1 анализируемой статьи определяет сферу действия закона, то ч. 2 содержит в себе исчерпывающий перечень отношений, на которые его требования не распространяются. Это отношения по обработке персональных данных для личных и семейных нужд, при отсутствии нарушения прав субъектов персональных данных, отношения в сфере организации хранения, комплектования, учета и использования документов Архивного фонда РФ, отношения по обработке персональных данных, отнесенных к сведениям, составляющим государственную тайну, а также отношения, возникающие при предоставлении уполномоченными органами информации о деятельности судов в России в соответствии с требованиями Федерального закона от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

Исключение законодателем возможности распространения действия комментируемого закона на отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, обусловлено тем, что в отношении указанных сведений действует особый режим государственной защиты. Обработка (сбор, ознакомление) сведений, составляющих государственную тайну, подразумевает ряд ограничений для лиц, допущенных к таким сведениям, в том числе принятие обязательств по нераспространению доверенных им сведений, составляющих государственную тайну, согласие на частичные, временные ограничения их прав, таких как выезд за пределы границ РФ, и неприкосновенность частной жизни, в части проведения проверочных мероприятий в отношении лиц, допущенных к работе с такими сведениями. Также сведения, составляющие государственную тайну, подлежат обязательному засекречиванию.

При этом комментируемый закон не налагает на участников правоотношений по обработке персональных данных подобных обязательств и ограничений при обработке персональных данных, а меры, принима-

емые операторами по защите персональных данных, не предусматривают режима, аналогичного режиму по защите сведений, составляющих государственную тайну.

Следует отметить, что п. 1 и 4 ч. 2 ст. 1 анализируемого закона соответствуют п. «а» и «б» ч. 1 Федерального закона от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», согласно которым Российской Федерацией были сделаны оговорки по неприменению Конвенции о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. (далее – Конвенция 1981 года) к персональным данным, обрабатываемым физическими лицами исключительно для личных и семейных нужд, и отнесенным в установленном порядке к сведениям, относящимся к государственной тайне.

Под обработкой персональных данных для личных и семейных нужд в рамках указанного исключения подразумеваются действия физического лица по формированию массива данных, предоставленных им третьими лицами, в том числе с использованием личных электронных устройств, личной электронной почты. Это могут быть списки контактов в мобильных телефонах, визитки, список пользователей в коммуникационных сервисах.

Организация хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда РФ и других архивных документов регламентируется Федеральным законом от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», а также принимаемыми в соответствии с ним иными нормативными правовыми актами РФ и субъектов РФ. Отличие данного вида правоотношений от правоотношений по обработке персональных данных заключается в том, что названный закон не регулирует отношения, связанные с автоматизированной обработкой, поскольку в архивном законодательстве отсутствует понятие «электронного архива».

В 2010 году из сферы регулирования комментируемого закона были исключены отношения, возникающие при предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом «Об обеспечении доступа к информации о деятельности судов в Российской Федерации». Согласно п. 2 ст. 1 указанного закона **информация о деятельности судов** — информация, подготовленная в пределах своих полномочий судами, Судебным департаментом, органами Судебного департамента, органами судейского сообщества либо поступившая в суды,

Судебный департамент, органы Судебного департамента, органы судейского сообщества и относящаяся к деятельности судов. Законодательство РФ, устанавливающее порядок судопроизводства, полномочия и порядок деятельности судов, Судебного департамента, органов Судебного департамента, органов судейского сообщества, судебные акты по конкретным делам и иные акты, регулирующие вопросы деятельности судов, также относятся к информации о деятельности судов. На иные виды судебной деятельности данное исключение не распространяется.

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.

Цель комментируемого закона направлена на обеспечение защиты прав и свобод человека и гражданина как субъекта персональных данных в соответствии с основными правоустанавливающими законодательными актами.

В целях защиты прав граждан в области персональных данных Российская Федерация с учетом трансграничности потоков персональных данных в первую очередь обеспечила имплементацию в российское законодательство требований общеевропейского права, создала систему защиты прав субъектов персональных данных, соответствующую основным принципам, заложенным в межгосударственных нормативных правовых актах в области персональных данных.

Первоначально положения, касающиеся защиты прав граждан в области персональных данных, были отражены во Всеобщей декларации прав человека, принятой Генеральной Ассамблеей ООН 10 декабря 1948 г. Впоследствии они получили развитие и отражение в Конвенции 1981 года, ратифицированной Российской Федерацией в 2013 году, а также в Директиве Европейского парламента и Совета Европейского союза от 24.10.1995 № 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных».

В положениях двух последних из названных актов конкретизировано понятие «персональные данные», установлены основные принципы и цели защиты прав субъектов персональных данных, определены права граждан, в том числе на доступ к информации, и обязанности операторов, осуществляющих обработку их персональных данных.

Законодательство РФ в области персональных данных, с учетом проведенных мероприятий по совершенствованию и гармонизации его положений, почти в полном объеме повторяет основные положения вышеуказанных международных актов.

Так, в ст. 23 Конституции РФ установлено, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только в исключительных случаях, предусмотренных законом.

Следующим шагом стало принятие Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Закон о персональных данных), который послужил основой возникновения обособленной отрасли информационного права, позволившей в Российской Федерации практически с нуля создать систему защиты прав граждан как субъектов персональных данных с учетом международного опыта.

В подтверждение данного вывода достаточно провести параллели между комментируемой статьей и формулировкой цели, заложенной в тексте Конвенции 1981 года, которая 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*».

При этом следует иметь в виду, что в сферу правового регулирования попадают не все общественные отношения, а лишь наиболее социально значимые, требующие воздействия и охраны со стороны государства. В связи с этим нормативные правовые акты, регулирующие соответствующие сферы общественных отношений, должны быть целесообразными, иметь определенное предназначение, оправдывающее вмешательство государства в эту область отношений.

Закрепленные в статье цели комментируемого закона представляют собой один из приемов юридической техники. Они призваны обозначить ориентиры правового регулирования общественных отношений в сфере защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни.

Под целями применительно к комментируемой статье необходимо понимать конечные результаты, на достижение которых направлено правовое регулирование в соответствии с Законом о персональных данных.

Результатом правового регулирования рассматриваемых общественных отношений является достижение личной безопасности, характеризующейся состоянием защищенности жизненно важных интересов личности от потенциально и реально существующих угроз, или отсутствие таких угроз, где права человека и состояние их защищенности являются отражением уровня зрелости социальной политики государства, которое одной из своих задач ставит обеспечение прав и безопасности своих граждан. Решению этой задачи должна быть подчинена деятельность всех государственных институтов. Состояние защищенности и баланс интересов личности, общества и государства во всех сферах жизнедеятельности может обеспечивать устойчивое развитие страны и способствовать достижению национальной безопасности.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)

В целях настоящего Федерального закона используются следующие основные понятия:

1) персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

В комментируемой статье раскрываются основные термины и понятия, используемые в Законе о персональных данных. По сути, данная статья носит разъяснительный характер, закрепляя единое толкование терминов, которые применяются в данном законодательном акте. Потребность их толкования обусловлена чаще всего тем, что одно и то же понятие (термин), используемое даже в рамках одной отрасли права, может интерпретироваться по-разному.

Кроме этого, законодателю важно, чтобы каждое из включаемых им в закон понятий было определенным и исключало бы его разнообразную трактовку.

Так, в анализируемой статье законодатель раскрывает понятие персональных данных, субъектный состав операторов персональных данных, а также виды обработки персональных данных.

В настоящее время наибольшую дискуссию вызывает понятие персональных данных. В связи с этим Роскомнадзором в рамках Консультативного совета при уполномоченном органе по защите прав субъектов персональных данных было предложено создать рабочую группу по определению матрицы персональных данных[1].

В соответствии с п. 1 комментируемой статьи **персональные данные** — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

[1] Материалы, используемые в комментарии к настоящей статье, предоставили члены рабочей группы под председательством В.В. Архипова (А.Э. Адилова, Е.А. Войниканис, А.Г. Бодров, М.С. Овешников, К.Т. Сумманен).

Данное определение практически идентично определению, установленному пп. «*а*» ст. 2 Конвенции 1981 года, согласно которому персональные данные означают любую информацию об определенном или поддающемся определению физическом лице («субъект данных»). В то же время с точки зрения принципов права, действующих в российской правовой системе, можно усомниться в формальной определенности[1] понятия «персональные данные».

При буквальном толковании (применяемом в правоприменительной практике «по умолчанию») рассматриваемой нормы к понятию «персональные данные» можно отнести широкий круг информации, в том числе выходящий за рамки разумно ожидаемого в данном контексте. В частности, в нем нет указания на связь между информацией и прямой или косвенной определенностью или «определяемостью» физического лица. Соответственно, отсутствует однозначное понимание того, в каких случаях собираемые и обрабатываемые данные будут относиться к персональным, а в каких — нет.

Вместе с тем рабочей группой были высказаны сомнения относительно возможности сформулировать адекватное определение, имеющее менее общий характер.

В целом члены рабочей группы согласны в том, что если совокупность данных необходима и достаточна для идентификации лица, такие данные следует считать персональными данными, даже если они не включают в себя данные документов, удостоверяющих личность. При этом данные нельзя считать персональными в том случае, если без использования дополнительной информации они не позволяют идентифицировать физическое лицо. Изложенный подход допустимо рассматривать как учитывающий баланс интересов всех участников отношений.

---

[1] Принцип формальной определенности закона, сформулированный в практике Конституционного Суда РФ, вытекает из ч. 1 ст. 1, ч. 2 ст. 4, ч. 2 ст. 6, ч. 2 ст. 15 и ч. 1 ст. 19 Конституции РФ и предполагает точность, ясность и недвусмысленность правовых норм, без чего не может быть обеспечено единообразное понимание и применение таких норм, а значит, и равенство всех перед законом (см., напр., постановление Конституционного Суда РФ от 08.04.2014 № 10-П «По делу о проверке конституционности положений пункта 6 статьи 2 и пункта 7 статьи 32 Федерального закона „О некоммерческих организациях“, части шестой статьи 29 Федерального закона „Об общественных объединениях“ и части 1 статьи 19.34 Кодекса Российской Федерации об административных правонарушениях в связи с жалобами Уполномоченного по правам человека в Российской Федерации, фонда „Костромской центр поддержки общественных инициатив“, граждан Л.Г. Кузьминой, С.М. Смиренского и В.П. Юкечева».

По результатам анализа российской судебной практики за 2014 год можно выделить следующие характерные примеры персональных данных, нашедшие прямое отражение в текстах правоприменительных актов:

- паспортные данные (см. например, апелляционное определение Московского городского суда от 22.05.2014 № 33-14709);
- данные технического паспорта на дом (см., например, определение Приморского краевого суда от 28.04.2014 № 33-3718);
- адреса места жительства индивидуальных предпринимателей, указанные в плане проведения проверок юридических лиц и индивидуальных предпринимателей, размещенном в общем доступе на официальном сайте администрации (см., например, апелляционное определение Волгоградского областного суда от 24.04.2014 № 33-4427/2014);
- сведения о пересечении государственной границы (см., например, апелляционное определение Московского городского суда от 10.04.2014 № 33-11688);
- адрес регистрации должностного лица, сведения о его доходах и собственности, распространяемые в непредусмотренных для официальной процедуры форме (см., например, определение Санкт-Петербургского городского суда от 31.03.2014 № 33-4198/14);
- данные работника, указанные в трудовом договоре (см., например, апелляционное определение Верховного суда Республики Саха (Якутия) от 23.10.2013 № 33-4172/13).

Членами рабочей группы были представлены также отдельные примеры, основанные на опыте работы с персональными данными. В частности, к числу идентификаторов (данных, позволяющих однозначно идентифицировать физическое лицо), которые сами по себе однозначно определяют физическое лицо, могут быть отнесены: номер и серия паспорта; страховой номер индивидуального лицевого счета; идентификационный номер налогоплательщика; биометрические данные; банковский счет, номер банковской карты.

Приоритет при этом следует отдавать идентификаторам, присваиваемым государством, однако остается открытым вопрос о том, что может являться персональными данными — сам идентификатор, идентификатор и информация о том, что это именно идентификатор, а не набор цифр, имеющий какое-либо иное значение. Кроме этого, следующие данные также можно рассматривать как персональные,

несмотря на то, что в их отношении остается некоторый аспект вероятного совпадения:

- фамилия, имя, отчество, дата рождения, место прописки;
- фамилия, имя, отчество, дата рождения, должность;
- фамилия, имя, отчество (возможно, фамилия и инициалы) плюс любая информация, выделяющая субъекта из уже ограниченного круга лиц.

☑ Например, житель дома А.А. Иванов имеет такие-то долги. Скорее всего, подобное объявление в подъезде однозначно идентифицирует субъекта, по меньшей мере, для жителей этого дома. Пока, однако, неясно, как точно дать определение ограниченного круга лиц, потому что «жители Москвы» — тоже ограниченный круг лиц, а житель Москвы А.А. Иванов — это уже не конкретный субъект (вместе с тем пример с «жителем дома А.А. Ивановым» подтверждается судебной практикой).

Членами рабочей группы также были представлены отдельные примеры, основанные на опыте работы с персональными данными. Так, к числу данных, которые не могут рассматриваться, по крайней мере, по отдельности друг от друга в качестве персональных, могут быть отнесены: фамилия, имя, отчество, адрес проживания, электронный адрес, номер телефона, дата рождения. Другие идентификаторы сами по себе не определяют однозначно конкретное физическое лицо. Такие данные должны быть отнесены к персональным данным только в том случае, если они хранятся и обрабатываются совместно с идентификаторами, которые сами по себе определяют физическое лицо.

Одним из ключевых понятий, содержащихся в комментируемой статье, является «**оператор персональных данных**», к которому относятся государственный орган, муниципальный орган, юридическое или физическое лицо. При этом следует отметить, что данное понятие не имеет национального признака, т.е. операторами могут быть как российские, так и иностранные граждане. Признаками причисления к данному понятию являются самостоятельная или совместно с другими лицами организация и (или) осуществление обработки персональных данных, а также определение целей обработки персональных данных, состава персональных данных, подлежащих обработке, действий (операций), совершаемых с персональными данными.

Еще одним собирательным понятием, имеющим высокую степень важности, является понятие «**обработка персональных данных**». Фактически обработка персональных данных подразумевает любые операции с ними — от сбора до полного уничтожения последних. Таким образом,

обработка включает в себя любые действия оператора с персональными данными: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Следует отметить, что законодателем не раскрывается определение понятий всего перечня видов обработки персональных данных.

Учитывая, что комментируемая статья не содержит определение понятия «**хранение**», полагаем, что законодатель вкладывает в него обычно используемое в повседневной жизни значение.

Так, согласно ГОСТ Р 7.0.8-2013 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения», утвержденному приказом Росстандарта от 17.10.2013 № 1185-ст, хранение документов представляет собой организацию рационального размещения и обеспечение сохранности документов. При этом указанный ГОСТ в рамках единого процесса хранения документов разделяет архивное, оперативное, ведомственное и иные виды хранения документов. В зависимости от срока хранения документов различают оперативное и архивное хранение, в зависимости от лиц, которые осуществляют хранение документов, хранение может быть ведомственным и архивным. Иными словами, хранение представляет собой срочный или бессрочный процесс, подразумевающий нахождение документов в какой-либо организации или месте.

Применяя аналогию права к отношениям в области персональных данных, можно сказать, что хранение представляет собой срочный или бессрочный процесс, подразумевающий нахождение персональных данных в какой-либо организации или месте.

Понятие «**передача**» также не раскрыто законодателем. Вместе с тем под передачей понимается процесс по направлению информации или документов какому-либо лицу каким-либо способом.

При этом согласно ГОСТ Р ИСО 15489-1-2007 «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования», утвержденному приказом Ростехрегулирования от 12.03.2007 № 28-ст, передача (*transfer*) (в отношении способа хранения) — это изменение способа хранения документов, права собственности и (или) ответственности за документы. То есть, если рассматривать процесс передачи более детально, он, безусловно, представляет собой перенос ответственности или части ответственности за инфор-

мацию на другое лицо и изменение способа и места хранения этой информации.

Однако применительно к персональным данным передача является самостоятельным процессом обработки данных, который должен осуществляться в заранее определенных и законных целях.

Надо иметь в виду, что трактовка таких понятий, как обезличивание, блокирование, удаление или уничтожение, может представлять собой не только действия по обработке персональных данных, но и меры, направленные на предотвращение или прекращение незаконной обработки персональных данных.

Блокирование персональных данных — это временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных является действием, в результате которого невозможно восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которого уничтожаются материальные носители персональных данных.

Обезличивание персональных данных — действие, в результате которого невозможно без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Весьма важное юридическое значение законодатель придает понятиям «распространение персональных данных» и «предоставление персональных данных». Различие указанных понятий заключается в том, что при распространении персональных данных информация раскрывается неограниченному кругу лиц, тогда как предоставление обращено на раскрытие персональных данных определенному лицу или определенному кругу лиц.

В практике Роскомнадзора имеются случаи выявления фактов распространения образовательными организациями персональных данных несовершеннолетних в Интернете. Размещение данной информации в Интернете квалифицируется именно как распространение информации неограниченному кругу лиц в публичном информационном источнике. Такое распространение может повлечь бесконтрольную обработку персональных данных третьими лицами, в частности, появляется возможность их копирования, трансформации, дополнения лживыми комментариями, домыслами и проч. Таким образом, оператор,

разместив в Интернете персональные данные граждан, которые он собрал в определенных целях, уже не сможет проконтролировать и обеспечить обещанные субъекту данных условия обработки.

Вместе с тем размещение, например, персональных данных учеников на стендах в образовательных организациях, будет квалифицироваться как «предоставление персональных данных», а значит, раскрытие персональных данных ограниченному кругу лиц: ученикам и их родителям, учителям и иным лицам, имеющим доступ в образовательную организацию.

Комментируемая статья содержит также понятие **трансграничной передачи персональных данных**, под которой понимается передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Согласно положениям Закона о персональных данных в части трансграничной передачи персональных данных в ряде случаев оператору потребуется согласие субъекта персональных данных на их передачу в иностранные государства, не являющиеся участниками Конвенции 1981 года, и не включенные в перечень иностранных государств, обеспечивающих адекватную защиту персональных данных.

Более подробное описание трансграничной передачи персональных данных см. в комментарии к ст. 12 Закона о персональных данных.

Статья 4. Законодательство Российской Федерации в области персональных данных

1. Законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из настоящего Федерального закона и других определяющих случаи и особенности обработки персональных данных федеральных законов.

2. На основании и во исполнение федеральных законов государственные органы, Банк России, органы местного самоуправления в пределах своих полномочий могут принимать нормативные правовые акты, нормативные акты, правовые акты (далее — нормативные правовые акты) по отдельным вопросам, касающимся обработки персональных данных. Такие акты не могут содержать положения, ограничивающие права субъектов персональных данных, устанавливающие не предусмотренные федеральными законами ограничения деятельности операторов или возлагающие на операторов не предусмотренные федеральными законами обязанности, и подлежат официальному опубликованию. *(часть вторая в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

3. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными

законами и иными нормативными правовыми актами Российской Федерации с учетом положений настоящего Федерального закона.

4. Если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора.

1. Комментируемая статья определяет систему законодательных и иных нормативных правовых актов РФ, регулирующих отношения в области персональных данных.

В соответствии с Конституцией РФ общепризнанные принципы и нормы международного права и международные договоры РФ являются составной частью ее правовой системы. Если международным договором РФ установлены иные правила, чем предусмотренные законом, то применяются правила международного договора.

Российское законодательство в области персональных данных тесно взаимосвязано с источниками международного права, прежде всего с Конвенцией 1981 года, участницей которой является Россия. Указанная конвенция была ратифицирована в 2005 году Федеральным законом «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» с отдельными поправками. В связи с этим Российская Федерация взяла на себя обязательства по приведению в соответствие с нормами европейского законодательства деятельности в области защиты прав субъектов персональных данных. Первым шагом в реализации взятых обязательств стало принятие Закона о персональных данных. Завершающим этапом процедуры ратификации Конвенции 1981 года стало принятие Федерального закона от 07.05.2013 № 99-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона „О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных“ и Федерального закона „О персональных данных“».

Для Российской Федерации Конвенция 1981 года вступила в силу с 1 сентября 2013 г. Данный срок вступления в силу Конвенции 1981 года обусловлен исполнением Российской Федерацией взятых обязательств в рамках этой конвенции.

Значимым достоинством Конвенции 1981 года является достаточно подробный акцент на ключевые положения в области персональных данных. В сущности, названная конвенция, определяя базовые понятия в области защиты персональных данных, является основным международным актом в области защиты персональных данных.

Конвенция 1981 года охватывает многие важные вопросы, связанные с ее целями, принципами защиты данных, трансграничными потоками, взаимной помощью, составом и функциями Консультативного комитета.

Определяющее положение по отношению ко всем другим источникам российского законодательства занимает Конституция РФ как Основной Закон государства. Она является источником права, выступая в качестве юридической базы его развития. В то же время Конституция РФ содержит нормы, имеющие непосредственное отношение к личной информации.

Статьи 23, 24 Конституции РФ устанавливают право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, а также запрещают сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Это положение является основополагающим при правовом регулировании деятельности в области персональных данных.

Важным источником также является Трудовой кодекс РФ. В гл. 14 ТК РФ сконцентрированы нормы, регулирующие основные положения по защите персональных данных работника, требования при обработке, в том числе хранении и использовании, а также передачи персональных данных работника и т.д.

Глава 7 Федерального закона от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации» посвящена персональным данным гражданского служащего.

> **Таким образом**, законодательство РФ в области персональных данных, основываясь на Конституции РФ и международных договорах РФ, состоит из Закона о персональных данных, а также других определяющих случаи и особенности обработки персональных данных федеральных законов.

Следует иметь в виду, что Закон о персональных данных является актом комплексного характера, содержащим не только гражданско-правовые нормы, но и нормы других отраслей права. Если проанализировать содержание норм и актов, составляющих законодательство в области персональных данных, то большинство из них принадлежит к гражданскому, административному, предпринимательскому и другим отраслям права и законодательства.

2. Часть 2 комментируемой статьи базируется на положении, определяющем полномочия государственных органов, Банка России, органов местного самоуправления по принятию на основании и во испол-

нение федеральных законов в пределах своих полномочий нормативных правовых актов по отдельным вопросам, касающимся обработки персональных данных.

При этом такие акты не могут содержать положения, ограничивающие права субъектов персональных данных, устанавливающие не предусмотренные федеральными законами ограничения деятельности операторов или возлагающие на операторов не предусмотренные федеральными законами обязанности, и подлежат официальному опубликованию.

> **Таким образом**, государственные органы, Банк России, органы местного самоуправления при подготовке внутренних ведомственных актов, затрагивающих вопросы обработки персональных данных, должны соблюдать указанные выше требования к актам.

В практике Роскомнадзора имелись случаи выявления ведомственных актов, не соответствующих Закону о персональных данных в части избыточного объема обработки персональных данных, несоответствия обработки персональных данных целям их сбора и др. По результатам выявления подобных фактов Роскомнадзором принимались соответствующие меры реагирования, направленные на приведение в соответствие таких актов Закону о персональных данных.

3. Часть 3 комментируемой статьи устанавливает, что особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами РФ с учетом положений Закона о персональных данных.

Так, постановлением Правительства РФ от 15.09.2008 № 687 утверждено Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.

Согласно данному положению обработкой персональных данных без применения средств автоматизации считаются использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека.

Вместе с тем в 2011 году законодатель закрепил новое понятие автоматизированной обработки персональных данных, под которой понимается обработка персональных данных с помощью средств вычислительной техники (ст. 3 Закона о персональных данных). Прежде обработка персональных данных в компьютерной (информационной)

системе не приравнивалась к обработке сведений с помощью средств автоматизации (п. 2 вышеназванного положения). В настоящее время вся обработка персональных данных с использованием вычислительной техники считается автоматизированной, и к ней применяются в том числе требования постановления Правительства РФ 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Каждый оператор персональных данных обязан привести в соответствие с этими требованиями систему защиты персональных данных, хранящихся и обрабатываемых в электронных информационных системах.

4. Как следует из ч. 4 анализируемой статьи, если международным договором РФ установлены иные правила, чем предусмотренные Законом о персональных данных, то применяются правила международного договора РФ. Указанная норма определяет правила разрешения правовых коллизий между положениями комментируемого закона и положениями международных договоров в случае их возникновения.

С момента принятия в 1993 году Конституции РФ общепризнанные нормы и принципы международного права и международные договоры РФ являются составной частью ее правовой системы (ст. 15). Утверждение приоритета норм международного права перед национальным законодательством потребовало серьезного изменения в подходах к разработке и оценке внутреннего законодательства.

Защита персональных данных является одним из направлений международного сотрудничества Российской Федерации и иностранных государств. В частности, международное сотрудничество Российской Федерации в области защиты персональных данных в настоящее время регулируется Конвенцией 1981 года.

Важным условием действия международного договора на территории Российской Федерации для презюмируемого комментируемой нормой приоритета над нормами российского законодательства является выражение согласия Российской Федерации на обязательность для нее международного договора. В соответствии с пп. «б» — «г» ст. 2 Федерального закона от 15.07.1995 № 101-ФЗ «О международных договорах Российской Федерации» формами выражения такого согласия Российской Федерации выступают ратификация, утверждение, принятие, присоединение, а также подписание и заключение международного договора.

Ратификация как форма выражения согласия Российской Федерации на обязательность для нее условий международных договоров тре-

бует принятия соответствующего федерального закона. Данная форма выражения согласия актуальна для тех международных договоров, в том числе в области персональных данных, которыми устанавливаются иные правила, чем предусмотренные российским законодательством (ст. 14, пп. «*а*» п. 1 ст. 15 названного закона). Следовательно, учитывая положения комментируемой нормы, международные договоры, о которых идет речь в ст. 4 Закона о персональных данных, подлежат в обязательном порядке ратификации в форме федерального закона.

Для России ратификация Конвенции 1981 года породила обязательства по приведению в соответствие с этой конвенцией норм национального законодательства.

Кроме этого, в рамках СНГ международные отношения в сфере защиты прав субъектов персональных данных регулируются Модельным законом «О персональных данных», принятым постановлением от 16.10.1999 № 14–19 на 14-м пленарном заседании Межпарламентской Ассамблеи государств — участников СНГ.

В модельном законе определено содержание категорий «персональные данные», «база персональных данных», «операции с персональными данными» и иных. Также в нем закреплены правовой режим персональных данных и основные формы государственного регулирования в данной области, уделено внимание трансграничной передаче персональных данных, предусмотрены права и обязанности субъекта персональных данных и держателя персональных данных.

Глава 2
Принципы и условия обработки персональных данных

Статья 5. Принципы обработки персональных данных
(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

1. Комментируемая статья базируется на нормах Конституции РФ. Так, в ст. 24 Основного Закона установлены запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия, а также обязанность со стороны органов государственной власти, органов местного самоуправления, их должностных лиц обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы.

Кроме этого, согласно ч. 4 ст. 29 Конституции РФ каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

Конституция РФ формирует и закрепляет отправные принципы правового регулирования обработки персональных данных.

> **Таким образом**, комментируемая статья определяет ряд отраслевых принципов, корреспондирующих положениям Конституции РФ и являющихся основополагающими началами обработки персональных данных в Российской Федерации.

Часть 1 ст. 5 Закона о персональных данных определяет, что обработка персональных данных должна осуществляться на законной и справедливой основе.

Данная норма является первым и главным постулатом обработки персональных данных, поскольку любая обработка персональных данных должна основываться на законах, т.е. на установленном государством своде обязательных правил и норм общественного поведения всех субъектов на территории страны, включающем перечень запретов и ограничений.

Помимо этого, любая обработка должна осуществляться на справедливой основе, т.е. на морально-правовой категории, отражающей представление о должном соблюдении общечеловеческих ценностей, принципов морали, чести, права, закона.

2. Часть 2 комментируемой статьи предусматривает, что обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Давая согласие на обработку своих персональных данных, субъект персональных данных должен быть проинформирован о целях их обработки. Соответственно, цели обработки должны быть включены в форму согласия субъекта персональных данных.

Зачастую при заключении гражданско-правовых договоров субъектам предлагается согласиться с распространением персональных дан-

ных третьим лицам. Однако при заключении гражданско-правового договора неправомерно требовать от субъекта согласия на распространение его персональных данных третьим лицам, если распространение не обусловлено самим договором или в силу требований законодательства.

Также в практике Роскомнадзора имели место случаи размещения персональных данных несовершеннолетних в открытом доступе в Интернете. Однако такой способ обработки персональных данных представляет собой распространение собранных данных неограниченному кругу лиц. Более того, целью сбора персональных данных несовершеннолетних (о результатах олимпиад, конкурсов, о зачислении в образовательные организации) является информирование участников образовательных отношений (обучающихся, родителей, законных представителей, учителей и иных лиц, ответственных за образование).

Учитывая, что цели сбора персональных данных предусматривают возможность получения личной информации и ее использование ограниченным кругом лиц (участниками образовательных отношений), оператором персональных данных должна быть обеспечена возможность доступа к собранным данным только указанной группе лиц.

☑ Так, доступ к обезличенным сведениям о результатах олимпиад, конкурсов, а также о зачислении в образовательные организации может быть предоставлен неограниченному кругу лиц. При этом доступ к сведениям, содержащим персональные данные, может быть обеспечен через «личные кабинеты» участников образовательных отношений — пользователей сайтов образовательных организаций в Интернете.

➥ **Таким образом**, в случае, когда данные о несовершеннолетних собираются для информирования их родителей, выкладывание эти данных в Интернете будет превышать цель обработки, ради которой они были собраны, даже при наличии отдельного согласия родителей на такую обработку.

В практической деятельности Роскомнадзор также сталкивается с вопросом согласования различных проектов международных соглашений о сотрудничестве и обмене информацией, в том числе содержащей персональные данные. В ходе проведенного анализа Роскомнадзор выявил, что в данных соглашениях зачастую отсутствуют цели обмена информацией об иностранных гражданах, лицах без гражданства. При этом не разграничиваются понятия «цели обмена персональными данными» и «цели заключения соглашения», последние, как правило, в проектах соглашений указаны.

3. В ч. 3 анализируемой статьи предусмотрен запрет на объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Положение о том, что нельзя совмещать базы данных с персональными данными, обрабатываемыми в различных целях представляется очевидным. Следует отметить, что обработке подлежат только персональные данные, которые отвечают целям их обработки.

☑ Так, например, база данных «Зарплата и управление персоналом» предназначена для автоматизации кадрового учета и расчета заработной платы на предприятиях. Указанная база данных не подлежит совмещению с базой данных, обрабатываемых в иных целях.

4. В ч. 4 комментируемой статьи установлено, что обработке подлежат только персональные данные, которые отвечают целям их обработки. Иными словами, для достижения поставленных целей оператор прибегает к обработке тех персональных данных, которые собраны для достижения определенных задач и целей. Например, работодатель обрабатывает персональные данные работников, состоящих с ним в трудовых отношениях, а также лиц, состоящих с ним в гражданско-правовых отношениях.

Ключевым принципом законодательства в области персональных данных является принцип, согласно которому содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. При этом обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

В данном принципе законодатель разграничивает понятия «содержание персональных данных» и «объем персональных данных».

Содержание персональных данных есть то, что наполняет данные и из чего они состоят, т.е. определяет внутреннее наполнение отдельно взятой категории данных. Например, адрес субъекта персональных данных может содержать совокупность сведений о стране, городе, улице, доме, этаже, квартире, индексе и проч. Также, например, раскрытие специальной категории персональных данных или биометрических персональных данных будет олицетворять содержание персональных данных.

Вместе с тем объем персональных данных представляет собой количественный показатель. Данный показатель раскрывает количество персональных данных, т.е. перечень сведений, содержащий персональные данные, которые подлежат обработке (например, фамилия, имя,

отчество, дата и место рождения, место жительства и регистрации, сетчатка глаза, отпечатки пальцев и др.).

По смыслу законодателя, содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

☑ Например, полученные судебным приставом-исполнителем в ходе принудительного исполнения судебных актов, актов других органов или должностных лиц персональные данные обрабатываются им исключительно в целях исполнения исполнительных документов в необходимом для этого объеме.

Для того чтобы установить, в каком объеме работодатель вправе получать от работника информацию о его персональных данных, необходимо обратить внимание на целевой характер использования персональных данных.

☑ Так, обработка персональных данных государственного служащего не требует получения соответствующего согласия указанного лица, при условии, что объем обрабатываемых работодателем персональных данных не превышает установленные перечни, а также соответствует целям обработки, предусмотренным законодательством РФ о государственной гражданской службе.

5. Актуальными остаются вопросы, связанные с избыточностью обрабатываемых персональных данных субъекта персональных данных применительно к целям обработки. Однако действующее законодательство не содержит критериев избыточности обрабатываемых персональных данных. Вместе с тем по смыслу закона обработка избыточных персональных данных означает превышение объема обработки персональных данных, установленного законом или договором.

6. В ч. 6 рассматриваемой статьи устанавливается обязанность по обеспечению точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных. При этом оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных. Установление указанной обязанности оператора направлено на защиту прав субъекта персональных данных и находит свое дальнейшее развитие в иных положениях комментируемого закона (*см. комментарии к ст. 18 и 19 Закона о персональных данных*).

7. Завершает систему принципов основополагающее положение, относящееся к хранению персональных данных. Так, в ч. 7 коммен-

тируемой статьи закреплены требования к длительности хранения персональных данных, а также к порядку завершения такого хранения. Законодатель установил, что хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных. При этом обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Статья 6. Условия обработки персональных данных

(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее — исполнение судебного акта);

4) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг; *(в ред. Федерального закона от 05.04.2013 № 43-ФЗ)*

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в том числе в случае реализации оператором своего права на уступку прав (требований) по такому договору, а

также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем; *(п. 5 в ред. Федерального закона от 21.12.2013 № 363-ФЗ)*

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее — персональные данные, сделанные общедоступными субъектом персональных данных);

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

2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего Федерального закона.

3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее — поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона.

4. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

5. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

1. Рассматриваемая статья определяет случаи, при которых допускается обработка персональных данных, т.е. устанавливает условия легитимности деятельности оператора по обработке персональных данных.

Концептуальным является положение п. 1 ч. 1 комментируемой статьи, согласно которому необходимым условием обработки персональных данных служит наличие согласия субъекта персональных данных на обработку его персональных данных. Исходя из правоприменительной практики, обработка персональных данных в других случаях не требует получения согласия, если иное не предусмотрено федеральными законами и принятыми на их основе нормативными правовыми актами.

Так, в постановлении Первого арбитражного апелляционного суда от 12.10.2011 № 01АП-4438/11 указано, что получение согласия субъекта (абонента) на обработку персональных данных, за исключением случаев, установленных действовавшими на момент рассмотрения спора Правилами оказания услуг подвижной связи, утвержденными постановлением Правительства РФ от 25.05.2005 № 328, является обязательным.

Согласно п. 2 ч. 1 комментируемой статьи обработка персональных данных допускается для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения возложенных законодательством РФ на оператора функций, полномочий и обязанностей.

На сегодняшний день действует значительное число международных договоров, регламентирующих порядок и условия обработки персональных данных в различных сферах жизнедеятельности, в том числе при оказании услуг авиаперевозок, осуществлении реадмиссии, оказании правовой и судебной помощи.

Соответственно, обработка персональных данных в рамках указанных договоров не только может устанавливать условия, отличные от положений Закона о персональных данных, но и не ставит под сомнение сам факт правомерности осуществления указанной деятельности.

Применительно к условиям обработки персональных данных во исполнение возложенных законодательством РФ на оператора функций, полномочий и обязанностей необходимо отметить, что под законодательством РФ понимается, в широком смысле слова, совокупность не только законов, но и иных нормативных правовых актов, принимаемых Президентом РФ, Правительством РФ, министерствами и ведомствами, уполномоченными на их принятие.

☑ Например, ст. 65 ТК РФ обязывает поступающего на работу гражданина предоставить работодателю следующие документы, содержащие персональные данные:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство обязательного пенсионного страхования;
- документы воинского учета — для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании и (или) о квалификации или наличии специальных знаний — при поступлении на работу, требующую специальных знаний или специальной подготовки;
- справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям, выданную в порядке и по форме, которые устанавливаются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, — при поступлении на работу, связанную с деятельностью, к осуществлению которой в соответствии с ТК РФ, иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию.

Обработка указанных сведений при выполнении работодателем возложенных на него трудовым законодательством обязанностей, в том числе связанных с их передачей в налоговые органы, внебюджетные фонды, подпадает под комментируемое основание и не требует согласия работника.

Такое основание обработки персональных данных, как обработка персональных данных, необходимая для исполнения полномочий соответствующих органов власти (а также внебюджетных фондов и

местного самоуправления) и функций организаций, участвующих в предоставлении государственных и муниципальных услуг, предусмотренных в соответствии с Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг, коррелируется с положениями ч. 4 ст. 7 этого закона, согласно которой органам, предоставляющим государственные и муниципальные услуги, и иным органам, участвующим в предоставлении государственных и муниципальных услуг, согласия получателя услуг как субъекта персональных данных не требуется.

Под данное основание подпадает также межведомственное взаимодействие, связанное с передачей персональных данных для предоставления государственных и муниципальных услуг.

В случае, когда для предоставления государственной или муниципальной услуги необходима обработка персональных данных лица, не являющегося заявителем, и если в соответствии с федеральным законом обработка таких персональных данных может осуществляться с согласия указанного лица, при обращении за получением государственной или муниципальной услуги заявитель дополнительно представляет документы, подтверждающие получение согласия указанного лица или его законного представителя на обработку персональных данных указанного лица (ч. 3 ст. 7 названного закона). Необходимо отметить, что в этом случае основание, допускающее обработку персональных данных без соответствующего согласия в рамках оказания государственных и муниципальных услуг, распространяется на субъекта персональных данных, которым помимо заявителя может быть и иное лицо.

В соответствии с п. 5 ч. 1 комментируемой статьи обработка персональных данных допускается для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

На основании пп. «д», «е», «ж» п. 20 Правил оказания услуг связи для целей телевизионного вещания и (или) радиовещания, утвержденных постановлением Правительства РФ от 22.12.2006 № 785, в договоре с абонентом в обязательном порядке должны быть указаны сведения о

нем: фамилия, имя, отчество, реквизиты документа, удостоверяющего личность, адрес установки пользовательского оборудования, вид информирования о состоянии счета или оказанных услугах.

> **Таким образом**, любая спутниковая компания (оператор) в рамках заключенного с субъектом персональных данных договора вправе осуществлять обработку персональных данных, в том числе фамилии, имени, отчества, реквизитов документа, удостоверяющего личность.

Следует заметить, что включение условий порядка обработки персональных данных сторон в гражданско-правовой договор не является обязательным и существенным условием договора. Так, факт заключения договора подразумевает согласие сторон на обработку персональных данных в целях исполнения договора.

Согласно ч. 16 ст. 155 ЖК РФ при привлечении наймодателем жилого помещения, управляющей организацией, иным юридическим лицом или индивидуальным предпринимателем представителей для осуществления расчетов с нанимателями жилых помещений государственного и муниципального жилищных фондов, собственниками жилых помещений и взимания платы за жилое помещение и коммунальные услуги согласие субъектов персональных данных на передачу персональных данных таким представителям не требуется.

> **Таким образом**, передача персональных данных граждан (собственников жилых помещений, нанимателей жилых помещений) в расчетный центр на основании заключенного договора, в целях оказания услуг по осуществлению расчетов, не требует согласия указанных лиц.

Обработка персональных данных, необходимая для осуществления прав и законных интересов оператора или третьих лиц, многогранна по своей правовой природе.

Так, в соответствии со ст. 382 ГК РФ право (требование), принадлежащее на основании обязательства кредитору, может быть передано им другому лицу по сделке (уступка требования).

> **Таким образом**, банки вправе при возникновении долгового портфеля переуступить право требования третьему лицу без соответствующего согласия заемщика.

В силу ст. 48 Закона РФ от 27.12.1991 № 2124-1 «О средствах массовой информации» редакция имеет право подать заявку в государственный орган, организацию, учреждение, орган общественного

объединения на аккредитацию при них своих журналистов, например на аккредитацию журналиста при Правительстве РФ. Для этих целей редакции необходимо представить в государственный орган, организацию, учреждение, орган общественного объединения определенные персональные данные журналиста, такие как фамилия, имя, отчество, место работы.

Порядок аккредитации иностранных журналистов регулируется также Правилами аккредитации и пребывания корреспондентов иностранных средств массовой информации на территории Российской Федерации, утвержденными постановлением Правительства РФ от 13.09.1994 № 1055.

Примером применения указанной нормы на практике может служить решение Верховного Суда Республики Коми от 28.11.2007 № 3-41-2007, оставленное в силе определением Судебной коллегии по гражданским делам Верховного Суда РФ от 27.02.2008 № 3-Г08-3, в котором указано, что аккредитация журналиста при органах, организациях и учреждениях непосредственно связана с его профессиональной деятельностью по поиску, получению и распространению информации, и поэтому в соответствии с п. 6 ч. 2 ст. 6 Закона о персональных данных (в редакции на момент рассмотрения спора) необходимый для реализации требований ст. 48 Закона РФ «О средствах массовой информации» минимум персональных данных журналиста может передаваться в орган, осуществляющий его аккредитацию, и без согласия этого журналиста.

Согласно п. 5 ст. 49 Закона РФ «О средствах массовой информации» существует запрет на распространение в СМИ сведений о личной жизни граждан, если от них или от их законных представителей не было получено на то согласие, за исключением случаев, когда это необходимо для защиты общественных интересов.

На основании постановления Пленума Верховного Суда РФ от 15.06.2010 № 16 «О практике применения судами закона Российской Федерации „О средствах массовой информации“» к общественным интересам следует относить не любой интерес, проявляемый аудиторией, а, например, потребность общества в обнаружении и раскрытии угрозы демократическому правовому государству и гражданскому обществу. Так, в этом постановлении Пленума Верховного Суда РФ указано, что судам необходимо проводить разграничение между сообщениями о фактах (даже весьма спорных), способных оказать положительное влияние на обсуждение в обществе вопросов, касающихся, например,

исполнения своих функций должностными лицами и общественными деятелями, и сообщением подробностей частной жизни лица, не занимающегося какой-либо публичной деятельностью.

В первом случае СМИ выполняют общественный долг в деле информирования граждан по вопросам, представляющим общественный интерес, во втором случае такой роли они не играют.

Статья 152 ГК РФ предусматривает возможность в судебном порядке требовать опровержения сведений, порочащих честь, достоинство и деловую репутацию гражданина.

Кроме этого, согласно п. 10 ст. 152 ГК РФ применение судебного порядка возможно в отношении случаев распространения любых не соответствующих действительности сведений о гражданине, если такой гражданин докажет несоответствие указанных сведений действительности.

Обезличивание персональных данных представляет собой действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Статья 97 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» предусматривает ведение статистического наблюдения в сфере здравоохранения. Официальная статистическая информация в сфере здравоохранения является общедоступной и размещается уполномоченным федеральным органом исполнительной власти в СМИ, в том числе в Интернете. Сведения, используемые для ведения вышеуказанной деятельности, не позволяют определить личность субъекта персональных данных, в связи с чем согласие субъекта на использование персональных данных для медицинской статистики не требуется.

Более того, обезличивание персональных данных предусмотрено пп. «з» п. 1 Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденного постановлением Правительства РФ от 21.03.2012 № 211. Данный подпункт обязывает проводить обезличивание в случаях, определенных нормативными правовыми актами. Требования и методы по обезличиванию персональных данных утверждены приказом Роскомнадзора от 05.09.2013 № 996.

Еще одним обязательным условием обработки персональных данных является обработка таких данных в случаях их обязательного опуб-

ликования или обязательного раскрытия в соответствии с федеральным законом.

☑ Так, например, в соответствии с положениями п. 3 ст. 66 Федерального закона от 10.01.2003 № 19-ФЗ «О выборах Президента Российской Федерации» в помещении для голосования либо непосредственно перед этим помещением участковая избирательная комиссия оборудует информационный стенд, на котором размещает информацию обо всех кандидатах, внесенных в избирательный бюллетень, включающую наряду с прочими сведениями биографические данные кандидатов в объеме, установленном ЦИК России, но не меньшем, чем объем биографических данных, внесенных в избирательный бюллетень.

Согласно постановлению ЦИК России от 25.05.2011 № 12/128-6 «О Комплексе мер по обеспечению информирования избирателей о зарегистрированных кандидатах на должность Президента Российской Федерации, о политических партиях, выдвинувших кандидатов» биографические данные о зарегистрированном кандидате включают следующие сведения:

- фамилию, имя, отчество;
- год рождения;
- наименование субъекта РФ, района, города, иного населенного пункта, где находится место жительства кандидата;
- основное место работы или службы, занимаемую должность (в случае отсутствия основного места работы или службы указывается род занятий). Если зарегистрированный кандидат является депутатом и осуществляет свои полномочия на непостоянной основе, вносятся сведения об этом с указанием наименования соответствующего представительного органа;
- информацию о неснятой и непогашенной судимости с указанием номера (номеров) и наименования (наименований) статьи (статей) УК РФ, на основании которой (которых) был осужден зарегистрированный кандидат, а также статьи (статей) УК РФ, принятого в соответствии с Основами уголовного законодательства Союза ССР и союзных республик, статьи (статей) закона иностранного государства, если зарегистрированный кандидат был осужден в соответствии с указанными законодательными актами за деяния, признаваемые преступлением действующим УК РФ, с указанием наименования соответствующего закона (в случае наличия судимости);

- если зарегистрированный кандидат выдвинут политической партией, указываются слова «выдвинут политической партией» с указанием используемого в избирательной кампании наименования соответствующей политической партии;
- если зарегистрированный кандидат сам выдвинул свою кандидатуру, указывается слово «самовыдвижение»;
- если кандидат в соответствии с п. 8 ст. 34 или пп. 1 п. 11 ст. 35 Федерального закона «О выборах Президента Российской Федерации» указал свою принадлежность к политической партии либо не более чем к одному иному общественному объединению, зарегистрированному не позднее чем за один год до дня голосования, указываются наименование данной политической партии, данного общественного объединения и статус зарегистрированного кандидата в данной политической партии, данном общественном объединении;
- иные сведения биографического характера: сведения о трудовом (творческом) пути, уровне образования, ученой степени, ученых и почетных званиях, наличии государственных наград, сведения о семейном положении, наличии детей.

☑ Согласно ст. 8 Федерального закона от 25.12.2008 № 273-ФЗ «О противодействии коррупции» сведения о доходах, об имуществе и обязательствах имущественного характера, предоставляемые лицами, замещающими определенные должности государственной или муниципальной службы, в государственных корпорациях, ПФР, ФСС России, ФФОМС, иных организациях, создаваемых Российской Федерацией на основании федеральных законов, размещаются в информационно-телекоммуникационной сети Интернет на официальных сайтах федеральных государственных органов, государственных органов субъектов РФ, органов местного самоуправления, Банка России, государственных корпораций, ПФР, ФСС России, ФФОМС, иных организаций, создаваемых Российской Федерацией на основании федеральных законов, и предоставляются для опубликования СМИ.

Порядок размещения сведений о доходах, расходах, об имуществе и обязательствах имущественного характера отдельных категорий лиц и членов их семей на официальных сайтах федеральных государственных органов, органов государственной власти субъектов РФ и организаций и предоставления этих сведений общероссийским СМИ для опубликования установлен Указом Президента РФ от 08.07.2013 № 613 «Вопросы противо-

действия коррупции». В частности, предоставляются следующие сведения:

- перечень объектов недвижимого имущества, принадлежащих служащему (работнику), его супруге (супругу) и несовершеннолетним детям на праве собственности или находящихся в их пользовании, с указанием вида, площади и страны расположения каждого из таких объектов;
- перечень транспортных средств с указанием вида и марки, принадлежащих на праве собственности служащему (работнику), его супруге (супругу) и несовершеннолетним детям;
- декларированный годовой доход служащего (работника), его супруги (супруга) и несовершеннолетних детей;
- сведения об источниках получения средств, за счет которых совершена сделка по приобретению земельного участка, другого объекта недвижимого имущества, транспортного средства, ценных бумаг, акций (долей участия, паев в уставных (складочных) капиталах организаций), если сумма сделки превышает общий доход служащего (работника) и его супруги (супруга) за три последних года, предшествующих совершению сделки.

Указанные персональные данные подлежат раскрытию и опубликованию без согласия лица, занимающего соответствующие должности, в силу закона. Иные персональные данные лица, замещающего соответствующие должности, и членов его семьи указывать запрещено.

2. В ч. 2 комментируемой статьи определено, что особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно ст. 10 и 11 Закона о персональных данных.

Подробнее об особенностях обработки специальных категорий персональных данных, а также биометрических персональных данных см. в комментариях к ст. 10 и 11 Закона о персональных данных.

3. Часть 3 комментируемой статьи вводит такое понятие, как поручение оператора, которое предусматривает возможность поручения обработки персональных данных оператором другому лицу при наличии следующих условий:

- согласия субъекта персональных данных на поручение обработки другому лицу;
- договора, в том числе государственного или муниципального контракта, между оператором и третьим лицом, одним из условий которого является обработка персональных данных субъекта,

либо соответствующего акта государственного или муниципального органа.

При этом в ч. 3 анализируемой статьи установлены требования к лицу, осуществляющему обработку персональных данных по поручению оператора. Указанное лицо обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных.

В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки. Кроме этого, в нем должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст. 19 комментируемого закона. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных. Эта обязанность возложена непосредственно на оператора. При отсутствии согласия субъекта персональных данных на поручение оператором обработки данных другому лицу оператор не вправе передавать данные субъекта. При несоблюдении существенных условий договора, содержащего поручение оператора, передача персональных данных субъектов для обработки третьим лицом также недопустима.

Так, Кировский областной суд в постановлении от 24.04.2012 № 7-А-98/2012 отметил, что в нарушение ч. 3 ст. 6 Закона о персональных данных управляющей компанией при поручении расчетно-информационному центру обработки персональных данных собственников и нанимателей обслуживаемых ею жилых помещений, а также членов их семей в рамках агентского договора не было получено согласие субъектов персональных данных на такую обработку. Агентский договор не содержит существенного условия, предусмотренного ч. 3 ст. 6 названного закона, а именно в нем отсутствуют требования к защите обрабатываемых персональных данных в соответствии со ст. 19 указанного закона.

Реализация агентской схемы в большинстве случаев, но не всегда, предполагает получение согласия. Так, например, согласно ст. 53 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», если оператор связи поручает обработку персональных данных абонента-гражданина третьему лицу в целях заключения и (или) исполнения договора об оказании

услуг связи, стороной которого является абонент-гражданин, и (или) в целях осуществления прав и законных интересов оператора связи или абонента-гражданина, согласие абонента-гражданина на это поручение, в том числе на передачу его персональных данных такому третьему лицу, обработку персональных данных таким третьим лицом в соответствии с поручением оператора связи, не требуется.

Необходимо отметить, что если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Статья 7. Конфиденциальность персональных данных
(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Комментируемая статья нормативно закрепляет общее правило защиты прав субъектов персональных данных, выраженное в установлении обязанности оператора и иного лица, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных. Данная статья обеспечивает общее правовое регулирование по отношению к специальным правилам, установленным иными федеральными законами.

Так, согласно трудовому законодательству работодатель не должен сообщать персональные данные работника в коммерческих целях без его письменного согласия.

Кроме этого, органы государственной власти в сфере охраны здоровья, в сфере социальной помощи, а также в сфере образования при ведении баз данных обязаны обеспечивать конфиденциальность содержащихся в них персональных данных в соответствии с законодательством РФ.

В отношении персональных данных, внесенных в личные дела государственных служащих, также устанавливается обязанность соблюдать конфиденциальность и обеспечивать их безопасность при обработке.

Медицинские организации, страховые медицинские организации и территориальные фонды определяют работников, допущенных к рабо-

те с данными персонифицированного учета сведений о медицинской помощи, оказанной застрахованным лицам, и обеспечивают их конфиденциальность в соответствии с установленными законодательством РФ требованиями по защите персональных данных.

Лицо, которому были уступлены права (требования), например по договору потребительского кредита (займа), обязано хранить персональные данные, обеспечивать конфиденциальность и безопасность указанных данных и нести ответственность за их разглашение.

Исключением, не требующим получения согласия субъекта на передачу его персональных данных третьим лицам, являются положения п. 1 ст. 64 Федерального закона «О связи», согласно которому «*операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, информацию о пользователях услугами связи и об оказанных им услугах связи, а также иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами*».

➥ **Таким образом**, законодательно закрепленное правило о конфиденциальности персональных данных имеет принципиальное значение для определения правовой основы при регулировании отношений субъекта персональных данных и оператора в различных сферах деятельности.

На практике, имеются случаи разглашения, раскрытия, распространения персональных данных без согласия субъекта персональных данных.

☑ Так, например, зачастую уполномоченным органом по защите прав субъектов персональных данных в ходе мониторинга информационно-телекоммуникационной сети Интернет устанавливаются факты предоставления интернет-ресурсами доступа неограниченному кругу лиц к персональным данным граждан без их соответствующего согласия.

В подобных случаях на сайтах отсутствует информация, подтверждающая наличие у администраторов доменных имен согласия граждан либо иных законных оснований на обработку их персональных данных. Таким образом, администраторами доменных имен допускаются нарушения требований конфиденциальности полученных персональных данных.

Статья 8. Общедоступные источники персональных данных

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные кни-

ги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных. *(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов. *(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

1. Комментируемая статья определяет цели, содержание, условия формирования общедоступного источника персональных данных. В то же время предусмотренная законодателем в ч. 1 комментируемой статьи возможность создания общедоступного источника в форме справочника, адресных книг может быть реализована с единственной целью, а именно информационного обеспечения. Как правило, указанные формы общедоступных источников могут содержать фамилию, имя, отчество, наименование должности, служебный абонентский номер, электронный адрес, рабочий адрес.

К общедоступным источникам персональных данных можно отнести:

- справочники, в том числе размещаемые в информационно-телекоммуникационной сети Интернет (справочники телефонные, адресные, предприятий);
- информационные базы данных государственных, муниципальных органов, общедоступность которых определена законом.

Условием, при котором сведения о субъекте персональных данных могут быть включены в общедоступные источники, является письменное согласие этого субъекта, если иное не предусмотрено федеральным законом.

Письменное согласие может быть дано на помещение персональных данных как в определенном общедоступном источнике, так и в нескольких. Однако письменное согласие на размещение персональных данных в определенном общедоступном источнике персональных данных не дает основания оператору размещать полученные в результате такого согласия персональные данные в других общедоступных источниках без соответствующего согласия.

2. Часть 2 комментируемой статьи устанавливает обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование удалить персональные данные из общедоступных источников. При этом указанное требование может ис-

ходить как от самого субъекта персональных данных, так и от суда или уполномоченного государственного органа.

Таким образом, законодатель закрепляет за субъектом, судом или уполномоченным органом право требовать удаления сведений о субъекте персональных данных. Данному праву корреспондирует обязанность оператора не допускать распространение в общедоступных источниках личной информации без согласия субъекта персональных данных.

Статья 9. Согласие субъекта персональных данных на обработку его персональных данных
(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)

1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2–11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.

3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в пунктах 2–11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона, возлагается на оператора.

4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

5. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

8. Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2–11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.

1. В комментируемой статье содержатся общие требования, предъявляемые к согласию субъекта персональных данных на обработку его персональных данных.

Часть 1 анализируемой статьи устанавливает условия принятия решения субъектом персональных данных о предоставлении своих персональных данных и дачи согласия на их обработку своей волей и в сво-

ем интересе. Следует отметить, что согласие должно быть конкретным, информированным и сознательным.

Конкретное согласие означает явно выраженное, предметное, определенное и неабстрактное согласие.

Под **информированным согласием** подразумевается уведомительное, сообщающее намерение о подтверждении того или иного события, факта, действия.

Под **сознательным согласием** имеется в виду осмысленное, обдуманное, разумное согласие.

☑ Так, например, субъект персональных данных (пользователь) при регистрации на интернет-сайте принимает условия пользования указанным интернет-сайтом (пользовательское соглашение) и тем самым берет на себя обязательства, установленные указанным соглашением, а также всеми дополнительными правилами (правила верификации), которые являются неотъемлемой частью пользовательского соглашения. Перед регистрацией на интернет-сайте пользователь обязан ознакомиться с вышеуказанным пользовательским соглашением.

➥ **Таким образом**, пользователь Интернета при регистрации на любом сайте самостоятельно принимает решение о предоставлении своих персональных данных и дает конкретное, информированное и сознательное согласие на их обработку своей волей и в своем интересе. То есть при использовании интернет-сервисов и согласно их политике в области конфиденциальности пользователь безоговорочно принимает условия данной политики в полном объеме в момент начала использования сервисов. В случае несогласия с каким-либо пунктом политики пользователь не имеет права использовать сервисы.

Зачастую в пользовательских соглашениях указано, что пользователь понимает и согласен с тем, что правообладатель вправе использовать информацию в сервисах, а также размещать комментарии пользователя, предоставленные и (или) добавленные им с помощью сервисов, в официальных группах социальных сетей и иных сообществах правообладателя в Интернете. Таким образом, факт размещения какой-либо информации (фамилии, имени, отчества, электронного адреса) на странице сайта предполагает согласие пользователя с условиями политики, а значит, согласие на размещение тех или иных комментариев на сервисе.

Также, например, субъект персональных данных при регистрации в качестве участника конкурса на интернет-сайтах принимает условия правил проведения конкурса, размещенных на сайте, и тем самым берет на себя обязательства, установленные указанными правилами.

При этом факт участия в конкурсе означает конкретное, информированное и сознательное согласие участника на обработку организатором конкурса предоставленных участником персональных данных, в том числе фамилии, имени, отчества, номера телефона, а также почтового адреса.

В практике Роскомнадзора имеются случаи, когда субъект персональных данных после участия в конкурсе обращается в Роскомнадзор с требованием удалить информацию о себе, размещенную в открытом доступе. Вместе с тем на первоначальном этапе участия в конкурсе участник дает согласие на обработку персональных данных своей волей и в своем интересе и осознает, что раскрытие такой информации об участниках конкурса содержится в положениях ряда нормативных правовых актов.

В ч. 1 комментируемой статьи установлено, что согласие на обработку персональных данных может быть дано не только лично субъектом персональных данных, но и его представителем. Исходя из этого, согласие на обработку персональных данных, предоставленное представителем субъекта персональных данных, должно быть подтверждено соответствующим документом о представительстве (доверенностью).

Следует отметить, что требования к оформлению доверенности установлены в ст. 185–186 ГК РФ.

2. Часть 2 комментируемой статьи предусматривает, что согласие на обработку персональных данных может быть отозвано субъектом персональных данных. Исходя из буквального толкования этой нормы следует, что право отзыва согласия закреплено только за субъектом персональных данных лично, а не за его представителем.

В ряде случаев в Роскомнадзор поступают обращения от субъектов персональных данных на предмет отсутствия уведомления оператора о факте прекращения обработки персональных данных. Между тем обязанность оператора персональных данных предоставлять субъекту персональных данных разъяснения юридических последствий отзыва согласия на обработку персональных данных действующим законодательством не предусмотрена.

Так, согласно ч. 5 ст. 21 Закона о персональных данных в случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить

прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 дней с даты поступления отзыва, если иное не предусмотрено законодательством о персональных данных.

Следует подчеркнуть, что нормами Закона о персональных данных не предусмотрена обязанность оператора уведомлять субъекта персональных данных о факте прекращения обработки персональных данных в связи с удовлетворением отзыва согласия субъекта на обработку его персональных данных.

В связи с этим Роскомнадзор поясняет субъекту персональных данных о его праве, в силу ст. 14 Закона о персональных данных, обратиться к оператору для получения информации, касающейся обработки его персональных данных.

Часть 2 комментируемой статьи устанавливает исключения из общего правила, предусматривающего отзыв согласия. В частности, данная норма ориентирует на то, что при отзыве субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных. Однако этим правом оператор может воспользоваться лишь при наличии оснований, указанных в п. 2–11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 Закона о персональных данных.

☑ Например, обработка персональных данных без согласия субъекта персональных данных допускается в случае, если она осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством РФ о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях. Поэтому отзыв работником своего согласия на обработку персональных данных не может являться основанием для прекращения обработки его персональных данных работодателем.

3. Согласно ч. 3 комментируемой статьи обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в п. 2–11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 Закона о персональных данных, возлагается на оператора. Именно оператору в

любом случае надлежит доказывать наличие законных оснований получения согласия субъектов персональных данных.

В силу положений ГПК РФ доказательствами по делу являются полученные в предусмотренном законом порядке сведения о фактах, на основе которых суд устанавливает наличие или отсутствие обстоятельств, обосновывающих требования и возражения сторон, а также иных обстоятельств, имеющих значение для правильного рассмотрения и разрешения дела. В случае спора оператор будет доказывать наличие полученного согласия субъекта в письменной форме или в любой иной позволяющей подтвердить факт его получения форме, либо будет доказывать наличие оснований, указанных в п. 2–11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 комментируемого закона, при которых согласия не требуется.

В контрольно-надзорной деятельности Роскомнадзора сформировалась практика, из которой следует, что запрос у операторов согласий субъектов персональных данных осуществляется вне рамок мероприятий, проводимых в соответствии с Федеральным законом от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (далее — Закон о защите прав юридических лиц и индивидуальных предпринимателей при осуществлении контроля). Таким образом, Роскомнадзор имеет право запрашивать у операторов данные согласия, не проводив документарную проверку.

4. Часть 4 комментируемой статьи регулирует форму и содержание согласия субъекта персональных данных. При этом в нее включена императивная норма об обработке персональных данных только с согласия в письменной форме субъекта персональных данных в случаях, предусмотренных федеральным законом.

Так, зачастую в Интернете размещают списки воспитанников, зачисленных в детский сад; учеников, зачисленных в школу или переведенных в следующий класс; студентов, принятых на первый курс, без получения письменного согласия их законных представителей.

Следует отметить, что равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Положениями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» определены два вида электронных подписей: простая электронная подпись и усиленная электронная подпись. При этом раз-

личаются усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись.

Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Усиленной неквалифицированной электронной подписью является электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

Усиленной квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам усиленной неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи».

Таким образом, использование указанных видов электронной подписи предполагает наличие согласия субъекта персональных данных на обработку его персональных данных.

☑ Так, например, регистрация пользователя Интернета на сайте, подтвержденная логином и паролем, означает согласие субъекта на обработку его персональных данных.

Кроме этого, ч. 4 комментируемой статьи содержит исчерпывающий перечень сведений, которые должны быть включены в письменное согласие субъекта персональных данных на обработку его персональных данных.

5. Частью 5 анализируемой статьи определено, что порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления

государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством РФ.

Согласно ст. 21.2 Федерального закона «Об организации предоставления государственных и муниципальных услуг» правила использования простых электронных подписей при оказании государственных и муниципальных услуг, в том числе правила создания и выдачи ключей простых электронных подписей, а также перечень органов и организаций, имеющих право на создание и выдачу ключей простых электронных подписей в целях оказания государственных и муниципальных услуг, устанавливаются Правительством РФ.

Так, постановлением Правительства РФ от 25.01.2013 № 33 утверждены Правила использования простой электронной подписи при оказании государственных и муниципальных услуг. Указанными правилами устанавливается порядок использования простой электронной подписи любыми лицами при обращении за получением государственных и муниципальных услуг в электронной форме. Следует отметить, что под простой электронной подписью понимается электронная подпись, которая посредством использования ключа простой электронной подписи подтверждает факт формирования электронной подписи конкретным заявителем.

Операторы выдачи ключа, а также многофункциональные центры предоставления государственных и муниципальных услуг обязаны обеспечить заявителю подачу заявления при личном приеме. При этом обязательным условием обработки персональных данных при подаче заявления на выдачу ключа является согласие заявителя на обработку его персональных данных, указываемых в заявлении, в соответствии с Законом о персональных данных.

6. Часть 6 комментируемой статьи устанавливает, что согласие на обработку персональных данных недееспособных субъектов персональных данных дается их законными представителями.

Согласно п. 1 ст. 29 ГК РФ гражданин, который вследствие психического расстройства не может понимать значения своих действий или руководить ими, может быть признан судом недееспособным в порядке, установленном гражданским процессуальным законодательством. Над ним устанавливается опека.

В соответствии с п. 2 ст. 32 ГК РФ опекуны являются представителями подопечных в силу закона и совершают от их имени и в их интересах все необходимые сделки.

Следует отметить, что опекуны выступают в защиту прав и интересов своих подопечных в отношениях с любыми лицами, в том числе в судах, без специального полномочия.

Согласно ст. 15 Федерального закона от 24.04.2008 № 48-ФЗ «Об опеке и попечительстве» при осуществлении своих прав и обязанностей опекуны имеют право на оказание им содействия в предоставлении медицинской, психологической, педагогической, юридической, социальной помощи.

7. На основании ч. 7 комментируемой статьи в случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни. К форме и содержанию такого согласия применяются общие правила, установленные для согласия субъекта персональных данных.

8. Часть 8 анализируемой статьи предусматривает, что персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в п. 2–11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 комментируемого закона. Таким образом, на лицо, не являющееся субъектом персональных данных, возложена обязанность предоставить оператору законные основания своего обращения.

☑ Например, нотариусом, как оператором, могут быть получены от обратившегося к нему лица персональные данные, касающиеся других лиц (поверенных, других наследников), если это необходимо для выполнения его полномочий по совершению нотариального действия.

Статья 10. Специальные категории персональных данных

1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка указанных в части 1 настоящей статьи специальных категорий персональных данных допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные сделаны общедоступными субъектом персональных данных; *(п. 2 в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

2.1) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии; *(п. 2.1 введен Федеральным законом от 25.11.2009 № 266-ФЗ)*

2.2) обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года № 8-ФЗ «О Всероссийской переписи населения»; *(п. 2.2 введен Федеральным законом от 27.07.2010 № 204-ФЗ)*

2.3) обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации; *(п. 2.3 введен Федеральным законом от 25.07.2011 № 261-ФЗ, в ред. Федерального закона от 21.07.2014 № 216-ФЗ)*

3) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно; *(п. 3 в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

4) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

5) обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

6) обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия; *(п. 6 в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

7) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации; *(п. 7 в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

7.1) обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора; *(п. 7.1 введен Федеральным законом от 23.07.2013 № 205-ФЗ)*

8) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством; *(п. 8 в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

9) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства

детей, оставшихся без попечения родителей, на воспитание в семьи граждан; *(п. 9 введен Федеральным законом от 25.07.2011 № 261-ФЗ)*

10) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации. *(п. 10 введен Федеральным законом от 04.06.2014 № 142-ФЗ)*

3. Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

4. Обработка специальных категорий персональных данных, осуществлявшаяся в случаях, предусмотренных частями 2 и 3 настоящей статьи, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом. *(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

1. Комментируемая статья устанавливает исчерпывающий перечень специальных категорий персональных данных, а также определяет правило обработки этих категорий данных. Общее правило обработки специальных категорий персональных данных сформулировано в виде прямого запрета осуществлять любую обработку данных.

В анализируемой статье не раскрывается понятие «специальные категории персональных данных», но представлен исчерпывающий перечень определенных сведений, которые помимо иных отнесены к специальным категориям. При этом именно в отношении указанного перечня сформулирован запрет на обработку данных, остальные данные подлежат обработке в соответствии с общими правилами.

К специальным категориям персональных данных, любая обработка которых запрещена, законодатель относит сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни субъекта персональных данных.

Следует заметить, что к рассматриваемым категориям законодатель не отнес сведения о социальной, языковой принадлежности, которые указаны в качестве признаков возможного неравенства, ограничения прав и свобод человека и гражданина в ч. 2 ст. 19 Конституции РФ. В связи с этим запрет на обработку указанных данных не применяется.

Сведения о расовой и национальной принадлежности рассматриваются как данные о принадлежности лица к каким-либо исторически сложившимся культурно-этническим общностям людей (нации, народности, этнические группы).

Согласно ст. 19 Конституции РФ гарантируется равенство прав и свобод человека и гражданина независимо от пола, расы, национально-

сти, языка, происхождения, имущественного и должностного положения, места жительства, отношения к религии, убеждений, принадлежности к общественным объединениям, а также других обстоятельств. Запрещаются любые формы ограничения прав граждан по признакам социальной, расовой, национальной, языковой или религиозной принадлежности. Можно сделать вывод, что данная норма исключает условия неравенства в подходах к обработке персональных данных с учетом вышеуказанных критериев.

Сведения о политических взглядах, религиозных или философских убеждениях представляют собой данные о принадлежности лица к каким-то группам, связанным общностью убеждений, интересов, взглядов, предпочтений. При этом такая общность субъектов данных должна быть основана именно на политических, религиозных или философских учениях. Таким образом, профессиональная принадлежность или сведения о спортивных предпочтениях лица не относятся к запрещенным для обработки специальным категориям персональных данных.

Сведения о состоянии физического, психического благополучия человека или сведения об изменении организма, возникающие в связи с воздействием патогенных и (или) физиологических факторов и требующие оказания медицинской помощи, а также сведения о сексуальной ориентации, парафилии относятся к категории состояния здоровья, интимной жизни субъекта персональных данных.

2. В ч. 2 комментируемой статьи установлены основания, при которых обработка специальных категорий персональных данных может осуществляться, несмотря на общее положение о запрете обрабатывать эти данные. Перечень таких оснований является исчерпывающим. Рассмотрим их по порядку.

Первое основание — наличие письменного согласия субъекта персональных данных на обработку специальных категорий данных. При этом требования к содержанию письменного согласия на обработку персональных данных установлены в ст. 9 комментируемого закона (*см. комментарий к ст. 9 Закона о персональных данных*). В таком согласии субъекта следует указать категорию специальных данных, перечень которых приводится в ч. 1 комментируемой статьи. В любом случае согласие должно содержать наименования конкретного перечня данных в рамках специальной категории, право на обработку которых предоставлено оператору персональных данных.

Второе основание — осуществление обработки общедоступных персональных данных, при условии, что они сделаны общедоступными самим субъектом персональных данных.

При рассмотрении данного основания следует различать понятия «общедоступный источник персональных данных» и «персональные данные, сделанные общедоступными субъектом персональных данных». Так, общедоступный источник данных представляет собой объект, где располагаются общедоступные данные (в том числе справочники, адресные книги). Названные источники не являются единственным местом размещения данных для неограниченного круга лиц (*см. комментарий к ст. 8 Закона о персональных данных*).

При этом в комментируемой статье законодатель определяет не место размещения информации, а действие субъекта персональных данных, которое должно выражаться либо в просьбе кому-либо разместить личные данные в месте, доступном для неограниченного круга лиц, либо в самостоятельном размещении этой информации. То есть действие субъекта персональных данных должно быть направлено на придание информации о себе общедоступности.

☑ Типичным примером случая, когда персональные данные сделаны общедоступными самим субъектом персональных данных, является размещение данных о себе на различных сайтах в Интернете, в том числе социальных сетях. Так, в случае если субъектом персональных данных не были сделаны соответствующие настройки приватности и доступ к личной информации разрешен для неограниченного круга лиц, такая информация будет являться общедоступной.

В современном мире скорость распространения информации является молниеносной, и однажды размещенные данные в публичном доступе могут «разойтись» в сети огромным количеством копий на различных сайтах.

При этом если размещение субъектом персональных данных в форме открытых данных в будущем повлечет за собой нарушение его прав, то удаление такой информации из Интернета может быть произведено только по решению суда.

Именно поэтому представители уполномоченного органа по защите прав субъектов персональных данных неоднократно на многих конференциях, посвященных защите персональных данных, призывают граждан к бережному отношению к своим персональным данным, к сознательному размещению их в Интернете[1].

---

[1] Онлайн-конференция «День защиты персональных данных детей» // <http://pd.rkn.gov.ru/multimedia/news4209/>.

Упрощенная процедура удаления персональных данных, т.е. на основании требования уполномоченного органа по защите прав субъектов персональных данных, будет возможна только в случае, если размещение персональных данных в форме открытых данных осуществлялось с нарушением комментируемого закона, например, третьими лицами без согласия субъекта персональных данных.

Третье основание — необходимость обработки персональных данных в связи с реализацией международных договоров РФ о реадмиссии.

> **Реадмиссия** означает передачу запрашивающим государством и принятие запрашиваемым государством лиц (граждан запрашиваемого государства, граждан третьих государств или лиц без гражданства), чей въезд, пребывание или проживание в запрашивающем государстве признаны незаконными в соответствии с положениями международного соглашения о реадмиссии (ст. 1 Соглашения между Российской Федерацией и Европейским сообществом о реадмиссии от 25 мая 2006 г.).

Следует заметить, что вопросы реадмиссии не были актуальны для России вплоть до 2000-х гг. Так, задача заключения соглашений о реадмиссии была впервые продекларирована Концепцией регулирования миграционных процессов в Российской Федерации, одобренной распоряжением Правительства РФ от 01.03.2003 № 256-р[1]. В настоящее время Российская Федерация является участницей либо проводит переговоры о подписании международных соглашений о реадмиссии, в том числе с Европейским союзом, Арменией, Узбекистаном, Украиной, Вьетнамом, Норвегией, Данией, Исландией, Швейцарией, Казахстаном, Киргизией, Турцией, Украиной, Республикой Молдова, Азербайджаном и Таджикистаном. Ведутся переговоры с Китаем, Индией, КНДР, Пакистаном, Ливаном, Шри-Ланкой и Филиппинами.

Соглашения о реадмиссии содержат перечень документов и сведений, необходимых для реадмиссии. В частности, в приложении № 2 к Соглашению между Российской Федерацией и Европейским сообществом о реадмиссии приводится список документов, предоставление которых считается доказательством наличия гражданства. Такими документами могут быть:

- паспорта любого рода Российской Федерации и государств — членов Соглашения (например, внутренние паспорта, общегражданские заграничные паспорта, национальные паспорта,

[1] Утратило силу.

дипломатические паспорта, служебные паспорта и документы, заменяющие паспорта, в том числе детские паспорта);
- свидетельства на возвращение в Российскую Федерацию;
- национальные удостоверения личности государств — членов Европейского союза;
- свидетельства о гражданстве или другие официальные документы, в которых упоминается или указывается гражданство (например, свидетельство о рождении);
- служебные книжки и удостоверения личности военнослужащих;
- регистрационные книжки моряков, капитанские служебные карточки и паспорта моряков.

Списки таких документов в каждом международном соглашении может быть различными. Тем не менее все указанные документы содержат персональные данные субъекта, подлежащего реадмиссии, и могут включать в себя в том числе специальные категории данных, например, сведения о гражданстве, национальности (см. Соглашение между Правительством Российской Федерации и Правительством Королевства Норвегия о реадмиссии от 8 июня 2007 г.).

Вместе с тем получаемые и предоставляемые персональные данные подлежат обработке в соответствии с целями, предусмотренными в данных международных соглашениях, т.е. могут быть использованы только для осуществления действий, указанных в соглашениях о реадмиссии.

Четвертое основание — осуществление обработки персональных данных в соответствии с Федеральным законом от 25.01.2002 № 8-ФЗ «О Всероссийской переписи населения».

Всероссийская перепись населения представляет собой сбор сведений о лицах, находящихся на определенную дату на территории Российской Федерации, и проводится на всей территории Российской Федерации в целях формирования официальной статистической информации о демографических, экономических и социальных процессах.

Федеральным законом «О Всероссийской переписи населения» четко определена цель сбора персональных данных при переписи населения — формирование официальной статистической информации.

Под **статистической информацией** можно понимать любую информацию, которая в количественном и качественном измерении характеризует массовые явления и процессы, имеющие место в экономической, социальной и других сферах общественной жизни.

Таким образом, собранные данные используются исключительно для формирования обезличенной статистической информации.

При этом в рамках проведения Всероссийской переписи населения подлежат сбору следующие персональные данные: пол; возраст (дата рождения); гражданство; национальная принадлежность; владение языками; образование; состояние в браке; количество детей; место рождения; место жительства и (или) место пребывания; жилищные условия; источники средств к существованию; занятость либо безработица; миграция.

О лицах, временно находящихся на территории Российской Федерации, но постоянно проживающих за пределами Российской Федерации, осуществляется сбор сведений, касающихся цели их приезда в Российскую Федерацию.

Пятое основание — осуществление обработки персональных данных в соответствии с законодательством РФ, регулирующим иные сферы общественных отношений. При этом законодатель четко определил, какие именно сферы правоотношений могут относиться к исключительным основаниям обработки специальных категорий данных.

В рассматриваемом случае необходимо руководствоваться предоставленным соответствующим законодательством правом оператору персональных данных обрабатывать персональные данные. Так, в комментируемой части статьи указаны:

- законодательство о гражданстве РФ;
- законодательство об обязательных видах страхования, страховое законодательство;
- законодательство об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительное законодательство РФ;
- законодательство о государственной социальной помощи, трудовое законодательство, пенсионное законодательство.

Шестое основание — осуществление оператором персональных данных определенной деятельности. К такой деятельности относятся осуществление прокурорского надзора органами прокуратуры, осуществление правосудия.

Седьмое основание — осуществление обработки специальных категорий данных определенными категориями операторов персональных данных

и цели такой обработки. К указанным категориям операторов были отнесены:

- государственные органы, муниципальные органы или организации в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;
- общественные объединения или религиозные организации для достижения законных целей, предусмотренных их учредительными документами, которые вправе обрабатывать только данные своих членов;
- лица, профессионально занимающиеся медицинской деятельностью, в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг.

Восьмое основание — необходимость обработки персональных данных в целях защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц.

3. Часть 3 комментируемой статьи устанавливает правила обработки данных о судимости лица. При этом размещение рассматриваемой нормы в конструкции статьи, регламентирующей порядок обработки специальных персональных данных, свидетельствует об отнесении законодателем данных о судимости к специальным категориям данных. Вместе с тем сведения о судимости лица представляют собой категорию социальной принадлежности, в которую входят в том числе сведения о профессии (сотрудники правоохранительных органов, судьи и проч.), ином социальном статусе лиц (малообеспеченные семьи, безработные).

> **Таким образом**, несмотря на то что категория персональных данных, касающаяся социальной принадлежности, не указана в ч. 1 ст. 10 Закона о персональных данных, запрет на обработку будет по умолчанию распространяться на такие данные.

Следует учитывать, что согласно ст. 86 УК РФ лицо, осужденное за совершение преступления, считается судимым со дня вступления обвинительного приговора суда в законную силу до момента погашения или снятия судимости.

В постановлении Конституционного Суда РФ от 19.03.2003 № 3-П «По делу о проверке конституционности положений Уголовного кодекса Российской Федерации, регламентирующих правовые последствия судимости лица, неоднократности и рецидива преступлений, а также пунктов 1–8 Постановления Государственной Думы от 26 мая 2000 года

„Об объявлении амнистии в связи с 55-летием Победы в Великой Отечественной войне 1941–1945 годов“ в связи с запросом Останкинского межмуниципального (районного) суда города Москвы и жалобами ряда граждан» судимость трактуется как правовое состояние лица, обусловленное фактом осуждения и назначения ему по приговору суда наказания за совершенное преступление.

➥ **Таким образом**, простое сообщение о наличии (отсутствии) судимости лица без дополнительной информации о факте осуждения и назначения субъекту персональных данных приговором суда наказания не может характеризоваться в качестве специальных персональных данных. Сведения о судимости представляют собой совокупность данных, содержащих определенную или определяемую информацию о лице в качестве осужденного, т.е. подтвержденную сведениями о вступившем в законную силу обвинительном приговоре суда.

К сведениям о судимости могут быть отнесены данные о когда-либо имевшихся судимостях с указанием номера и наименования статьи УК РФ, на основании которой был осужден субъект персональных данных, даты приговора, наименования суда, вынесшего приговор, даты вступления данного приговора в законную силу.

Согласно ч. 3 анализируемой статьи обработка данных о судимости может осуществляться государственными и муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством РФ. Следовательно, обработка данных о судимости для органов власти всегда будет ограничена полномочиями, функциями и обязанностями соответствующего государственного и муниципального органа, и нарушение комментируемой части будет свидетельствовать не только о нарушении законодательства о персональных данных, но также и о превышении объема полномочий соответствующего органа власти.

☑ Например, согласно ст. 16 Федерального закона «О государственной гражданской службе» одним из ограничений, связанных с гражданской службой, является наличие неснятой или непогашенной в установленном федеральным законом порядке судимости. При этом в соответствии с п. 16 ч. 1 ст. 44 указанного закона кадровая работа включает в себя организацию проверки достоверности представляемых гражданином персональных данных и иных сведений при поступлении на гражданскую службу.

Следовательно, любой орган, профессиональная служебная деятельность в котором является государственной гражданской службой, вправе обрабатывать сведения о судимости исключительно кандидатов на должности гражданской службы. Обработка этих данных осуществляется посредством получения сведений от кандидатов на должности государственной гражданской службы с последующим направлением в компетентные учреждения запросов с просьбой предоставить сведения о наличии (отсутствии) судимости для подтверждения имеющейся у соответствующего органа власти информации.

☑ В соответствии с п. 39 ч. 1 ст. 12 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции» полиция обязана представлять по межведомственным запросам органов государственной власти, органов местного самоуправления, предоставляющих государственные или муниципальные услуги, сведения о наличии у лица непогашенной или неснятой судимости, если для предоставления государственной или муниципальной услуги предусмотрено представление таких сведений или документа, содержащего такие сведения, в указанные государственные органы или органы местного самоуправления.

Помимо государственных и муниципальных органов, обработка данных о судимости может осуществляться иными лицами в случаях и в порядке, установленными федеральными законами.

☑ Так, в ст. 23 Федерального закона от 29.07.1998 № 135-ФЗ «Об оценочной деятельности в Российской Федерации» указано, что для включения некоммерческой организации в единый государственный реестр саморегулируемых организаций оценщиков необходимо представить заверенные некоммерческой организацией копии справок об отсутствии у ее членов неснятой или непогашенной судимости за преступления в сфере экономики, а также за преступления средней тяжести, тяжкие и особо тяжкие преступления. Таким образом, саморегулируемые организации оценщиков вправе осуществлять обработку сведений о судимости членов саморегулируемой организации.

4. Часть 4 комментируемой статьи устанавливает основание для прекращения обработки специальных категорий персональных данных. Так, оператор персональных данных обязан прекратить обработку специальных категорий персональных данных в случае устранения причин, вследствие которых ранее данная обработка осуществлялась.

Основанием для прекращения такой обработки являются следующие случаи:

- отзыв субъектом персональных данных письменного согласия, данного им ранее, на обработку своих персональных данных;
- окончание Всероссийской переписи населения и подведение ее итогов;
- отпадение угрозы инфекционных заболеваний, массовых отравлений и поражений или иных обстоятельств, требующих защиты жизни, жизненно важных интересов субъекта персональных данных или иных лиц;
- прекращение членства субъекта персональных данных в религиозной организации или общественном объединении, ликвидация религиозной организации, общественного объединения;
- исключение полномочий соответствующего органа государственной власти или местного самоуправления по устройству детей, оставшихся без попечения родителей, на воспитание в семьи граждан;
- прекращение профессиональной медицинской деятельности или изменение цели обработки данных;
- исключение из федерального закона нормы, установившей право или обязанность какого-либо лица обрабатывать персональные данные о судимости иных лиц;
- внесение изменений в законодательство РФ в части исключения положения о наделении органа или органа местного самоуправления полномочием по обработке персональных данных о судимости;
- расторжение договора о реадмиссии с определенным иностранным государством.

Статья 11. Биометрические персональные данные

(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о

безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации. *(в ред. Федерального закона от 04.06.2014 № 142-ФЗ)*

1. Часть 1 комментируемой статьи определяет понятие биометрических персональных данных, а также устанавливает общее правило их обработки.

Под **биометрическими персональными данными** понимаются сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

Несмотря на то что законодатель закрепил понятие биометрических данных в комментируемом законе, до настоящего времени отсутствует единообразное толкование данного термина, а соответственно, и понимание, какие данные о человеке могут являться его биометрией. Так, в разъяснениях Роскомнадзора «О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки» изображение лица человека на таком материальном носителе, как фотография или видео, расценено в качестве биометрических данных, позволяющих установить личность субъекта персональных данных. Представляется, что особенность данной категории персональных данных выражена в высокой степени точности идентификации человека среди множества иных определяемых лиц ввиду уникальности его физиологических характеристик.

Вместе с тем фотография или видеоизображение человека, который является близнецом или чье внешнее сходство с иным человеком очевидно, а также в случаях осуществления пластических операций, при визуальной оценке рассматриваемых материальных носителей не позволит произвести достоверную идентификацию субъекта.

В связи с этим биометрическая информация должна характеризоваться уникальными физиологическими и биологическими данными, которые свойственны исключительно для одного субъекта персональных данных, носят более или менее неизменный характер и могут быть отражены на материальном носителе в виде цифровой, графической и иной кодовой информации. Такому пониманию биометрии соответствуют, например, папиллярные узоры, рисунок радужной оболочки глаза и др.

Законодатель четко определил, что отнесение сведений персонального характера к биометрическим персональным данным следует рассматривать с точки зрения возможности установления, подтверждения личности конкретного лица. Следовательно, биометрическими персональными данными могут являться те сведения, которые используются для идентификации, подтверждения личности по физиологическим параметрам, что предполагает применение особых методов установления личности, биометрических методов аутентификации личности.

> **Таким образом**, законодательное понятие биометрических данных предполагает не только наличие определенных сведений, содержащих информацию о физиологических и биологических особенностях человека, но также использование биометрических методов идентификации личности.

Существующие технологии биометрической идентификации позволяют установить личность как по уникальным физиологическим характеристикам человека, посредством распознавания по отпечатку пальца, по сетчатке глаза, по радужной оболочке глаза, по форме и термограмме лица, по ДНК, так и по изменяющейся поведенческой характеристике человека, путем идентификации по почерку и по голосу[1].

При этом биометрия как метод идентификации человека через его физиологические или биологические характеристики основан на сопоставлении данных идентифицируемого объекта — субъекта персональных данных и биометрического эталона, т.е. биометрических данных. Такое сопоставление невозможно без записи и сохранения биометрической информации, без ее документирования. Более того, документированная информация о физиологических и биологических особенностях человека должна быть достаточной для производства идентификации личности.

Следует заметить, что понятия «видеозапись» и «фотография», рассматриваемые в разъяснениях Роскомнадзора «О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки», представляют собой исключительно материальный носитель информации, при этом данная информация не является биометрической по своей сути, поскольку не отражает индивидуальных параметров, таких как термограмма лица, рисунок радужной оболочки глаза, папиллярных узоров, позволяющих установить личность.

---

[1] См.: *Двоеносова Г., Двоеносова М.* Биометрия как наука, метод и способ документирования // Управление персоналом. 2009. № 11.

☑ Так, например, биометрический паспорт представляет собой документ, содержащий информацию об индивидуальных характеристиках человека, выраженную в цифровом формате и записанную в электронном виде на специальное устройство. Фактически биометрический паспорт отличается от обычного тем, что в него встроен специальный чип, который содержит трехмерную фотографию его владельца. Таким образом, фотография может относиться к категории биометрических персональных данных в случае, если идентификация личности осуществляется посредством биометрического метода распознавания изображения лица по трехмерному 3*D*-фото.

Автоматическое распознавание только по двухмерной фотографии связано с большой вероятностью ошибки. Двухмерная фотография представляет собой распределение яркости, поэтому она может изменяться под воздействием различных факторов, например, освещения, ракурса, расстояния до лица, макияжа, наличия очков и т.п. В связи с такой неустойчивостью к внешним воздействиям при автоматическом сравнении по двухмерной фотографии вероятность ошибки идентификации крайне высока.

Поэтому при применении технологии биометрической идентификации личности используется стандарт трехмерной фотографии, совмещающей в себе обычную двухмерную фотографию и высокоточную цифровую копию поверхности лица.

Трехмерные геометрические параметры лица напрямую связаны с антропометрическими характеристиками, которые являются уникальными для каждого человека, и могут служить более надежными признаками для составления алгоритмов распознавания, чем привычные двухмерные изображения. Вместе с тем традиционные двухмерные фотографии лучше интерпретируются человеком — оператором, призванным «вручную» перепроверить компьютер и принять окончательное решение.

К материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных российским законодательством также предъявляются определенные требования (см. постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»).

К понятию биометрических данных не могут быть отнесены данные об инвалидности или наличии конкретного заболевания, несмотря на то, что такие сведения характеризуют особенности, вызванные наличием каких-то биологических отклонений. Подобные сведения являются специализированной категорией данных о состоянии здоровья. При этом отдельные приметы внешности (родинки, шрамы и проч.) не могут являться ни биометрическими данными субъекта персональных данных, ни специальными категориями персональных данных.

Помимо понятия биометрических персональных данных, комментируемая часть статьи устанавливает специальное условие обработки биометрических персональных данных. Таким условием является обязательное наличие письменного согласия субъекта персональных данных на обработку биометрических персональных данных.

2. Часть 2 анализируемой статьи устанавливает исключения из общего правила обработки персональных данных, а именно условия, при которых обработка биометрических персональных данных может осуществляться без письменного согласия субъекта персональных данных.

Определенные законодателем исключительные случаи обработки биометрии можно условно разделить на три категории:

1) в связи с осуществлением правосудия и исполнением судебных актов;
2) в связи с реализацией международных договоров РФ;
3) в случаях, предусмотренных законодательством РФ.

При этом в комментируемой части указан исчерпывающий перечень законодательств, которыми могут устанавливаться случаи обработки биометрических персональных данных. Так, законодательством РФ об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством РФ, законодательством РФ о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве РФ определяются случаи обработки биометрических персональных, при которых согласия субъекта персональных данных на такую обработку не требуется.

В соответствии со ст. 8 Федерального закона от 28.03.1998 № 53-ФЗ «О воинской обязанности и военной службе» при осуществлении первичного воинского учета органы местного самоуправления поселений и органы местного самоуправления городских округов обязаны осу-

ществлять сбор, хранение и обработку сведений, содержащихся в документах первичного воинского учета, в порядке, установленном законодательством РФ в области персональных данных и Положением о воинском учете, утвержденным постановлением Правительства РФ от 27.11.2006 № 719. Пункт 19 Положения о воинском учете указывает на обязательность содержания в документах следующих сведений о гражданах: фамилии, имени и отчества, даты рождения, места жительства, семейного положения, образования, места работы, годности к военной службе по состоянию здоровья, основных антропометрических данных и др.

Согласно ст. 13 Федерального закона от 03.04.1995 № 40-ФЗ «О Федеральной службе безопасности» органы федеральной службы безопасности имеют в том числе следующие права:

- проверять у лиц документы, удостоверяющие их личность, осуществлять их личный досмотр и досмотр находящихся при них вещей, если имеются достаточные основания подозревать их в совершении административных правонарушений или преступлений, производство либо дознание или предварительное следствие по которым отнесено законодательством РФ к ведению органов федеральной службы безопасности, а также досмотр транспортных средств и находящихся в них грузов при подозрении, что они используются в целях совершения указанных административных правонарушений или преступлений. Перечень должностных лиц органов федеральной службы безопасности, уполномоченных на осуществление личного досмотра, досмотра вещей, транспортных средств и находящихся в них грузов, определяется руководителем федерального органа исполнительной власти в области обеспечения безопасности;
- осуществлять административное задержание лиц, совершивших правонарушения, связанные с попытками проникновения и проникновением на специально охраняемые территории особорежимных объектов, закрытых административно-территориальных образований и иных охраняемых объектов, а также проверять у этих лиц документы, удостоверяющие их личность, получать от них объяснения, осуществлять их личный досмотр, досмотр и изъятие их вещей и документов;
- получать биологический материал и осуществлять обработку геномной информации по преступлениям, дознание и предварительное следствие по которым отнесено законодательством РФ к ведению органов федеральной службы безопасности.

На основании ст. 6 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» оперативно-розыскные мероприятия осуществляются, в частности, в форме сбора образцов для сравнительного исследования и отождествления личности. Эти формы проведения мероприятий непосредственно связаны с получением биометрических персональных данных.

В соответствии со ст. 47.1, 188 УИК РФ получение биометрических данных от субъектов прямо предусмотрено в рамках специального порядка исполнения наказания в виде ограничения свободы и порядка осуществления контроля за поведением условно осужденных. Необходимо отметить, что при постановке на учет осужденный подлежит дактилоскопической регистрации.

Статья 12. Трансграничная передача персональных данных

(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)

1. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

2. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень 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. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.

3. Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами Российской Федерации;

3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

4) исполнения договора, стороной которого является субъект персональных данных;

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

1. Часть 1 комментируемой статьи регламентирует отношения по трансграничной передаче персональных данных с территории Российской Федерации на территорию иностранных государств и устанавливает основные требования и правила такой передачи.

В то же время нормы российского законодательства о передаче персональных данных на территорию иностранных государств следует рассматривать в контексте обязательств, взятых на себя Российской Федерацией при ратификации Конвенции 1981 года. Так, в ее ст. 12 изложены принципы национального законодательного регулирования процесса трансграничных потоков данных.

Согласно п. 2 ст. 12 Конвенции 1981 года российская сторона не должна запрещать или требовать специальных разрешений от операторов в случаях, когда передача данных осуществляется на территорию другой страны — участницы этой конвенции, если их единственной целью является защита частной жизни. То есть в иных целях, список которых может быть достаточно широким, такой запрет или ограничение имеет право на существование.

Кроме этого, в п. 3 ст. 12 Конвенции 1981 года также сделана оговорка, согласно которой стороны вправе отступить от общего правила недопустимости запрета или ограничения трансграничных потоков данных в случаях, когда речь идет об определенных категориях данных, требующих специальных правил защиты, либо об автоматизированных файлах, имеющих особенные характеристики такого файла, или персональных данных, которые на этом файле содержатся.

При этом в Конвенции 1981 года не конкретизированы категории данных и особенности характеристик файлов и данных, позволяющие ограничить их потоки, что также представляет широкий простор

странам на пути принятия решения в пользу запрета или ограничения трансграничных потоков существенных объемов личной информации.

Еще одним исключением из общего правила «недопустимости запрета трансграничной передачи данных» является возможность установления запрета на трансграничную передачу данных на территорию страны — участницы Конвенции 1981 года в случае, если такой трансфер данных позволит обойти российское законодательство о персональных данных, и передать их на территорию третьего государства — не участника данной конвенции.

> **Таким образом**, свободная передача персональных данных на территорию стран — участниц Конвенции 1981 года обусловлена не только способностью таких стран обеспечить гражданам защиту их личной информации не ниже уровня, который гарантирован российским законодательством, но также соблюдением принципа добросовестного выполнения международных обязательств.

Российский законодатель в комментируемой статье не предъявляет дополнительных требований к порядку трансграничной передачи данных в отношении стран — участниц Конвенции 1981 года. Более того, оператор персональных данных может руководствоваться общими нормами российского законодательства о персональных данных не только в случае передачи данных на территорию стран, которые являются участницами этой конвенции, но также стран, которые не присоединились к ней, но признаются в Российской Федерации в качестве государств, обеспечивающих адекватную защиту персональных данных.

Оператор персональных данных может осуществлять трансграничную передачу данных на территорию указанных государств в аналогичном режиме, как если бы передача производилась на территории Российской Федерации.

Подходы Европейского союза к передаче персональных данных в страны, не присоединившиеся к Конвенции 1981 года, и критерии оценки адекватности защиты персональных данных, изложены в документе рабочей группы по защите прав частных лиц применительно к обработке персональных данных, принятом 24 июля 1998 г.

Согласно данному документу анализ адекватной защиты должен состоять из двух основных элементов: оценки содержания применяемых иностранным государством правил и средств для их эффективного применения.

Таким образом, оцениваемое иностранное государство должно иметь специальное законодательство, содержащее положения, необходимые для соответствующего уровня защиты физических лиц.

Реализация законодательных норм должна быть гарантирована специальными и упрощенными средствами судебной защиты прав граждан, наличием контролирующего органа, предпринимающего все меры для выполнения целей и положений законодательства и наделенного соответствующими полномочиями, а также административными и уголовными санкциями за нарушение требований законодательства.

В соответствии с указанными критериями Европейским союзом в качестве обеспечивающих адекватную защиту персональных данных был признан ряд стран, не присоединившихся к Конвенции 1981 года, в том числе Аргентина, Австралия, Канада, Швейцария, Государство Израиль.

Комментируемая норма означает, что оператор персональных данных в случае принятия решения о необходимости трансфера данных за рубеж должен определить статус государства в качестве участника Конвенции 1981 года или обеспечивающего «режим адекватной защиты», прежде чем применять требования к обработке персональных данных, установленные Законом о персональных данных.

Вместе с тем операторам персональных данных следует определить, о каких требованиях законодательства в области персональных данных идет речь (*см. комментарий к ст. 5 Закона о персональных данных*).

Прежде всего, трансграничная передача, наравне с любым иным способом обработки персональных данных, должна соответствовать целям сбора персональных данных.

☑ Например, передача за границу данных студентов для организации летней стажировки на территории этого государства будет соответствовать цели сбора данных в случае, если данные переданы в страну, где будет проходить стажировка. В то же время передача персональных данных школьников на серверные мощности иностранных провайдеров хостинга электронных дневников не соответствует цели сбора персональных данных, а именно предоставление родителям сведений об успеваемости учащихся, поскольку не ясна цель передачи данных, допустим, на территорию Виргинских островов, если родители ученика проживают в России.

В комментируемой статье законодатель также предусмотрел ряд ограничений и запретов для передачи данных на территорию иностран-

ных государств. Так, трансграничная передача может быть ограничена или запрещена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства. Безусловно, такие ограничения и запреты подлежат законодательному установлению, и в случае если нормы федеральных законов РФ не содержат таких ограничений и запретов применительно к определенным случаям, то их передача возможна.

2. Часть 2 комментируемой статьи устанавливает полномочие уполномоченного органа по защите прав субъектов персональных данных по утверждению перечня иностранных государств, обеспечивающих адекватную защиту персональных данных, а также определяет критерии оценки адекватности такой защиты.

Постановлением Правительства РФ от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» функции государственного органа, уполномоченного осуществлять защиту прав в сфере персональных данных, были возложены на Роскомнадзор.

Приказом Роскомнадзора от 15.03.2013 № 274 был утвержден Перечень 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. В указанный перечень вошли 18 стран и один административный район иностранного государства.

Впоследствии приказом Роскомнадзора от 29.10.2014 № 152 из указанного перечня были исключены Специальный административный район Гонконг Китайской Народной Республики и Швейцарская Конфедерация. Данные изменения фактически являются редакционными, поскольку Гонконг не является суверенным государством, а Швейцария ратифицировала Конвенцию 1981 года, и, соответственно, относится к тем государствами, чья адекватность в защите персональных данных не требует дополнительных оценок.

В настоящее время в перечень стран, обеспечивающих адекватную защиту персональных данных, входят 17 государств, а именно: Австралия — Австралийский союз, Аргентинская Республика, Государство Израиль, Канада, Королевство Марокко, Малайзия, Мексиканские Соединенные Штаты, Монголия, Новая Зеландия, Республика Ангола, Республика Бенин, Республика Кабо-Верде, Республика Корея, Республика Перу, Республика Сенегал, Тунисская Республика, Республика Чили.

Операторам персональных данных, осуществляющих трансграничную передачу персональных данных, в целях соблюдения правил передачи данных на территорию иностранного государства следует наблюдать за изменениями в рассматриваемом перечне, поскольку актуализация сведений о странах, обеспечивающих адекватную защиту персональных данных, производится Роскомнадзором периодически по мере такой необходимости. Так, в случае получения информации о соответствии (несоответствии) того или иного государства существующим критериям будут вноситься корректировки в указанный список стран.

Комментируемая статья также определяет критерии, которыми Роскомнадзору следует руководствоваться при оценке адекватности защиты и принятии решения о необходимости включения (исключения) в перечень той или иной страны.

При этом законодатель выделил лишь два критерия оценки адекватности: во-первых, соответствие норм права иностранного государства положениям Конвенции 1981 года; во-вторых, применение на территории государства мер безопасности в отношении персональных данных.

> **Таким образом**, уполномоченный орган по защите прав субъектов персональных данных при принятии решения о включении в перечень того или иного государства должен в первую очередь оценить нормативную базу другого государства на предмет ее соответствия положениям Конвенции 1981 года. Представляется, что такая оценочная деятельность может осуществляться компетентными органами Совета Европы, а уполномоченный орган РФ может проводить сравнение зарубежного нормотворчества со своим внутренним законодательством и впоследствии давать какую-либо оценку.

Более того, установление факта применения на территории иностранного государства мер безопасности персональных данных в качестве одного из критериев адекватности защиты данных, по сути, является условным, поскольку их наличие не всегда может обеспечивать защищенность данных. Кроме этого, не ясно, что следует понимать под термином «меры безопасности». На наш взгляд, вопрос отнесения требований иностранного государства к защите персональных данных в качестве адекватных мер защиты требует дополнительной регламентации в подзаконных нормативных правовых актах, в которых в том числе должен быть более четко раскрыт перечень мер безопасности, достаточный для включения страны в рассматриваемый перечень.

3. В ч. 3 комментируемой статьи закреплена обязанность оператора персональных данных до начала осуществления трансграничной передачи данных убедиться в том, что иностранным государством, на территорию которого осуществляется передача данных, обеспечивается адекватная защита прав субъектов персональных данных.

При этом надлежащее исполнение такой обязанности оператором фактически сводится к проверке перед трансграничной передачей персональных данных статуса Конвенции 1981 года и перечня, утвержденного Роскомнадзором, на предмет наличия в указанных документах сведений о стране, в которую предполагается осуществить передачу данных.

Из литературы, а также из материалов форумов и сайтов, посвященных указанной тематике, следует, что рассматриваемая норма ставит операторов персональных данных в затруднительное положение в связи с необходимостью оператора самостоятельно проводить сравнительно-правовые исследования в целях определения наличий у той или иной страны адекватной защиты прав субъектов персональных данных[1].

Вместе с тем положения ч. 2 ст. 12 комментируемого закона свидетельствуют о том, что подобные оценки лежат в плоскости публичных правоотношений и могут устанавливаться только органом государственной власти. Так, утверждение перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, является исключительным полномочием Роскомнадзора. Исследования операторов персональных данных не могут повлечь за собой правовых последствий в отношении неограниченного круга лиц в части распространения результатов исследований на общественные отношения в сфере персональных данных.

Подтверждение факта надлежащего исполнения оператором персональных данных указанной обязанности никак не документируется и в случае проведения проверочных мероприятий со стороны контрольного органа власти сводится к проверке наличия сведений о соответствующем иностранном государстве в перечне стран, обеспечивающих адекватную защиту персональных данных, на момент осуществления трансграничной передачи данных проверяемого оператора. Так, свидетельством неисполнения оператором персональных данных рассматриваемой обязанности служит отсутствие информации об иностранном

---

[1] См.: *Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С.* Комментарий к Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» (постатейный) // СПС «КонсультантПлюс».

государстве в утвержденном Роскомнадзором перечне на момент осуществления трансграничной передачи данных.

4. Часть 4 комментируемой статьи содержит норму, определяющую условия трансграничной передачи данных на территорию иностранных государств, не обеспечивающих адекватной защиты персональных данных. Таким образом, несмотря на общее правило о возможности осуществления трансграничной передачи данных на территории тех государств, которые являются либо сторонами Конвенции 1981 года, либо обеспечивают адекватную защиту прав субъектов персональных данных, в определенных случаях законодатель предусмотрел возможность передавать данные на территорию иных стран.

Согласно п. 1 рассматриваемой части статьи исключением из общего правила является наличие согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных. Указанное положение направлено на реализацию и развитие установленного ч. 1 ст. 9 Закона о персональных данных права субъекта персональных данных свободно, в своем интересе и своей волей распоряжаться личной информацией. Таким образом, если субъект персональных данных не возражает против рассматриваемой трансграничной передачи и подтверждает свое согласие в письменной форме, то оператор персональных данных, основываясь на положениях п. 1 ч. 4 ст. 12 комментируемого закона, вправе передавать персональные данные за границу.

Вместе с тем анализируемая норма должна рассматриваться оператором персональных данных в соотношении с иными положениями Закона о персональных данных, регламентирующими принципы обработки персональных данных. Так, согласно ч. 2 ст. 5 комментируемого закона не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. При этом трансграничная передача персональных данных представляет собой один из видов обработки персональных данных.

> **Таким образом**, в случае если трансграничная передача персональных данных на территорию государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, не соответствует цели сбора данных, то передача данных будет нарушать требования законодательства в сфере персональных данных, даже при наличии согласия субъекта персональных данных на такую передачу.

☑ Например, сбор персональных данных школьников для ведения электронного журнала осуществляется с целью предоставления родителям информации о текущей успеваемости их ребенка. В связи с этим рассматриваемая трансграничная передача персональных данных детей, даже при наличии согласия родителей, не будет соответствовать цели сбора данных.

Пункт 2 ч. 4 комментируемой статьи определяет в качестве условия, допускающего трансграничную передачу данных на территорию государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, наличие международного договора РФ, положения которого устанавливают случаи такой передачи. Более того, дополнительное получение оператором согласия субъекта персональных данных на такую передачу его данных не требуется.

При этом в качестве международных договоров РФ рассматриваются не только межгосударственные договоры, но также межправительственные договоры и договоры межведомственного характера, как двусторонние, так и многосторонние. Такое понимание международных договоров РФ соответствует положениям п. 2 ст. 3 Федерального закона «О международных договорах Российской Федерации».

В указанных международных договорах могут отсутствовать термины «трансграничная передача», «персональные данные», однако содержание конкретных норм таких соглашений или соглашения в целом должно быть направлено именно на осуществление действий, которые классифицируются законодательством в сфере персональных данных в качестве трансграничной передачи данных. Зачастую в таких международных соглашениях определяется объем личных данных, который подлежит обмену между сторонами договора, или предписание, обязывающее ту или иную категорию субъектов различных правоотношений передавать часть имеющихся у них личных данных лицам, находящимся на территории иностранного государства.

Можно привести большое количество примеров международных соглашений, предусматривающих возможность трансграничной передачи персональных данных на территорию стран, не обеспечивающих адекватной защиты персональных данных. К ним можно отнести международные договоры РФ о реадмиссии, большую часть международных соглашений РФ об оказании международной правовой помощи, предусматривающих пересылку документов, содержащих персональные данные, в частности Минскую конвенцию о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам от 22 января 1993 г., и др.

Согласно п. 3 ч. 4 анализируемой статьи трансграничная передача данных на территорию государств, не обеспечивающих адекватной защиты персональных данных, может также осуществляться в случаях, когда такая передача прямо предусмотрена иными федеральными законами.

Вместе с тем наличие норм-исключений в таких федеральных законах должно быть обусловлено целями, которые указаны в п. 3 ч. 4 комментируемой статьи, в виде исчерпывающего перечня. К таким целям относятся:

- защита основ конституционного строя РФ;
- обеспечение обороны страны и безопасности государства;
- обеспечение безопасности устойчивого и безопасного функционирования транспортного комплекса;
- защита интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

В соответствии с п. 4 ч. 4 комментируемой статьи исполнение оператором положений договора, стороной которого является субъект персональных данных, также является исключением, позволяющим трансграничную передачу персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных.

Договорные обязательства оператора персональных данных позволяют производить трансграничную передачу данных без учета согласия субъекта персональных данных на территорию государств, не обеспечивающих адекватной защиты персональных данных. Данная норма закона позволяет оператору персональных данных руководствоваться коммерческим интересом при выборе контрагентов в рамках сферы деятельности своей организации и не доказывать необходимость реализации того или иного бизнес-процесса именно на территории страны своего зарубежного контрагента. Вместе с тем оператор может передавать персональные данные исключительно с целью исполнения взятых на себя обязательств по договору, и в этом смысле он ограничен сроком действия договора или сроком исполнения своих обязательств.

В п. 5 ч. 4 анализируемой статьи предусмотрен случай, когда получение согласия на обработку персональных данных в части их трансграничной передачи от субъекта персональных данных не представляется возможным. Вместе с тем их обработка необходима для защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц.

При этом законодатель не конкретизирует обстоятельства, которые могут свидетельствовать о невозможности получения согласия субъекта персональных данных. Норма сформулирована таким образом, что к данным обстоятельствам могут быть отнесены не только форс-мажорные, но также любые затруднения, не позволяющие оператору связаться с субъектом персональных данных в ситуации, когда требуется моментальное принятие решения для защиты жизни и здоровья.

Статья 13. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных

1. Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных.

2. Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.

3. Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.

4. В целях обеспечения реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах персональных данных может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.

1. В ч. 1 комментируемой статьи законодатель установил право государственных и муниципальных органов создавать информационные системы персональных данных.

При этом создание информационных систем персональных данных должно быть обусловлено полномочиями, установленными в федеральных законах. Таким образом, государственными и муници-

пальными органами могут создаваться информационные системы персональных данных исключительно во исполнение полномочий, установленных в федеральных законах. Такое требование комментируемого закона не предъявляется к иным информационным системам персональных данных, создание которых осуществляется непубличными организациями.

Следует заметить, что понятие государственных и муниципальных информационных систем персональных данных является более узким по сравнению с государственными и муниципальными информационными системами.

> В соответствии с ч. 1 ст. 13 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» **государственные информационные системы** — это федеральные и региональные информационные системы, созданные на основании федеральных законов, законов субъектов РФ и актов государственных органов. **Муниципальные информационные системы** — это системы, созданные на основании решений органов местного самоуправления.

В настоящее время персональные данные граждан находятся в различных информационных системах и базах данных и обрабатываются во всех сферах государственного и муниципального управления: налоговой службой, службой занятости, ПФР, ФФОМС, органами загса и т.д.

При этом полномочия данных государственных и муниципальных органов определены соответствующими федеральными законами в области регистрации актов гражданского состояния, налогообложения, социального обеспечения и т.д.

2. Часть 2 анализируемой статьи определяет возможность установления особенностей учета персональных данных, а также способов обозначения принадлежности данных конкретному субъекту персональных данных в государственных и муниципальных информационных системах персональных данных в федеральных законах. Иными нормативными правовыми актами особенности учета персональных данных в государственных информационных системах персональных данных устанавливаться не могут.

3. При обозначении принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных, согласно ч. 3 комментируемой статьи, не допускается исполь-

зование способов, оскорбляющих чувства граждан или унижающих человеческое достоинство.

Кроме этого, в ч. 3 рассматриваемой статьи содержится запрет на ограничение прав и свобод человека и гражданина по мотивам, связанным с использованием различных способов обработки персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных.

В связи с этим оператор персональных данных не должен использовать способы обработки персональных данных, которые могут привести к нарушению прав и свобод человека и гражданина.

4. Часть 4 комментируемой статьи предусматривает возможность создания в Российской Федерации государственного регистра населения. При этом целью создания государственного регистра населения может являться только обеспечение реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах.

Правовой статус регистра, а также порядок его работы должны быть определены нормативным правовым актом, обладающим юридической силой федерального закона.

Следует заметить, что до сих пор в Российской Федерации нет единого государственного регистра населения, обеспечивающего 100%-ный охват населения страны. Однако отдельные попытки создать такой регистр предпринимались. Так, в 2000 году Минсвязи России был разработан проект Концепции создания автоматизированной системы «Государственный регистр населения», которая не была одобрена. Позднее распоряжением Правительства РФ от 09.06.2005 № 748-р была одобрена Концепция создания системы персонального учета населения Российской Федерации.

До настоящего времени государственные и муниципальные органы осуществляют автономную регистрацию различных категорий населения в своих информационных системах, автоматизированных базах, реестрах персональных данных.

> **Таким образом**, можно констатировать, что определенные персональные данные в государственных и муниципальных информационных системах имеются, но разбросаны по разным базам, не централизованы и дублируются в не согласованных друг с другом системах. При этом рассматриваемая норма лишь допускает возможность создания государственного регистра населения, но не обязывает.

Глава 3
Права субъекта персональных данных

Статья 14. Право субъекта персональных данных на доступ к его персональным данным
(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)

1. Субъект персональных данных имеет право на получение сведений, указанных в части 7 настоящей статьи, за исключением случаев, предусмотренных частью 8 настоящей статьи. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2. Сведения, указанные в части 7 настоящей статьи, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

3. Сведения, указанные в части 7 настоящей статьи, предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

4. В случае, если сведения, указанные в части 7 настоящей статьи, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный

запрос в целях получения сведений, указанных в части 7 настоящей статьи, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4 настоящей статьи, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в части 3 настоящей статьи, должен содержать обоснование направления повторного запроса.

6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 настоящей статьи. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

1. Комментируемая статья раскрывает имеющее важное юридическое и практическое значение для субъекта персональных данных право на доступ к его персональным данным.

В основе норм этой статьи лежит принцип диспозитивности, суть которого сводится к самостоятельному определению участником правоотношений способа своего поведения, в частности реализации предоставленных прав и свобод по своему усмотрению, за исключением случаев, установленных в ч. 8 комментируемой статьи, когда право на доступ к персональным данным может быть ограничено.

В указанной статье установлены процедурные моменты реализации права на доступ, в том числе конкретизированы механизмы направления запроса и получения ответа, сроки и возможные каналы документооборота, права и обязанности сторон.

Так, ч. 1 анализируемой статьи содержит отсылочные нормы к ч. 7 и 8 этой статьи, регулирующим право субъекта на получение определенного объема информации, касающейся обработки его персональных данных, и случаи ограничения права субъекта на доступ к его персональным данным.

В Законе о персональных данных установлено, что сведения, указанные в ч. 7 комментируемой статьи, должны быть предоставлены субъекту персональных данных оператором в доступной форме при обращении либо при получении запроса от субъекта персональных данных.

Например, согласно пп. «д» п. 31 Правил предоставления коммунальных услуг собственникам и пользователям помещений в многоквартирных домах и жилых домов, утвержденных постановлением Правительства РФ от 06.05.2011 № 354, исполнитель обязан производить непосредственно при обращении потребителя проверку правильности исчисления предъявленного потребителю к уплате размера платы за коммунальные услуги, задолженности или переплаты потребителя за коммунальные услуги, правильности начисления потребителю неустоек (штрафов, пеней) и немедленно по результатам проверки выдавать потребителю документы, содержащие правильно начисленные платежи.

Исходя из данной нормы, оператор обязан предоставить информацию потребителю об отсутствии (наличии) у него задолженности за коммунальные услуги за интересующий его период времени.

Между тем, согласно ч. 8 комментируемой статьи, право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

☑ Например, в соответствии с п. 1 ст. 53 Федерального закона «О связи» предоставление третьим лицам сведений об абонентах-гражданах может осуществляться только с их согласия, за исключением случаев, предусмотренных федеральными законами. В силу п. 1 ст. 64 указанного закона «*операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, информацию о пользователях услугами связи и об оказанных им услугах связи, а также иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами*».

Следует заметить, что право на доступ является воплощением нормы, установленной в ст. 8 Конвенции 1981 года, согласно которой любому лицу должна быть предоставлена возможность:

1) знать о существовании автоматизированного файла персональных данных, знать его основные цели, а также название и место обычного проживания или местонахождение контролера файла;
2) получить через разумный промежуток времени и без чрезмерной задержки или чрезмерных расходов подтверждение того, хранят-

ся ли касающиеся его персональные данные в автоматизированном файле данных, а также получить такие данные в доступной для пониманий форме;

3) добиваться в случае необходимости исправления или уничтожения таких данных, если они подвергались обработке в нарушение норм внутреннего законодательства, воплощающего основополагающие принципы, изложенные в ст. 5 и 6 Конвенции 1981 года;
4) прибегать к средствам правовой защиты в случае невыполнения просьбы о подтверждении или в случае необходимости предоставления данных, их изменении или уничтожении, как это предусмотрено в п. 2 и 3 данного перечня.

В ч. 1 комментируемой статьи установлено также право субъекта персональных данных требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Зачастую в Роскомнадзор поступают жалобы от субъектов персональных данных по вопросу оказания помощи в удалении аккаунтов в социальных сетях, уничтожении персональных данных на определенных интернет-ресурсах. Вместе с тем в данном случае субъект персональных данных в рамках ч. 1 комментируемой статьи вправе самостоятельно обратиться к администратору сайта, как оператору персональных данных, с требованием удалить, уточнить, уничтожить неточные, неполные, устаревшие персональные данные.

В 2014 году Судом Европейского союза было узаконено «право быть забытым», означающее, что персональные данные гражданина по его запросу должны быть полностью удалены из регистров. В Российской Федерации данное право реализуется, в том числе в виде права субъекта персональных данных требовать от оператора прекратить обработку его персональных данных, уточнить и актуализировать сведения о себе.

Первым последствием решения Суда Европейского союза по делу Марио Костеха Гонсалеса, закрепившего это право, стал запуск в Европе функции изъятия личных данных из поиска *Google*. Так, любой гражданин Европейского союза может потребовать удаления из результата поиска, сделанного по его имени, ссылки на документы, которые не соответствуют действительности или содержат устаревшую информацию. Для этого гражданин должен напрямую обратиться с запросом в поисковую систему *Google*, *Yahoo*, *Bing* или любую другую, которая

обязана выяснить его обоснованность. Согласно решению Суда Европейского союза, граждане вправе обратиться к поисковому сервису в определенных случаях: когда данные размещены законно, но при этом устарели и потеряли актуальность.

Вместе с тем в Российской Федерации «право быть забытым» может рассматриваться в разрезе удаления информации не только из поисковиков, но и из социальных сетей и иных информационных ресурсов. При взаимодействии с операторским сообществом Роскомнадзор использует корректные механизмы защиты персональных данных и удаления личной информации в Интернете, часто не прибегая к судебным процедурам, а используя правила работы отрасли, механизмы саморегулирования.

2. В ч. 2 комментируемой статьи определены требования, предъявляемые к форме и содержанию предоставляемых в соответствии с ч. 7 указанной статьи оператором сведений субъекту персональных данных. Так, информация, касающаяся обработки персональных данных, предоставляется оператором в доступной форме. Вместе с тем законодателем не раскрывается понятие «доступная форма».

Следует отметить, что в указанной информации не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Данная норма направлена на реализацию положений ст. 23 Конституции РФ. Так, гарантируемое ч. 1 ст. 23 Конституции РФ право на неприкосновенность частной жизни распространяется на ту сферу жизни, которая относится к отдельному лицу, касается только этого лица и охватывает охрану тайны всех сторон личной жизни лица, оглашение которых лицо по тем или иным причинам считает нежелательным.

Право на неприкосновенность частной жизни означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера.

> **Таким образом**, комментируемая норма создает правовую основу обращения с персональными данными физических лиц в целях реализации конституционных прав человека, в том числе права на неприкосновенность частной жизни, личную и семейную тайну.

3. В ч. 3 ст. 14 Закона о персональных данных обозначен порядок предоставления субъекту персональных данных или его представителю оператором сведений, указанных в ч. 7 анализируемой статьи.

Указанные сведения предоставляются субъекту персональных данных при обращении либо при получении запроса субъекта персональных данных или его представителя.

Кроме этого, в ч. 3 рассматриваемой статьи определены требования к содержанию запроса, а именно: запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством РФ.

Вопросы доступности получения информации и ее защиты затрагиваются также в других федеральных законах.

☑ Например, работник как субъект персональных данных обладает определенными правами на защиту своих персональных данных, имеющихся у работодателя. Статья 89 ТК РФ конкретизирует такие права работника. В частности, он имеет право на полную информацию о его персональных данных и об обработке этих данных и свободный бесплатный доступ к своим данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом.

☑ Подобные требования заложены в Федеральном законе «Об организации предоставления государственных и муниципальных услуг», согласно которому запрос заявителя в орган, предоставляющий услугу, приравнивается к согласию такого заявителя с обработкой его персональных данных в целях и объеме, необходимых для предоставления государственной или муниципальной услуги. Если для предоставления государственной или муниципальной услуги необходима обработка персональных данных лица, не являющегося заявителем, и если в соответствии с федеральным законом обработка таких персональных данных может осуществляться с согласия указанного лица, при обращении за получением государственной или муниципальной услуги заявитель дополнительно представляет документы, подтверждающие получение согласия указанного лица или его законного пред-

ставителя на обработку персональных данных указанного лица. Документы, подтверждающие получение согласия, могут быть представлены в том числе в форме электронного документа.

☑ В соответствии со ст. 22 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» информация о состоянии здоровья предоставляется пациенту лично лечащим врачом или другими медицинскими работниками, принимающими непосредственное участие в медицинском обследовании и лечении. Пациент либо его законный представитель имеет право непосредственно знакомиться с медицинской документацией, отражающей состояние его здоровья, в порядке, установленном уполномоченным федеральным органом исполнительной власти, а также на основании письменного заявления получать отражающие состояние здоровья медицинские документы, их копии и выписки из медицинских документов.

4. В ч. 4 комментируемой статьи определены требования к порядку направления и срок повторного запроса в целях получения сведений, указанных в ч. 7 рассматриваемой статьи, а также процедура ознакомления с такими персональными данными.

В частности, в ней предусмотрено, что право повторного обращения к оператору или направления ему повторного запроса возникает не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса. Таким образом, в этой норме установлены ограничения в реализации права субъекта на доступ к его персональным данным.

Указанное ограничение направлено на предотвращение злоупотреблением правом на доступ к персональным данным со стороны субъектов персональных данных.

5. В ч. 5 анализируемой статьи определены условия, при которых срок, указанный в ее ч. 4, может быть сокращен. Так, субъект персональных данных вправе обратиться к оператору или направить повторный запрос до истечения 30 дней, если по результатам рассмотрения первоначального обращения субъекта персональных данных сведения, указанные в ч. 7 комментируемой статьи, были предоставлены для ознакомления не в полном объеме.

Еще одним условием сокращения установленного срока является обоснование, предоставленное субъектом персональных данных в случае направления повторного запроса.

6. В ч. 6 рассматриваемой статьи определены основания для отказа в выполнении повторного запроса. Так, оператор вправе отказать субъ-

екту персональных данных в выполнении повторного запроса, если он не соответствует условиям, предусмотренным ч. 4 и 5 комментируемой статьи. При этом такой отказ должен быть мотивированным.

Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

7. В ч. 7 ст. 14 Закона о персональных данных приводится перечень сведений, право на получение которых имеет субъект персональных данных. При этом данный перечень сведений не является исчерпывающим, и субъект вправе получать иные сведения, необходимые ему для реализации права на доступ, за исключением случаев, предусмотренных ч. 8 анализируемой статьи.

Следует отметить, что в запрашиваемых субъектом персональных данных у оператора сведениях не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

➥ **Таким образом**, законодатель гарантирует субъекту персональных данных достаточно полную осведомленность о текущем положении дел с его персональными данными, обрабатываемыми конкретным оператором.

8. Частью 8 комментируемой статьи определены основания для ограничения права субъекта на доступ к его персональным данным. При этом данный перечень оснований не является исчерпывающим, соответственно, право на доступ может быть ограничено по иным основаниям, установленным федеральными законами.

Данное ограничение права на доступ связано с интересами безопасности и правосудия, с нарушением конституционных прав и свобод других лиц. Так, получение данных о себе из органа, осуществляющего оперативно-разыскную деятельность, возможно в объеме, обеспечивающем защиту охраняемых законом интересов, например, строго охраняются сведения об источниках оперативной информации, если ими являются лица, добровольно сотрудничающие с правоохранительными органами.

Рассмотрим основания для ограничения права на доступ, указанные в ч. 8 анализируемой статьи.

⇨ Во-первых, право субъекта на доступ к его персональным данным ограничено в тех случаях, когда обработка персональных данных осуществляется в целях обороны страны, безопасности государства и охраны правопорядка. К данной информации могут относиться пер-

сональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности.

⇨ Во-вторых, основанием для ограничения права доступа к персональным данным является обработка персональных данных, которая производится органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения. Между тем в установленных уголовно-процессуальным законодательством случаях допускается ознакомление подозреваемого или обвиняемого с такими персональными данными.

⇨ В-третьих, основанием для ограничения рассматриваемого права является обработка персональных данных, осуществляемая в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

⇨ В-четвертых, основанием такого ограничения является обработка персональных данных в случаях, предусмотренных законодательством РФ о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

⇨ В-пятых, право субъекта персональных данных на доступ к его персональным данным ограничивается, если этот доступ нарушает права и законные интересы третьих лиц.

При применении рассматриваемой нормы следует учитывать сложившуюся судебную практику.

Так, Приморский краевой суд в своем определении от 13.02.2014 № 33-1032 указал следующее.

«В соответствии с пунктом 4 части 8 статьи 14 Федерального закона от 27 июля 2006 года № 152-ФЗ „О персональных данных“ право субъекта персональных данных на доступ к его персональным данным может быть ограничено, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

В то же время, в случае, когда третье лицо выступает контрагентом по договору купли-продажи транспортного средства, заключенному между ним и Б. (К.), исходя из положений гражданского

законодательства, регулирующего порядок заключения сделок, данное третье лицо при заключении договора выражает согласие предоставить персональные данные о себе продавцу автомашины (в тех пределах, которые указаны в договоре), следовательно, Б. (К.) имеет право на ознакомление с договором купли-продажи (справкой-счетом) транспортного средства марки... с доверенностью на право продажи автомобиля, а также документами о регистрации снятия автомашины с учета по ее заявлению».

Статья 15. Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации

1. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.

2. Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных, указанную в части 1 настоящей статьи.

1. Часть 1 комментируемой статьи устанавливает требование, предъявляемое к оператору при обработке персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации. В этих случаях обработка персональных данных допускается только при условии предварительного согласия субъекта персональных данных. Причем обязанность по доказыванию получения такого согласия лежит на операторе.

В то же время если персональные данные обрабатываются в целях исполнения договора, одной из сторон которого является субъект персональных данных, то в соответствии с п. 5 ч. 1 ст. 6 Закона о персональных данных согласия этого субъекта не требуется.

На практике встречаются случаи, когда оператор, ссылаясь на п. 5 ч. 1 ст. 6 комментируемого закона, заключая договор с физическим лицом, использует данные физического лица (номер телефона) для рекламной рассылки в целях продвижения товаров без получения согласия физического лица.

Однако, исходя из положений ст. 6 Закона о персональных данных, получение согласия субъекта на обработку персональных данных не требуется, если это непосредственно связано с исполнением и (или) зак-

лючением договора. Последующее использование персональных данных в маркетинговых целях никак не связано с исполнением договора, стороной или выгодоприобретателем которого является физическое лицо. Таким образом, оператору персональных данных требуется получение согласия на использование данных в целях продвижения своих товаров. При нарушении указанного требования оператор персональных данных подлежит привлечению к ответственности на основании ст. 13.11 КоАП РФ.

В судебной практике возникают споры, когда управляющая организация многоквартирными домами рассылает по почтовым ящикам жильцов счета-квитанции на оплату жилья и коммунальных услуг, на обратной стороне которых содержится реклама товаров, работ и услуг различных организаций.

Так, постановлением заместителя прокурора Ленинского района г. Ярославля от 23.09.2010 было возбуждено производство по делу об административном правонарушении, предусмотренном ст. 13.11 КоАП РФ, в отношении ОАО «Управляющая организация многоквартирными домами Ленинского района». В постановлении указывается, что общество на счетах-квитанциях на оплату коммунальных услуг, содержащих персональные данные граждан, размещало рекламу товаров работ и услуг организаций, не получив предварительного согласия субъектов персональных данных в нарушение ч. 1 ст. 15 Закона о персональных данных.

Постановлением мирового судьи от 07.12.2010 производство по делу прекращено за отсутствием состава административного правонарушения.

Решением судьи районного суда от 29.12.2010 указанное постановление мирового судьи отменено, производство по делу прекращено в связи с истечением срока давности привлечения к административной ответственности.

Суд надзорной инстанции отменил решение судьи районного суда, оставив в силе постановление мирового судьи, с учетом следующего.

В силу ч. 1 ст. 15 Закона о персональных данных обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой

без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.

При этом согласно п. 3 ст. 3 названного закона обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных; в соответствии с п. 4 указанной статьи распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в СМИ, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Как видно из материалов дела, ОАО «Управляющая организация многоквартирными домами Ленинского района» осуществляет обработку персональных данных жильцов обслуживаемых домов с целью регистрационного учета граждан и осуществления им начислений за оказанные коммунальные услуги и услуги по содержанию и ремонту жилья на основании договоров на управление многоквартирными домами. Во исполнение указанных договоров общество рассылает по почтовым ящикам жильцов счета-квитанции на оплату жилья и коммунальных услуг, на обратной стороне которых содержится реклама различных организаций. При этом, как установлено в судебных заседаниях, действий, направленных на передачу персональных данных каким-либо третьим лицам, общество не допускало. Доведение же персональных данных до их обладателя распространением по смыслу вышеуказанных положений закона не является. Поэтому утверждение в решении судьи районного суда, что общество осуществляло обработку персональных данных в форме их распространения не основано на положениях п. 3, 4 ст. 3, ч. 1 ст. 15 Закона о персональных данных. В связи с этим не имеют значения для рассмотрения данного дела содержащиеся в решении судьи районного суда ссылки на то, что общество преследовало факультативную цель продвижения товаров работ и услуг и извлекало из этого доход.

См.: Постановление Президиума Ярославского областного суда от 28.03.2011.

2. Частью 2 анализируемой статьи предусмотрена обязанность оператора немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных, указанную в ч. 1 комментируемой статьи. То есть оператор обязан прекратить обработку персональных данных по требованию субъекта персональных данных, в том числе тогда, когда такая обработка проводится в рекламных целях или для политической агитации. На обработку персональных данных оператор обязан получить согласие субъекта персональных данных до ее начала.

В практике имеются случаи сбора и передачи персональных данных субъектов в целях политической агитации (рассылка агитационных писем) без предварительного согласия субъектов персональных данных в нарушение Закона о персональных данных. При этом агитационные материалы направляются избирателям с указанием их персональных данных, что является нарушением положений Закона о персональных данных.

> **Таким образом**, в случае поступления соответствующего требования от субъекта персональных данных оператор будет обязан немедленно прекратить обработку его персональных данных, осуществляемую в целях политической агитации.

Законодатель ограничил возможность обработки персональных данных в целях продвижения товаров, работ, услуг на рынке путем прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации, установив, что обработка информации в таких целях допускается только при условии предварительного согласия субъекта.

На практике случаи запрашивания предварительного согласия субъекта персональных данных на рассылку рекламной или иной подобной корреспонденции крайне редки.

В некоторых европейских государствах, в частности в Испании, лиц, занимающихся рассылкой рекламной и иной подобной корреспонденции, закон обязывает в каждом письме субъекту указывать не только источник получения персональных данных субъекта и его права в отношении их использования, но также и сведения о личности держателя (т.е. автора корреспонденции)[1].

---

[1] См.: *Защита* персональных данных. Опыт правового регулирования / сост. Е.К. Волчинская. М., 2001. С. 119.

Статья 16. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных

1. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

3. Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

4. Оператор обязан рассмотреть возражение, указанное в части 3 настоящей статьи, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения. *(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

1. Часть 1 ст. 16 Закона о персональных данных предусматривает запрет на принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

2. Часть 2 комментируемой статьи устанавливает исключительные случаи, когда решения, порождающие юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, могут быть приняты на основании исключительно автоматизированной обработки персональных данных. По общему правилу это возможно лишь с письменного согласия субъекта персональных данных. Кроме этого, указанные решения могут быть приняты в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

Вместе с тем законодатель не установил требования к содержанию такого согласия, а также, в отличие от согласия на обработку персональных данных, не предусмотрел права субъекта персональных дан-

ных отозвать ранее данное согласие на принятие решений, порождающих юридические последствия в отношении этого субъекта или иным образом затрагивающих его права и законные интересы.

3. Согласно ч. 3 анализируемой статьи оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

Законодатель не устанавливает обязательных требований к порядку разъяснения прав субъектов персональных данных, а также не предусматривает требования, в том числе к форме такого документа, которым должно соответствовать возражение против решения, принятого на основании исключительно автоматизированной обработки. Представляется, что формы таких документов могут быть установлены операторами персональных данных самостоятельно в документах, определяющих политику в отношении обработки персональных данных, локальных актах по вопросам обработки персональных данных.

4. Часть 4 ст. 16 комментируемого закона устанавливает срок, в течение которого оператор обязан рассмотреть возражение против решения, принятого на основании исключительно автоматизированной обработки, который составляет 30 дней со дня его получения. По итогам рассмотрения оператор обязан уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

Статья 17. Право на обжалование действий или бездействия оператора

1. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

1. Комментируемая статья устанавливает гарантии права субъектов персональных данных на обжалование действий или бездействия операторов. Данная норма детализирует общее право на защиту, закрепленное в ст. 46 Конституции РФ, применительно к отношениям в сфере защиты персональных данных. Так, субъект персональных дан-

ных может обжаловать действия (бездействие) оператора персональных данных в уполномоченный орган по защите прав субъектов персональных данных или в суд.

При этом анализируемая статья не предусматривает обязательного досудебного порядка обжалования действий или бездействия оператора, т.е. действия или бездействие оператора могут быть обжалованы непосредственно в суд без предварительного обжалования в уполномоченный орган.

Следует заметить, что в Законе о персональных данных не детализируется понятие жалобы, не раскрывается ее содержание, и не устанавливается порядок подачи и рассмотрения жалобы субъекта персональных данных, так как отношения, связанные с реализацией гражданином закрепленного за ним Конституцией РФ права на обращение в государственные органы, а также порядок рассмотрения таких обращений государственными органами и должностными лицами установлены специальным законодательным актом — Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

> Согласно ст. 4 названного закона **жалоба** представляет собой просьбу гражданина о восстановлении или защите его нарушенных прав, свобод или законных интересов других лиц.

В жалобе должны быть указание о нарушении конкретных прав гражданина как субъекта персональных данных, подробное описание всех событий, связанных с нарушением этих прав, название оператора персональных данных, в действиях которого имеются признаки нарушения.

По результатам рассмотрения жалоб уполномоченный орган, в случае обнаружения в действиях (бездействии) операторов персональных данных нарушений законодательства о персональных данных, вправе принимать меры, предусмотренные ст. 23 Закона о персональных данных (*см. комментарий к ст. 23 Закона о персональных данных*).

Судебный порядок обжалования действий (бездействия) операторов персональных данных осуществляется по правилам гражданского судопроизводства.

2. Часть 2 комментируемой статьи направлена на реализацию субъектами персональных данных права на судебную защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда.

При этом реализовать свое право на возмещение убытков и (или) компенсацию морального вреда субъект персональных данных может исключительно в судебном порядке. В данном случае не предусмотрена возможность подачи жалобы в уполномоченный орган.

Глава 4
Обязанности оператора

Статья 18. Обязанности оператора при сборе персональных данных

(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)

1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 настоящего Федерального закона.

2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 настоящей статьи, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные настоящим Федеральным законом права субъекта персональных данных;

5) источник получения персональных данных.

4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные частью 3 настоящей статьи, в случаях, если:

1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

5) предоставление субъекту персональных данных сведений, предусмотренных частью 3 настоящей статьи, нарушает права и законные интересы третьих лиц.

1. Часть 1 комментируемой статьи дублирует положения ст. 14 Закона о персональных данных в части представления информации по запросу субъекта персональных данных или его представителя.

2. Последующие положения анализируемой статьи направлены на реализацию права гражданина на получение информации об обработке его персональных данных. При этом ч. 2 ст. 18 Закона о персональных данных касается больше обязанности субъекта представить необходимую информацию в случаях, предусмотренных законодательством, и обязанности оператора в части разъяснения последствий невыполнения этого требования.

3. Часть 3 комментируемой статьи содержит норму, которая предусматривает обязанность оператора информировать субъекта персональных данных о начале обработки персональных данных, полученных не от субъекта персональных данных.

Необходимо отметить, что указанная обязанность не распространяется на дилерские схемы, при реализации которых привлекаемые лица, являющиеся первичными организациями по сбору персональных данных, осуществляют свою деятельность от имени оператора.

4. Часть 4 рассматриваемой статьи устанавливает исключения, при которых оператор освобождается от необходимости информирования субъекта персональных данных.

Так, в п. 1 и 2 ч. 4 анализируемой статьи в качестве исключения указаны ситуации, связанные с реализацией различных агентских схем, в рамках которых оператор поручает осуществлять отдельные действия третьим лицам, проинформировав об этом субъекта персональных данных. Это, например, привлечение коллекторских агентств в рамках взыскания задолженности, передача управляющей компанией персональных данных третьим лицам для осуществления деятельности по приему платежей от населения. Под исключения, установленные в п. 2 ч. 4 комментируемой статьи, можно подвести деятельность по оказанию государственных и муниципальных услуг, предусматривающих межведомственное взаимодействие.

Пункт 3 ч. 4 комментируемой статьи предусматривает ситуацию, которая на сегодняшний день является наиболее актуальной.

Вопрос общедоступности персональных данных и их использования неограниченным кругом лиц тесно связан с различными интерактивными сервисами, социальными сетями, базами данных, находящимися в общем доступе. При этом зачастую при рассмотрении жалоб граждан на распространение их персональных данных в Интернете все сводится к положениям пользовательского соглашения, устанавливающего право неограниченного круга лиц получать доступ к персональным данным, к которому данные граждане присоединились на этапе регистрации в определенной социальной сети, интерактивном сервисе.

Обособленно стоят вопросы использования персональных данных из общедоступных баз данных (единого государственного реестра юридических лиц и единого государственного реестра индивидуальных предпринимателей). В данном случае нужно четко понимать, что размещение указанных данных продиктовано требованиями налогового законодательства и дальнейшее их распространение возможно только при условии их неизменности по отношению к первоисточнику с обязательным указанием ссылки на правоустанавливающий интернет-ресурс (сайт ФНС России).

Остальные случаи, связанные с деятельностью журналиста, научной, литературной и творческой деятельностью, обеспечением соблюдения прав третьих лиц, носят общий характер и регламентируются профильным законодательством.

5. С 1 сентября 2015 г. вступит в силу Федеральный закон от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях». В соответствии с этим законом ст. 18 Закона о персональных данных будет дополнена новой частью следующего содержания: «*5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети „Интернет“, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона*».

Статья 18.1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

(введена Федеральным законом от 25.07.2011 № 261-ФЗ)

1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональ-

ных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

3. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

4. Оператор обязан представить документы и локальные акты, указанные в части 1 настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в части 1 настоящей статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных.

1. По итогам проведенной в 2011 году масштабной работы по имплементации в профильное российское законодательство требований общеевропейского права в области персональных данных, являвшейся необходимым условием завершения процедуры ратификации Конвенции 1981 года, был принят Федеральный закон от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон „О персональных данных“». Этим законом, в частности, Закон о персональных данных был дополнен комментируемой статьей.

Основным нововведением данной статьи стал вектор саморегуляции, определивший право оператора самостоятельно устанавливать перечень мер, необходимых для выполнения обязанностей, предусмотренных Законом о персональных данных. Этим нововведением была понижена директивная составляющая законодательства РФ в области персональных данных.

Согласно ч. 1 комментируемой статьи оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами.

Однако законодателем приводится перечень мер, которые можно расценивать как необходимый минимум. К таким мерам, в частности, относятся:

- назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных (*см. подробнее комментарий к ст. 22.1 Закона о персональных данных*);

- издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.

Четкий перечень этих документов законодательно не установлен, и форма их жестко не регламентирована, но, опираясь на положения иных федеральных законов и подзаконных актов, можно сделать вывод, что основополагающим документом является положение об обработке персональных данных, устанавливающее цели, задачи деятельности по обработке персональных данных, перечень действий, категории персональных данных, категории субъектов персональных данных, способы обработки, сроки хранения, правила доступа и уничтожения персональных данных для каждой цели.

Наиболее полная градация таких документов представлена в постановлении Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом „О персональных данных“ и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», содержащем перечень мер, необходимый для соблюдения обязанностей, предусмотренных Законом о персональных данных, для операторов, являющихся государственными и муниципальными органами.

В частности, нормативная правовая база государственного или муниципального органа должна включать в себя:

- правила рассмотрения запросов субъектов персональных данных или их представителей;
- правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным комментируемым законом, принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора;
- правила работы с обезличенными данными в случае обезличивания персональных данных;
- перечень информационных систем персональных данных;
- перечни персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией служеб-

ных или трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций;

- перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- должностной регламент (должностные обязанности) или должностную инструкцию ответственного за организацию обработки персональных данных в государственном или муниципальном органе;
- типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;
- порядок доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка персональных данных и т.д.

В соответствии с ч. 1 анализируемой статьи к мерам, направленным на обеспечение соблюдения оператором законодательства о персональных данных, помимо вышеуказанных, также относятся:

- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со ст. 19 комментируемого закона;
- осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора. На внутриорганизационном уровне должен быть принят акт, регламентирующий порядок и условия проведения внутреннего контроля, сформирована действующая на постоянной основе комиссия. Данная мера коррелируется с положениями постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», возлагающими на оператора обязанность самостоятельно осуществлять контроль за соблюдением требова-

ний по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона о персональных данных, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных указанным законом. Вред должен определяться исходя из оценки всех неблагоприятных последствий, которые может повлечь несоблюдение требований Закона о персональных данных, от размера штрафных санкций до репутационных рисков и судебных издержек;
- ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников. Как правило, это происходит на этапе приема на работу и фиксируется в листе ознакомления.

2. Часть 2 комментируемой статьи обязывает оператора опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Примером является размещение соответствующих документов на информационном стенде, доступном неограниченному кругу лиц.

Также оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей сети. В качестве примера можно привести процедуру регистрации в отдельных социальных сетях, где пользователю изначально предлагают ознакомиться с документами, регламентирующими порядок и условия обработки его персональных данных.

3. Часть 3 анализируемой статьи определяет особенности мер, направленных на обеспечение выполнения обязанностей, предусмотрен-

ных Законом о персональных данных, операторами, являющимися государственными или муниципальными органами.

Перечень этих мер мало чем отличается от требований, предъявляемых к юридическим лицам и индивидуальным предпринимателям, за исключением пп. «з» п. 1 Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденного постановлением Правительства РФ от 21.03.2012 № 211, согласно которому государственные или муниципальные органы осуществляют обезличивание персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ. Изначальная формулировка этого подпункта носила императивный характер и обязывала государственные и муниципальные органы наряду с выполнением требований по технической защите персональных данных осуществлять обезличивание персональных данных, что по своей природе является одной из мер по обеспечению их безопасности при обработке в информационных системах персональных данных. Для устранения данной коллизии постановлением Правительства РФ от 06.09.2014 № 911 «О внесении изменений в перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом „О персональных данных“ и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» в указанный подпункт были внесены изменения, устанавливающие обязанность осуществлять обезличивание персональных данных только в случаях, определенных законодательством РФ, с использованием Требований и методов по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, утвержденных приказом Роскомнадзора от 05.09.2013 № 996.

4. Часть 4 ст. 18.1 Закона о персональных данных обязывает оператора по запросу Роскомнадзора представить документы и локальные акты, указанные в ч. 1 комментируемой статьи, и (или) иным образом подтвердить принятие определенных в ней мер. Необходимо отметить, что направление данных запросов может осуществляться вне контрольно-надзорных мероприятий в рамках реализации полномочий по пресечению и предупреждению возможных нарушений прав субъектов

персональных данных с соблюдением сроков представления запрашиваемых материалов, установленных ч. 4 ст. 20 Закона о персональных данных.

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

4. Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 3 настоящей статьи требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

5. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

6. Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 настоящей статьи, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

7. Проекты нормативных правовых актов, указанных в части 5 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в части 6 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти,

уполномоченным в области противодействия техническим разведкам и технической защиты информации, в порядке, установленном Правительством Российской Федерации. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, об отказе в согласовании проектов решений, указанных в части 6 настоящей статьи, должно быть мотивированным.

8. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

9. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

10. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

11. Для целей настоящей статьи под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз без-

опасности персональных данных при их обработке в информационных системах персональных данных.

1. Часть 1 рассматриваемой статьи устанавливает обязанность оператора принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. Часть 2 комментируемой статьи определяет условия, при которых обеспечивается безопасность обрабатываемых персональных данных, однако приведенный перечень мер не является закрытым.

В соответствии с п. 1 ч. 2 анализируемой статьи обеспечение безопасности персональных данных достигается определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

> Под **угрозами безопасности персональных данных** понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

Также в комментируемой статье предусмотрена обязанность федеральных органов исполнительной власти, осуществляющих функции по выработке государственной политики и нормативному правовому регулированию в установленной сфере деятельности, органов государственной власти субъектов РФ, Банка России, органов государственных внебюджетных фондов, иных государственных органов определить в положениях нормативных правовых актов угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

Кроме этого, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персо-

нальных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

Проекты вышеуказанных нормативных правовых актов и решений подлежат согласованию в федеральном органе исполнительной власти, уполномоченном в области обеспечения безопасности, и федеральном органе исполнительной власти, уполномоченном в области противодействия техническим разведкам и технической защиты информации.

Согласно п. 2 ч. 2 комментируемой статьи обеспечение безопасности персональных данных достигается применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных.

Мерой обеспечения безопасности персональных данных является применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации (п. 3 ч. 1 Закона о персональных данных).

Порядок и условия проведения процедуры оценки соответствия регулируются Федеральным законом от 27.12.2002 № 184-ФЗ «О техническом регулировании».

В п. 4–9 ч. 2 рассматриваемой статьи установлено, что обеспечение безопасности персональных данных достигается:

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер по его обнаружению и пресечению;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а

также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

В соответствии с п. 17 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства РФ от 01.11.2012 № 1119, контроль за выполнением указанных требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Порядок лицензирования деятельности по технической защите конфиденциальной информации установлен Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства РФ от 03.02.2012 № 79.

3. Часть 3 комментируемой статьи закрепляет за Правительством РФ с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных право устанавливать:

- уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных. Данные угрозы перечислены в п. 6 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства РФ от 01.11.2012 № 1119;
- требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Пунктами 8–12 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства РФ от 01.11.2012 № 1119, определены четыре уровня защищенности персональных данных при их обработке в информационных системах и условия их разграничения.

⇨ Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа, и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;
- для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает специальные категории персональных данных более чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора.

⇨ Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа, и информационная система обрабатывает общедоступные персональные данные;
- для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает биометрические персональные данные;
- для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает общедоступные персональные данные более чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора;

- для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает иные категории персональных данных более чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает специальные категории персональных данных более чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора.

⇨ Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает биометрические персональные данные;
- для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает иные категории персональных данных более чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора.

⇨ Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает общедоступные персональные данные;
- для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора.

Пункты 12, 13 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства РФ от 01.11.2012 № 1119, определяют требования, необходимые для обеспечения защищенности персональных данных при их обработке в информационных системах согласно соответствующим уровням.

Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных утверждены постановлением Правительства РФ от 06.07.2008 № 512.

4. Часть 8 рассматриваемой статьи возлагает полномочия по контролю и надзору за выполнением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в государственных информационных системах на федеральные органы исполнительной власти в области обеспечения безопасности, в области противодействия техническим разведкам и технической защите информации в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

Согласно Федеральному закону «О Федеральной службе безопасности», п. 1 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента РФ от 11.08.2003 № 960, федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, является ФСБ России.

В соответствии с п. 1 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента РФ от 16.08.2004 № 1085, федеральным органом исполнительной власти,

уполномоченным в области противодействия техническим разведкам и технической защиты информации, является ФСТЭК России.

Статья 20. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных

(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)

1. Оператор обязан сообщить в порядке, предусмотренном статьей 14 настоящего Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 настоящего Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

3. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

4. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

1. Комментируемая статья регулирует вопросы, связанные с обязанностями оператора, возникающими у него в момент обращения субъекта персональных данных или его представителя либо получения от них запроса. При поступлении данного запроса оператор обязан сообщить информацию о наличии персональных данных в отношении субъекта персональных данных, обратившегося к оператору лично или через представителя, и (или) обеспечить возможность ознакомления с этими персональными данными.

Информация предоставляется в той же форме, в какой получен запрос, если иное не предусмотрено законодательством или не указано в обращении заявителя, при этом она не должна содержать персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Срок предоставления информации при направлении запроса определен в течение 30 дней с даты его получения.

2. В соответствии с ч. 2 анализируемой статьи оператор вправе ограничить право субъекта персональных данных на доступ к его персональным данным в соответствии с федеральными законами (ч. 8 ст. 14 комментируемого закона). К таким ограничениям относятся случаи, когда обработка персональных данных осуществляется в целях обороны страны, безопасности государства и охраны правопорядка, в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, а также когда доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц и др.

В случае принятия оператором решения об отказе в предоставлении сведений в адрес субъекта персональных данных должен быть направлен мотивированный ответ, содержащий ссылку на правовое основание отказа.

3. Часть 3 рассматриваемой статьи регулирует обязанности оператора, связанные с правом субъекта персональных данных (его представителя) на ознакомление с персональными данными и возможными последствиями реализации субъектом своего права требовать от оператора уточнения либо уничтожения своих персональных данных в случае их недостоверности, неактуальности, неточности.

Право ознакомления с персональными данными, относящимися к этому субъекту персональных данных, предоставляется субъекту персональных данных или его представителю безвозмездно.

Выдачу населению справок о составе семьи и выписок из домовой книги за плату следует расценивать как ограничение права субъекта персональных данных на доступ к своим персональным данным, т.е. как ограничение права граждан на информацию.

См.: Кассационное определение Нижегородского областного суда от 09.08.2011 № 33-8160/2011.

4. Частью 4 ст. 20 Закона о персональных данных установлена обязанность оператора в случае направления Роскомнадзором, являющимся уполномоченным органом по защите прав субъектов персональных данных, запроса о предоставлении данных сообщить необходимую информацию в течение 30 дней с даты получения запроса.

Непредставление, а равно несвоевременное представление запрашиваемой информации влечет административную ответственность, предусмотренную ст. 19.7 КоАП РФ.

Статья 21. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных

(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)

1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование

персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

2. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные дан-

ные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

6. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3–5 настоящей статьи, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

1. Комментируемая статья устанавливает обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных.

Нарушения законодательства, являющиеся предметом рассматриваемой статьи, касаются фактов неправомерной обработки персональных данных, а также случаев обработки оператором неточных персональных данных.

Кроме этого, положениями ст. 21 Закона о персональных данных устанавливается обязанность оператора по принятию мер по уничтожению персональных данных в случае достижения цели обработки или поступления отзыва субъектом персональных данных ранее предоставленного согласия на обработку его персональных данных.

Часть 1 комментируемой статьи предусматривает обязанность оператора блокировать персональные данные в случае поступления обращения или запроса субъекта персональных данных или его представителя, а также запроса уполномоченного органа по защите прав субъектов персональных данных.

При выявлении фактов неправомерной обработки персональных данных блокирование осуществляется только в отношении персональных данных лица, направившего обращение или запрос, на период проведения проверки. Необходимо отметить, что проверка в указанном случае проводится непосредственно самим оператором.

2. Часть 2 анализируемой статьи определяет порядок дальнейших действий оператора в случае подтверждения информации о неточности обрабатываемых персональных данных. При подтверждении факта

неточности обрабатываемых персональных данных оператор обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в течение семи рабочих дней со дня представления таких сведений снять блокирование персональных данных.

3. Часть 3 комментируемой статьи предусматривает дальнейшие действия оператора в случае получения информации о неправомерной обработке персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора. Так, оператор в указанном случае обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных в срок, не превышающий трех рабочих дней с даты выявления неправомерной обработки персональных данных.

В случае если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить данные или обеспечить их уничтожение.

После завершения указанных действий оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган об устранении допущенных нарушений или об уничтожении персональных данных.

Срок информирования субъекта персональных данных действующим законодательством для оператора не установлен. Вместе с тем, исходя из концепции построения рассматриваемой статьи, логично увязывать уничтожение неправомерно обрабатываемых персональных данных с достижением цели их обработки. В связи с этим срок информирования субъекта персональных данных не должен превышать 30 дней с момента уничтожения персональных данных.

4. Последующие положения комментируемой статьи устанавливают условия, при наступлении которых оператор обязан прекратить (принять меры по прекращению (если речь идет об аутсорсинге)) обработку персональных данных.

Указанными условиями являются достижение оператором цели обработки и отзыв субъектом персональных данных ранее представленного согласия на обработку персональных данных.

При достижении цели обработки оператор обязан принять соответствующие меры по прекращению обработки в срок, не превышающий 30 дней. При отсутствии возможности уничтожения персональных данных в указанный срок законодатель предусмотрел продление контрольного срока до шести месяцев при условии блокирования обрабатываемых персональных данных.

Важным исключением в отношении срока исполнения соответствующей обязанности являются положения отдельных федеральных законов. То есть, если оператор достиг цели обработки персональных данных, он вправе осуществлять их дальнейшую обработку в объеме и в сроки, установленные законодательством РФ.

☑ Так, согласно ст. 7 Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» документы, содержащие сведения, указанные в этой статье, и сведения, необходимые для идентификации личности, подлежат хранению не менее пяти лет со дня прекращения отношений с клиентом.

Относительно обязанности оператора в части прекращения обработки персональных данных, в случае отзыва ранее представленного согласия на обработку персональных данных, необходимо отметить, что согласно ст. 9 Закона о персональных данных оператор вправе продолжить обработку персональных данных, в случае отзыва субъектом персональных данных своего согласия по основаниям, предусмотренным п. 2–11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 комментируемого закона.

☑ Так, например, при отзыве заемщиком, имеющим кредиторскую задолженность, своего согласия на обработку персональных данных банк вправе осуществлять обработку его персональных данных до наступления момента прекращения договорных обязательств.

Следует отметить, что уничтожение персональных данных не может носить выборочный характер и должно затрагивать как автоматизированную обработку, так и обработку осуществляемую без использования средств автоматизации.

Факт уничтожения персональных данных может подтверждаться актом, подписанным уполномоченными лицами (лицом) либо комиссией оператора, созданной на постоянной основе.

Справедливо встает вопрос о правомерности включения в этот акт персональных данных лица с целью дальнейшего подтверждения фак-

та их уничтожения. В данном случае необходимо проводить параллели между целями обработки, поскольку включение сведений личного характера в акт об уничтожении персональных данных никоим образом не связано с ранее достигнутой целью обработки. Более того, в целях избежания негативных последствий оператор может воспользоваться методом идентификаторов либо внести в акт сведения в объеме, не позволяющем без дополнительной информации однозначно установить личность конкретного физического лица.

Статья 22. Уведомление об обработке персональных данных

1. Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) обрабатываемых в соответствии с трудовым законодательством; *(п. 1 в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных; *(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

4) сделанных субъектом персональных данных общедоступными; *(п. 4 в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защи-

ты безопасности государства и общественного порядка; *(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства. *(п. 9 введен Федеральным законом от 25.07.2011 № 261-ФЗ)*

3. Уведомление, предусмотренное частью 1 настоящей статьи, направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление должно содержать следующие сведения: *(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

7) описание мер, предусмотренных статьями 18.1 и 19 настоящего Федерального закона, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств; *(п. 7 в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

7.1) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты; *(п. 7.1 введен Федеральным законом от 25.07.2011 № 261-ФЗ)*

8) дата начала обработки персональных данных;

9) срок или условие прекращения обработки персональных данных;

10) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки; *(п. 10 введен Федеральным законом от 25.07.2011 № 261-ФЗ)*

11) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации. *(п. 11 введен Федеральным законом от 25.07.2011 № 261-ФЗ)*

4. Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения, указанные в части 3 настоящей статьи, а также сведения о дате направления указанного уведомления в реестр опе-

раторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

5. На оператора не могут возлагаться расходы в связи с рассмотрением уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также в связи с внесением сведений в реестр операторов.

6. В случае предоставления неполных или недостоверных сведений, указанных в части 3 настоящей статьи, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от оператора уточнения предоставленных сведений до их внесения в реестр операторов.

7. В случае изменения сведений, указанных в части 3 настоящей статьи, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных. *(часть седьмая в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

1. Комментируемая статья раскрывает условия выполнения оператором обязанности по представлению в Роскомнадзор уведомления о намерении осуществлять обработку персональных данных. Порядок, условия и сроки предоставления соответствующей государственной услуги регулируются Административным регламентом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных», утвержденным приказом Минкомсвязи России от 21.12.2011 № 346.

Правовая конструкция ст. 22 Закона о персональных данных относительно уведомления заключается в следующем: уведомление подается оператором во всех случаях, кроме исключений, указанных в ч. 2 комментируемой статьи. При этом надо понимать, что оператор не представляет уведомление только в том случае, если его деятельность полностью подпадает под данные исключения. В обратном случае, даже при наличии одного вида деятельности, не предусмотренного положениями ч. 2 указанной статьи, оператор обязан подать уведомление, содержащее сведения обо всех видах деятельности, связанных с обработкой персональных данных.

2. В соответствии с ч. 2 анализируемой статьи оператор вправе осуществлять обработку персональных данных без уведомления уполномоченного органа в следующих случаях:

- осуществление обработки персональных данных в соответствии с трудовым законодательством. Согласно ст. 86 ТК РФ обработка

персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества. Таким образом, при осуществлении работодателем иных видов деятельности с использованием персональных данных работников, в том числе в рамках зарплатного проекта, сведения об указанных видах деятельности включаются в уведомление;

- получение персональных данных оператором в связи с заключением договора, стороной которого является субъект персональных данных, при условии, что персональные данные:
  - не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных (это значит, что оператор не будет предпринимать действия, направленные на передачу данных определенному кругу лиц или на ознакомление с ними неограниченного круга лиц, в том числе размещение в СМИ, в информационно-телекоммуникационных сетях или предоставление доступа к данным иным возможным способом);
  - используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных. Несоблюдение указанных условий влечет за собой представление уведомления (см., например, решение Арбитражного суда Ставропольского края от 20.09.2010 № А63-6610/2010);
- осуществление обработки персональных данных без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами РФ, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Обработка персональных данных без использования средств автоматизации осуществляется в соответствии с Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства РФ от 15.09.2008 № 687.

Уведомление также можно не подавать, если обработка производится в отношении общедоступных персональных данных, персональных

данных, включающих в себя только фамилии, имена и отчества субъектов персональных данных, персональных данных, необходимых в целях однократного пропуска их субъекта на территорию оператора, персональных данных, включенных в государственные автоматизированные информационные системы и государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка, персональных данных, обрабатываемых в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса.

Относительно обработки персональных данных в государственных автоматизированных информационных системах необходимо учитывать, что исключения распространяются только на те системы, чей статус определен федеральным законом. В иных случаях данная деятельность подлежит уведомлению.

3. Часть 3 комментируемой статьи устанавливает требования к содержанию уведомления. В обязательном порядке подлежат включению следующие сведения:

- наименование (фамилия, имя, отчество), адрес оператора (если оператором является государственный орган, муниципальный орган или юридическое лицо, указываются его полное наименование, адрес (юридический и почтовый, а также контактные данные), идентификационный номер налогоплательщика (необязательное условие). Если оператор имеет филиалы или представительства, не являющиеся обособленными структурными подразделениями, указываются их наименования и адреса. Если оператором является физическое лицо, указываются его фамилия, имя, отчество, адрес (места нахождения, почтовый адрес, контактные данные), данные документа, удостоверяющего личность; идентификационный номер налогоплательщика (необязательное условие));
- цель обработки, правовое основание обработки персональных данных (цель и правовые основания обработки персональных данных должны соответствовать полномочиям оператора, отраженным в уставных документах, федеральных законах и принятых на их основе нормативных правовых актов в части, касающейся компетенции оператора);
- категории персональных данных (персональные данные, биометрические персональные данные, специальные категории персональных данных);

- категории субъектов, персональные данные которых обрабатываются, а также виды отношений с указанными субъектами (в частности, работники, соискатели на вакантные должности, лица, с которыми заключены гражданско-правовые договора, т.п.);
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных (неавтоматизированная обработка персональных данных; исключительно автоматизированная обработка персональных данных с передачей полученной информации по сети или без таковой и смешанная обработка персональных данных);
- описание мер, предусмотренных ст. 18.1 и 19 комментируемого закона, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств (в частности, должны быть указаны класс информационной системы персональных данных; организационные и технические меры, применяемые для защиты персональных данных; сведения об использовании шифровальных (криптографических) средств);
- фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;
- дата начала обработки персональных данных (как правило, это дата начала осуществления оператором деятельности, закрепленная в уставных документах);
- срок или условие прекращения обработки персональных данных (он может быть определен как конкретная дата или основание (условие), наступление которого влечет прекращение обработки персональных данных);
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки (при наличии трансграничной передачи указывается перечень иностранных государств, на территорию которых осуществляется трансграничная передача персональных данных);
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ.

С 1 сентября 2015 г. вступает в силу Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в инфор-

мационно-телекоммуникационных сетях», в соответствии с которым в уведомлении необходимо будет также указывать сведения о месте нахождения базы данных информации, содержащей персональные данные граждан РФ.

Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа на бланке оператора и подписывается уполномоченным лицом. В электронном виде уведомление может быть направлено с использованием ресурсов единого портала государственных и муниципальных услуг или портала персональных данных. Направление уведомления через портал персональных данных после заполнения специальной формы должно соответствовать следующим условиям. После заполнения формы уведомления о намерении осуществлять обработку персональных данных и отправки ее в информационную систему уполномоченного органа по защите прав субъектов персональных данных ее необходимо распечатать, подписать и направить в соответствующий территориальный орган Роскомнадзора по месту регистрации оператора.

4. Уполномоченный орган по защите прав субъектов персональных данных ведет реестр операторов персональных данных. Сведения, содержащиеся в реестре, являются общедоступными, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке.

Порядок и условия внесения сведений в реестр, внесения информации об изменении сведений в ранее представленное уведомление, исключения сведений из реестра устанавливаются Административным регламентом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных», утвержденным приказом Минкомсвязи России от 21.12.2011 № 346.

Статья 22.1. Лица, ответственные за организацию обработки персональных данных в организациях

(введена Федеральным законом от 25.07.2011 № 261-ФЗ)

1. Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных.

2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему.

3. Оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22 настоящего Федерального закона.

4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

1. В ч. 1 комментируемой статьи устанавливается обязанность оператора персональных данных, являющегося юридическим лицом, назначить лицо, ответственное за обработку персональных данных.

2. В ч. 2 анализируемой статьи определяются организационно-правовые условия осуществления деятельности ответственными лицами. Так, лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором. Кроме этого, ответственное за обработку персональных данных лицо подотчетно только исполнительному органу юридического лица.

3. В ч. 3 рассматриваемой статьи содержатся информационные гарантии надлежащего исполнения лицом, ответственным за обработку персональных данных, своих обязательств. Так, оператор персональных данных обязан предоставить ответственному лицу следующие сведения:

- наименование, адрес оператора;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
- описание мер, направленных на обеспечение выполнения оператором обязанностей, предусмотренных Законом о персональных данных, а также мер по обеспечению безопасности персональ-

ных данных при их обработке, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

- фамилию, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;
- дату начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ.

4. В ч. 4 комментируемой статьи устанавливаются основные обязанности лица, ответственного за обработку персональных данных, к которым относятся:

- осуществление внутреннего контроля за соблюдением оператором и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников оператора положений законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществления контроля за приемом и обработкой таких обращений и запросов.

Глава 5
Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований настоящего Федерального закона

Статья 23. Уполномоченный орган по защите прав субъектов персональных данных

1. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

2. Уполномоченный орган по защите прав субъектов персональных данных рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение.

3. Уполномоченный орган по защите прав субъектов персональных данных имеет право:

1) запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

2) осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

3) требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

4) принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона;

5) обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде; *(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

5.1) направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, сведения, указанные в пункте 7 части 3 статьи 22 настоящего Федерального закона; *(п. 5.1 введен Федеральным законом от 25.07.2011 № 261-ФЗ)*

6) направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

7) направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

8) вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;

9) привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

4. В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

5. Уполномоченный орган по защите прав субъектов персональных данных обязан:

1) организовывать в соответствии с требованиями настоящего Федерального закона и других федеральных законов защиту прав субъектов персональных данных;

2) рассматривать жалобы и обращения граждан или юридических лиц по вопросам, связанным с обработкой персональных данных, а также принимать в пределах своих полномочий решения по результатам рассмотрения указанных жалоб и обращений;

3) вести реестр операторов;

4) осуществлять меры, направленные на совершенствование защиты прав субъектов персональных данных;

5) принимать в установленном законодательством Российской Федерации порядке по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, или федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, меры по приостановлению или прекращению обработки персональных данных;

6) информировать государственные органы, а также субъектов персональных данных по их обращениям или запросам о положении дел в области защиты прав субъектов персональных данных;

7) выполнять иные предусмотренные законодательством Российской Федерации обязанности.

5.1. Уполномоченный орган по защите прав субъектов персональных данных осуществляет сотрудничество с органами, уполномоченными по защите прав субъектов персональных данных в иностранных государствах, в частности международный обмен информацией о защите прав субъектов персональных данных, утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных. *(часть пятая.1 введена Федеральным законом от 25.07.2011 № 261-ФЗ)*

6. Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.

7. Уполномоченный орган по защите прав субъектов персональных данных ежегодно направляет отчет о своей деятельности Президенту Российской Федерации, в Правительство Российской Федерации и Федеральное Собрание Российской Федерации. Указанный отчет подлежит опубликованию в средствах массовой информации.

8. Финансирование уполномоченного органа по защите прав субъектов персональных данных осуществляется за счет средств федерального бюджета.

9. При уполномоченном органе по защите прав субъектов персональных данных создается на общественных началах консультативный совет, порядок формирования и порядок деятельности которого определяются уполномоченным органом по защите прав субъектов персональных данных.

1. В ч. 1 комментируемой статьи установлен уполномоченный орган по защите прав субъектов персональных данных в Российской Федерации (далее — уполномоченный орган).

Согласно положениям Конвенции 1981 года стороны обязуются назначить один или несколько органов, компетентных в области защиты персональных данных в целях, определенных в этой конвенции.

Каждое государство, являющееся стороной Конвенции 1981 года, учредило уполномоченный орган в области персональных данных на своей территории[1]. При этом положения указанной конвенции не предъявляют обязательных требований к таким уполномоченным органам.

В странах Европейского союза и странах — участницах Конвенции 1981 года обычно уполномоченный орган — это отдельная структура, наделенная надзорными и регулирующими полномочиями в области

[1] Список сайтов уполномоченных органов в сфере персональных данных, как являющихся участниками Конвенции 1981 года, так и не являющихся таковыми, размещен на сайте: http://www.dataprotection.ie/ViewDoc.asp?fn=%2Fdocuments%2Feuropean%2F6f%2Ehtm&CatID=37&m=i.

защиты персональных данных и прав граждан как субъектов персональных данных, возглавляемая руководителем (директором, комиссаром, генеральным инспектором, уполномоченным), назначаемым президентом или парламентом не более чем на два срока по пять лет, курируемая министерством юстиции (либо министерством внутренних дел, как, например, в Польше).

Вместе с тем в рамках диалога о присоединении к Дополнительному протоколу к Конвенции 1981 года от 8 ноября 2001 г. (Российская Федерация этот протокол не ратифицировала), а также модернизированной Конвенции 1981 года к уполномоченным органам предъявляются требования относительно независимости данных органов.

Четких критериев определения независимости уполномоченного органа указанные документы не содержат. Однако понимание независимости имеет принципиальное значение для подписания как Дополнительного протокола к Конвенции 1981 года, так и ряда других международных соглашений, затрагивающих вопросы персональных данных.

Под независимостью в пояснительной записке к Дополнительному протоколу к Конвенции 1981 года понимается функциональная независимость уполномоченного органа от других органов исполнительной власти. Это соответствует независимости Роскомнадзора как органа исполнительной власти согласно действующей системе организации органов государственной власти в Российской Федерации.

Однако, например, Объединенной наблюдательной комиссией Европола предлагается рассматривать понятие независимости уполномоченного органа по защите персональных данных с учетом решений Суда Европейского союза по делам № C-518/07 «Европейская комиссия против Федеративной Республики Германии» и № C-614/10 «Европейская комиссия против Австрийской Республики».

Указанные решения Суда Европейского союза были приняты в связи с отказом государств — членов Европейского союза от исполнения ст. 28 (1) Директивы Европейского парламента Совета Европейского союза от 24.10.1995 № 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» (далее — Директива). При этом в п. 18 решения Суда Европейского союза № C-518/07 особо отмечено, что даже в Директиве отсутствует определение «полной независимости», в связи с чем суд сформулировал представление о понятии «независимость» исходя из общего (обычного) толкования статуса государственного органа, характерного для Европейского союза.

Учитывая, что Российская Федерация не является членом Европейского союза, а также не принимала на себя обязательств по исполнению Директивы, решения Суда Европейского союза в отношении Австрии и Германии не могут быть перенесены на отношения Европейского союза с Российской Федерацией при заключении соглашений, также Российская Федерация, как суверенное государство, не может руководствоваться при принятии решений внутренними судебными актами Европейского союза.

В ч. 1 ст. 23 Закона о персональных данных определяется основная функция уполномоченного органа — обеспечение контроля и надзора за соответствием обработки персональных данных требованиям комментируемого закона.

Следует отметить, что Указом Президента РФ от 09.03.2004 № 314 «О системе и структуре федеральных органов исполнительной власти» было установлено, что в системе федеральных органов исполнительной власти контрольно-надзорные функции в сферах деятельности осуществляются исключительно федеральными службами. Таким образом, подобные полномочия не могут быть возложены на федеральные министерства, федеральные агентства.

Функции уполномоченного органа комментируемая часть статьи закрепила за федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере информационных технологий и связи. Таким органом исполнительной власти является Роскомнадзор, который осуществляет полномочия как непосредственно, так и через свои территориальные органы — управления Роскомнадзора в федеральных округах и субъектах РФ.

Аналогичная норма о статусе Роскомнадзора в качестве уполномоченного органа содержится также в Положении о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденном постановлением Правительства РФ от 16.03.2009 № 228. Кроме этого, в названном положении также закреплено полномочие Роскомнадзора по осуществлению государственного контроля и надзора за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных.

Государственный контроль (надзор) представляет собой деятельность органов государственной власти, направленную на предупреждение, выявление и пресечение нарушений законодательства РФ. Данная деятельность органа власти выражается в осуществлении определенных мероприятий по контролю, например, в проверке деятельности юри-

дического лица или органа местного самоуправления, систематическом наблюдении за исполнением обязательных требований законодательства и др.

Отношения в области организации и осуществления государственного контроля (надзора) регулируются Законом о защите прав юридических лиц и индивидуальных предпринимателей при осуществлении контроля, а также Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» (в части организации контроля и надзора за деятельностью органов местного самоуправления и должностных лиц местного самоуправления).

В связи с этим реализация Роскомнадзором полномочий по контролю (надзору) за соответствием обработки персональных данных требованиям законодательства РФ в сфере персональных данных осуществляется в отношении операторов персональных данных, являющихся юридическими лицами, индивидуальными предпринимателями, а также органами местного самоуправления и должностными лицами местного самоуправления, в порядке, определенном названными законами.

Так, Роскомнадзор и его территориальные органы проводят в отношении операторов персональных данных документарные и выездные плановые и внеплановые проверки деятельности.

Плановые проверки деятельности юридических лиц и индивидуальных предпринимателей проводятся не чаще чем один раз в три года органами Роскомнадзора на основании приказа Роскомнадзора или его территориального органа в соответствии с ежегодным сводным планом проведения плановых проверок, утвержденным Генпрокуратурой России.

В соответствии с ч. 7 ст. 9 Закона о защите прав юридических лиц и индивидуальных предпринимателей при осуществлении контроля ежегодный сводный план проведения плановых проверок размещается на сайте Генпрокуратуры России (*www.genproc.gov.ru*) в срок до 31 декабря года, предшествующего проведению проверок.

Внеплановые проверки деятельности юридических лиц и индивидуальных предпринимателей проводятся органами Роскомнадзора на основании приказа Роскомнадзора или его территориального органа, изданного в соответствии с поручениями Президента РФ, Правительства РФ и на основании требования прокурора о проведении внеплановой проверки в рамках надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

Таким образом, положения Закона о защите прав юридических лиц и индивидуальных предпринимателей при осуществлении контроля не предоставляют Роскомнадзору полномочий по организации проведения внеплановых проверок деятельности операторов персональных данных только на основании решения Роскомнадзора в связи с поступившим обращением или жалобой на нарушение прав субъекта персональных данных.

Конкретные сроки и последовательность действий (административных процедур) Роскомнадзора и его территориальных органов при организации и проведении мероприятий по контролю установлены Административным регламентом исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, утвержденным приказом Минкомсвязи России от 14.11.2011 № 312.

Плановые проверки деятельности органов местного самоуправления и должностных лиц местного самоуправления проводятся органами Роскомнадзора на основании ежегодных планов проведения проверок, согласованных прокуратурой субъекта РФ. Ежегодные планы проверок согласно ч. 2.5 ст. 77 Федерального закона «Об общих принципах организации местного самоуправления в Российской Федерации» подлежат размещению на официальных сайтах как прокуратуры субъекта РФ, так и соответствующего территориального органа Роскомнадзора не позднее 1 ноября года, предшествующего году проведения проверок.

Внеплановые проверки деятельности органов местного самоуправления и должностных лиц местного самоуправления, так же как и субъектов предпринимательства, проводятся органами Роскомнадзора на основании приказа Роскомнадзора или его территориального органа, изданного в соответствии с поручениями Президента РФ, Правительства РФ и на основании требования прокурора о проведении внеплановой проверки в рамках надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

2. В ч. 2 анализируемой статьи установлены полномочия Роскомнадзора по рассмотрению обращений субъектов персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки, а также по принятию в отношении таких обращений соответствующих решений.

При этом ч. 2 комментируемой статьи не следует соотносить с Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации», регламентирующим отношения, связанные с реализацией гражданином РФ права на обращение в государственные органы и органы местного самоуправления. Так, под обращением в смысле названного закона понимается обращение гражданина, выраженное в следующих формах:

- предложения по совершенствованию законов и иных нормативных правовых актов, деятельности государственных органов и органов местного самоуправления, развитию общественных отношений, улучшению социально-экономической и иных сфер деятельности государства и общества;
- заявления гражданина о содействии в реализации его конституционных прав и свобод или конституционных прав и свобод других лиц, либо сообщения о нарушении законов и иных нормативных правовых актов, недостатках в работе государственных органов, органов местного самоуправления и должностных лиц, либо критики деятельности указанных органов и должностных лиц;
- жалобы гражданина с просьбой о восстановлении или защите его нарушенных прав, свобод или законных интересов либо прав, свобод или законных интересов других лиц.

Вместе с тем в рассматриваемый перечень обращений не входят обращения граждан о соответствии содержания персональных данных и способов их обработки целям их обработки. Вопросы, изложенные в обращении субъекта персональных данных в смысле ч. 2 ст. 23 Закона о персональных данных, условно можно отнести к просьбе заявителя произвести экспертную оценку соответствия содержания и способа обработки персональных данных целям их обработки, без соответствующей жалобы, заявления или предложения гражданина. Следовательно, установленное в ч. 2 комментируемой статьи полномочие Роскомнадзора не должно согласовываться с положениями Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации» в силу уникальности вопроса, который подлежит разрешению в связи с рассмотрением данного обращения.

Кроме этого, такая экспертная оценка может быть произведена при наличии в обращении субъекта персональных данных достоверных материалов, в которых содержатся информация о порядке обработки персональных данных оператором, о цели такой обработки и иная ин-

формация, необходимая для производства оценки соответствия содержания и объема обрабатываемых персональных данных целям такой обработки.

В рамках рассмотрения Закона о персональных данных требует уяснения вопрос аутентификации субъекта персональных данных, обратившегося в Роскомнадзор с обращением, как лица, чьи персональные данные являются предметом обращения.

Учитывая положение ч. 2 ст. 23 комментируемого закона, согласно которому рассматриваемое обращение может быть подано субъектом персональных данных, уполномоченному органу при получении такого обращения необходимо убедиться, что заявитель обращается с просьбой в отношении своих персональных данных, а не персональных данных третьих лиц, например, родственников, друзей и т.д. Представляется, что обращения в отношении третьих лиц могут быть поданы в Роскомнадзор исключительно на основании доверенности субъекта персональных данных.

Вместе с тем ни вопросы идентификации заявителя, ни порядка подачи и сроков рассмотрения обращений субъектов персональных данных в настоящее время не урегулированы законодательством в области персональных данных. Представляется, что эти вопросы должны стать предметом регулирования отдельного нормативного правового акта.

Вопрос принятия уполномоченным органом соответствующих решений в отношении рассмотренного обращения также требует дополнительной регламентации. В настоящее время ч. 2 анализируемой статьи не указывает, в чем эти решения могут выражаться. Например, вправе ли уполномоченный орган принять решение о применении мер реагирования при определении, что содержание и способы обработки персональных данных не соответствуют целям обработки, учитывая, что обращение заявителя не содержит жалобы на нарушение его прав и просьбу об их восстановлении. В данном случае уполномоченному органу следует ограничиться принятием решения о предоставлении заявителю сообщения, заключения или иного документа, констатирующего наличие в действиях оператора признаков нарушения законодательства о персональных данных. Впоследствии данное сообщение (заключение) может быть использовано субъектом персональных данных для обращения в суд за защитой своих прав и интересов, за возмещением убытков и компенсацией морального вреда, причиненных субъекту персональных данных.

Таким образом, недостаточная регламентация ч. 2 ст. 23 Закона о персональных данных породила правовой вакуум в вопросах порядка рассмотрения Роскомнадзором обращений субъектов персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки.

3. В ч. 3 комментируемой статьи закреплены права уполномоченного органа, представляющие собой отдельные властные полномочия, направленные на защиту прав субъектов персональных данных.

Следует заметить, что на практике ввиду отсутствия норм, связанных с установлением порядка реализации данных полномочий, а также корреспондирующих норм в другие законодательные акты и по иным причинам не все права уполномоченного органа, определенные в ч. 3 анализируемой статьи, могут быть фактически реализованы (п. 4, 6, 8 ч. 3 ст. 23 Закона о персональных данных).

Пункт 1 ч. 3 ст. 23 комментируемого закона устанавливает право уполномоченного органа запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, а также право безвозмездно получать такую информацию. Данные права реализуются Роскомнадзором посредством направления оператору персональных данных требования о предоставлении информации в отношении обработки персональных данных конкретного лица или группы лиц в связи с рассмотрением обращений граждан с жалобами на нарушения их прав и законных интересов.

Указанному праву уполномоченного органа соответствует установленная в ч. 4 ст. 20 рассматриваемого закона обязанность оператора персональных данных сообщить в уполномоченный орган по запросу этого органа необходимую информацию в течение 30 дней с даты получения такого запроса (*см. комментарий к ст. 20 Закона о персональных данных*).

За непредставление информации по запросу уполномоченного органа или несвоевременное ее представление, а также представление информации в неполном объеме или в искаженном виде российским законодательством предусмотрена административная ответственность, назначаемая по ст. 19.7 КоАП РФ «Непредставление сведений (информации)».

Направление подобных запросов не следует рассматривать в качестве проведения внеплановой документарной проверки, в соответствии с требованиями Закона о защите прав юридических лиц и индивидуальных предпринимателей при осуществлении контроля.

Вместе с тем в практике деятельности Роскомнадзора указанное право уполномоченного органа по направлению оператору запроса об истребовании информации о порядке обработки персональных данных

в ряде случаев рассматривалось как неправомерное проведение внеплановой документарной проверки.

☑ Например, прокуратурой г. Сарапула Удмуртской Республики было вынесено постановление об административном правонарушении от 04.04.2014 в отношении главного специалиста-эксперта Управления Роскомнадзора по Удмуртской Республике. Основанием для вынесения постановления послужило направление Управлением Роскомнадзора по Удмуртской Республике в адрес оператора персональных данных требования о предоставлении информации (сведений) и изучение информации (сведений), содержащейся в представленных оператором документах, а также сведений, представленных оператором в письменном ответе, что было расценено прокуратурой как проведение внеплановой документарной проверки в соответствии с Законом о защите прав юридических лиц и индивидуальных предпринимателей при осуществлении контроля.

Следовательно, прокуратурой был сделан вывод, что должностное лицо, требующее информацию в соответствии с п. 1 ч. 3 ст. 23 Закона о персональных данных, совершает правонарушение, предусмотренное ч. 1 ст. 19.6.1 КоАП РФ (несоблюдение должностными лицами органов государственного контроля (надзора) требований законодательства о государственном контроле (надзоре)), поскольку отсутствовали основания для проведения проверки, предусмотренные Законом о защите прав юридических лиц и индивидуальных предпринимателей при осуществлении контроля, а приказ на ее проведение не составлялся.

Вместе с тем установленный Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации» порядок рассмотрения обращений граждан распространяется на все обращения граждан, за исключением обращений, которые подлежат рассмотрению в порядке, установленном федеральными конституционными законами и иными федеральными законами.

Несмотря на то что согласно ст. 11 Закона о защите прав юридических лиц и индивидуальных предпринимателей при осуществлении контроля в содержании предмета документарной проверки деятельность по рассмотрению обращений граждан не предусмотрена, данный порядок рассмотрения обращений граждан установлен п. 1 ч. 3 ст. 23 комментируемого закона, согласно которому уполномоченный орган по защите прав субъектов персональных данных вправе запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию.

Таким образом, учитывая, что Законом о персональных данных на Роскомнадзор возложена обязанность по рассмотрению жалоб и обращений граждан или юридических лиц по вопросам, связанным с обработкой персональных данных, принятию решений по результатам рассмотрения указанных жалоб и обращений, а также принимая во внимание, что согласно ч. 2 ст. 10 Закона о защите прав юридических лиц и индивидуальных предпринимателей при осуществлении контроля такие обращения не являются основанием для проведения внеплановой проверки, реализация полномочий Роскомнадзора по запросу информации у физических или юридических лиц при рассмотрении жалоб и обращений граждан или юридических лиц по вопросам, связанным с обработкой персональных данных, не должна регулироваться положениями Закона о защите прав юридических лиц и индивидуальных предпринимателей при осуществлении контроля.

Следует отметить, что такое понимание права уполномоченного органа по направлению запросов об истребовании информации у оператора также соответствует позиции Генпрокуратуры России, изложенной в письме от 13.10.2014, в отношении направления уполномоченным органом запросов об истребовании у операторов персональных данных сведений о наличии (отсутствии) согласия субъектов персональных данных на обработку.

Так, согласно позиции Генпрокуратуры России оператор персональных данных в соответствии со ст. 9 и 20 Закона о персональных данных обязан сообщить в уполномоченный орган по запросу этого органа необходимую информацию, а также предоставить доказательства получения согласия субъекта персональных данных на обработку его персональных данных. С учетом полномочий Роскомнадзора по защите прав субъектов персональных данных служба вправе запрашивать сведения о наличии согласия субъекта персональных данных на обработку персональных данных вне рамок мероприятий, проводимых в соответствии с Законом о защите прав юридических лиц и индивидуальных предпринимателей при осуществлении контроля.

Пункт 2 ч. 3 комментируемой статьи устанавливает право уполномоченного органа осуществлять проверку сведений, содержащихся в уведомлении оператора персональных данных об обработке персональных данных (*см. комментарий к ст. 22 Закона о персональных данных*). Порядок осуществления такой проверки не регламентирован нормативными правовыми актами.

Вместе с тем отдельные административные процедуры реализации полномочия Роскомнадзора по проверке сведений, содержащихся в уведомлении оператора персональных данных, содержатся в Административном регламенте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных», утвержденном приказом Роскомнадзора от 21.12.2011 № 346.

Согласно положениям указанного административного регламента проверка сведений, содержащихся в уведомлении оператора об обработке персональных данных, производится на этапе подачи данного уведомления в Роскомнадзор для включения сведений об операторе в реестр операторов персональных данных либо в случае направления в Роскомнадзор информационного письма о необходимости актуализации сведений об операторе персональных данных, содержащихся в реестре оператора персональных данных.

Несмотря на то что в этом административном регламенте нет указания на необходимость проведения систематических проверок сведений, содержащихся в уведомлении оператора после внесения данных сведений в реестр операторов, Роскомнадзором может быть поставлен вопрос об исключении сведений об операторе из реестра в случае выявления недостоверной информации, предоставленной оператором.

Кроме этого, проверка сведений, содержащихся в уведомлении, предполагает обязанность уполномоченного органа по проверке достоверности и актуальности предоставленных оператором сведений, например, об адресе места нахождения оператора, о производстве оператором трансграничной передачи персональных данных и проч. В связи с этим п. 2 ч. 3 комментируемой статьи предоставляет уполномоченному органу право привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий.

Пункт 3 ч. 3 анализируемой статьи устанавливает право уполномоченного органа требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных (*см. комментарий к ст. 21 Закона о персональных данных*).

Пункт 4 ч. 3 рассматриваемой статьи устанавливает право уполномоченного органа принимать в установленном законодательством РФ порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований комментируемого закона. Реализация этого полномочия Роскомнадзора

не урегулирована российским законодательством, в связи с чем данное право не может практически применяться в деятельности уполномоченного органа по защите прав субъектов персональных данных. Так, ни законодательными актами, ни подзаконными нормативными правовыми актами не установлены порядок, основания, сроки приостановления и прекращения обработки персональных данных.

Вместе с тем представляется, что правила, в соответствии с которыми будут осуществляться приостановление и прекращение обработки персональных данных, в целях устранения нарушений законодательства о персональных данных, а также в случаях уточнения персональных данных субъектом персональных данных или отзыва согласия субъекта персональных данных на обработку персональных данных должны стать предметом регулирования отдельного постановления Правительства РФ.

⇨ **Приостановление обработки персональных данных** представляет собой временную меру, направленную на защиту персональных данных как конкретного субъекта, так и неопределенного круга субъектов, данные о которых обрабатываются оператором. Можно предположить, что такая мера должна быть реализована, когда право обработки персональных данных оператором является спорным или имеются основания полагать, что оператор обрабатывает данные с нарушением законодательства о персональных данных, однако в случае устранения таких нарушений или установления, что в действиях оператора отсутствуют признаки нарушений правил обработки, обработка может быть возобновлена. При этом основанием для приостановления обработки данных может являться требование уполномоченного органа, например, в случае направления искового заявления в суд в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц.

⇨ **Прекращение обработки персональных данных** представляет собой меру, направленную на защиту прав субъектов персональных данных и выраженную в требовании прекратить обработку данных, осуществляемую с нарушением законодательства о персональных данных. Основанием для прекращения обработки может являться как вступившее в законную силу судебное решение, так и требование уполномоченного органа. Требование уполномоченного органа может быть вынесено оператору в случае установления, что оператор персональных данных не прекратил обработку персональных данных в связи с отзывом субъектом персональных данных своего согласия на обработку. Исполнение вступившего в законную силу

решения суда о прекращении обработки персональных данных осуществляется в порядке, установленном законодательством об исполнительном производстве.

Пункт 5 ч. 3 комментируемой статьи устанавливает право Роскомнадзора как уполномоченного органа обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде. Указанное право реализуется в порядке, определенном гражданским процессуальным законодательством РФ.

На практике право уполномоченного органа на обращение в суд в защиту прав третьих лиц реализовывается в связи с нарушением законодательства о персональных данных иностранными и российскими интернет-ресурсами.

В соответствии с ч. 6.1 ст. 29 ГПК РФ иски о защите прав субъекта персональных данных, в том числе о возмещении убытков и (или) компенсации морального вреда, могут предъявляться по выбору истца как в суд по месту жительства ответчика, так и в суд по месту жительства истца. Следует отметить, что ст. 29 ГПК РФ была дополнена ч. 6.1 лишь в 2013 году.

До внесения указанного дополнения подать иск в защиту прав субъекта персональных данных можно было по общему основанию только в суд, по месту нахождения ответчика. Данное положение усложняло процедуру защиты субъекта персональных данных в условиях трансграничности информационных потоков в Интернете. Защищать права и интересы при трансграничной передаче пользователю приходилось в иностранном суде, в случае, если пользователь найдет с кем судиться, установит ответчика — владельца интернет-ресурса.

Кроме этого, споры решались по законам страны подачи иска, в которой могло отсутствовать законодательство в области защиты персональных данных, либо им не обеспечивалась адекватная защита персональных данных граждан. Таким образом, судебный процесс становился трудоемкой, длительной и дорогостоящий процедурой с непредсказуемым результатом.

После внесения указанного дополнения в ГПК РФ процедура защиты прав субъекта персональных данных упростилась. Появилась возможность подать иск в суд по месту жительства истца и впоследствии исполнить решение суда в отношении сайтов в Интернете в рамках процедуры по ограничению доступа к сайтам. Кроме этого, стали возможными взыскание убытков и компенсация морального вреда с от-

ветчика посредством экзекватуры — процедуры признания и принудительного исполнения на территории одной страны судебного решения, вынесенного в другой стране. Однако экзекватура также представляет собой сложный и трудоемкий механизм исполнения судебного решения.

Принцип верховенства государства на своей территории в отношении осуществления правосудия свидетельствует о том, что в каждом государстве исполнению подлежат, как правило, лишь решения собственных судов. Решения иностранных судов не будут иметь юридической силы, равно как не имеют юридической силы и исполнительные документы иностранных государств на территории какого-либо государства.

Вместе с тем процедура признания и принудительного исполнения судебного решения фактически позволяет признать юридическую силу за судебным решением иностранного государства.

Законодательство иностранных государств по-разному определяет возможность признания и исполнения судебного решения на своей территории.

Так, экзекватура судебных решений зависит в ряде государств от наличия международного договора или обеспечения взаимности при исполнении решений. В некоторых странах признание и исполнение решений связано лишь с соблюдением обязательных условий признания, определенных национальным законодательством.

Согласно ч. 1 ст. 409 ГПК РФ, ч. 1 ст. 241 АПК РФ решения иностранных судов на территории Российской Федерации признаются и исполняются, если это предусмотрено международным договором.

> **Таким образом**, если между Российской Федерацией и иностранным государством не заключено соответствующее международное соглашение, то судебные решения данного государства не будут исполняться на территории России, равно как и не будет оснований для принудительного исполнения на территории иностранного государства решений суда Российской Федерации.

Объем правовой помощи, установленный соответствующим международным договором, может включать в себя возможность принудительного исполнения судебных решений лишь определенной категории дел, рассматриваемых судами.

Следует отметить, что в ряде случаев международные договоры позволяют взыскать моральный или имущественный вред. В то же время ни один международный договор, устанавливающий процедуру

экзекватуры, не предусматривает возможность принудительного исполнения судебного решения в части ограничения доступа или блокировки информации в Интернете. Таким образом, ограничить доступ к незаконно размещенным персональным данным, в случае если владелец интернет-ресурса находится за границей, либо прекратить делегирование доменного имени данному ресурсу не представляется возможным.

Положения ч. 6.1 ст. 29 ГПК РФ позволили Роскомнадзору как уполномоченному органу при подаче судебных исков в защиту прав субъектов персональных данных в Интернете в последующем ограничить доступ к сайтам, нарушающим законодательство о персональных данных и не реагирующим на требования Роскомнадзора об удалении противоправно размещенных данных.

Так, Роскомнадзор и его территориальные органы, реализуя право выступать в качестве истца в защиту интересов указанных субъектов, в 2014 году подали исковые заявления в отношении интернет-ресурсов, осуществляющих незаконную обработку персональных данных. Судами в пользу Роскомнадзора вынесены решения о принятии обеспечительных мер по исковым заявлениям в части блокировки сайтов в связи с распространением персональных данных до вынесения судебного решения по делу[1].

Пункт 5.1 ч. 3 комментируемой статьи устанавливает право Роскомнадзора направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности сведения о:

- мерах, направленных на обеспечение выполнения оператором обязанностей, предусмотренных анализируемым законом (*см. комментарий к ст. 18.1 Закона о персональных данных*);
- мерах по обеспечению безопасности персональных данных при их обработке (*см. комментарий к ст. 19 Закона о персональных данных*);
- наличии шифровальных (криптографических) средств и наименования этих средств.

---

[1] См.: Новости на сайте Роскомнадзора от 29.08.2014 (http://pd.rkn.gov.ru/press-service/subject1/news4195.htm); Роскомнадзор начал зачистку сайтов интим-услуг (http://izvestia.ru/news/576208).

Федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, является ФСБ России, а органом, уполномоченным в области противодействия техническим разведкам и технической защиты информации, — ФСТЭК России.

Пункт 6 ч. 3 рассматриваемой статьи устанавливает право Роскомнадзора как уполномоченного органа направлять в орган, осуществляющий лицензирование деятельности организаций, обрабатывающих персональные данные, заявление о принятии мер по приостановлению действия или аннулированию соответствующей лицензии. При этом обязательным условием такой лицензии на осуществление деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных.

Однако в настоящее время указанное право уполномоченного органа по защите прав субъектов персональных данных не может быть реализовано на практике ввиду отсутствия норм, связанных с установлением порядка реализации указанного полномочия, а также корреспондирующих норм в иные законодательные акты, в том числе в Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».

В связи с этим в практической деятельности Роскомнадзора указанное полномочие не реализуется. Во-первых, отсутствуют лицензии с условием запрета на передачу персональных данных третьим лицам без согласия субъекта персональных данных. Во-вторых, отсутствует порядок по приостановлению действия или аннулированию соответствующей лицензии по заявлению Роскомнадзора.

Для реализации рассматриваемого полномочия необходимо законодательно закрепить наличие в определенных лицензиях обязательного условия о запрете на передачу персональных данных третьим лицам без согласия субъекта персональных данных.

Пункт 7 ч. 3 ст. 23 Закона о персональных данных устанавливает право Роскомнадзора направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью.

Если в ходе проверки сотрудники Роскомнадзора выявят признаки преступления, они передадут соответствующие материалы в правоохранительные органы. При этом подследственность уголовных дел определяется ст. 151 УПК РФ.

Следует отметить, что в настоящее время меры ответственности за нарушение законодательства о защите персональных данных «разбросаны» по различным отраслям законодательства — административному, уголовному, трудовому. При этом ни в одной отрасли они пока не систематизированы должным образом, не выделены в отдельную группу как правонарушения, посягающие на конкретный вид общественных отношений.

Например, в Уголовном кодексе РФ отсутствуют специальные составы преступлений, предусматривающие ответственность за нарушения в сфере персональных данных. Вместе с тем отдельные статьи этого кодекса предусматривают ответственность за противоправные деяния с использованием персональных данных, либо объект посягательства которых тесно связан с персональными данными. К таким преступлениям можно отнести следующие составы.

⇨ Статья 137 УК РФ предусматривает ответственность за нарушение неприкосновенности частной жизни. Несмотря на то что частная жизнь и персональные данные не являются тождественными понятиями, персональные данные могут выступать неотъемлемой частью сведений о частной жизни, личной или семейной тайне. В связи с этим незаконная обработка персональных данных, выраженная в противоправном сборе, распространении или ином использовании персональных данных, может нарушить частную жизнь, личную и семейную тайну.

⇨ Статья 272 УК РФ устанавливает ответственность за неправомерный доступ к компьютерной информации. Так, в случае если персональные данные являются компьютерной информаций, ставшей предметом преступления, то данное нарушение будет являться уголовно наказуемым деянием.

⇨ Согласно ч. 2 ст. 173.2 УК РФ преступлением является использование персональных данных, полученных незаконным путем, если эти деяния совершены для внесения в единый государственный реестр юридических лиц сведений о подставном лице.

⇨ К категории преступлений, связанных с нарушением прав субъектов персональных данных, можно также отнести состав, установленный в ст. 155 УК РФ «Разглашение тайны усыновления (удочерения)».

Пункт 8 ч. 3 комментируемой статьи устанавливает право Роскомнадзора как уполномоченного органа по защите прав субъектов персональных данных вносить в Правительство РФ предложения о совер-

шенствовании нормативного правового регулирования защиты прав субъектов персональных данных.

Вместе с тем функции нормативно-правового регулирования закреплены за федеральными министерствами, а также за иными федеральными органами исполнительной власти — федеральными службами и федеральными агентствами, руководство деятельностью которых осуществляет Президент РФ или Правительство РФ.

Так, в соответствии с пп. «а», «в» п. 4 Указа Президента РФ «О системе и структуре федеральных органов исполнительной власти» федеральная служба является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в установленной сфере деятельности, и она не вправе осуществлять нормативно-правовое регулирование.

Функции по нормативно-правовому регулированию осуществляют федеральные министерства, кроме случаев, установленных указами Президента РФ или постановлениями Правительства РФ.

Согласно постановлению Правительства РФ от 02.06.2008 № 418 «О Министерстве связи и массовых коммуникаций Российской Федерации» функции по нормативно-правовому регулированию в сфере обработки персональных данных осуществляет Минкомсвязи России.

Система правового регулирования правотворческих процедур, направленных на регламентацию внутренней организации и взаимодействия федеральных органов исполнительной власти, а также правил подготовки нормативных правовых актов, разработанных федеральными органами исполнительной власти, исключает возможность реализации правотворческих процедур федеральными службами, руководство деятельностью которых осуществляют федеральные министерства.

Анализ системы нормативных правовых актов, регулирующих правотворческую деятельность федеральных органов исполнительной власти, позволяет сделать вывод о том, что к административно-правотворческим процедурам относятся процедуры подготовки предложений о совершенствовании нормативных правовых актов, проектов нормативных правовых актов, их согласования, направления на заключение, визирование, процедура подписания, направление на государственную регистрацию в Минюст России и др.

Встроенные в систему стадий правотворческого процесса, указанные административные процедуры реализуются посредством деятельности участников правотворческого процесса, чьи действия также регламентированы.

Так, в соответствии с п. 6 и 7 Регламента Правительства Российской Федерации, утвержденного постановлением Правительства РФ от 01.06.2004 № 260, проекты нормативных правовых актов, а также предложения о принятии нормативных правовых актов могут вноситься на рассмотрение в Правительство РФ лишь четко определенными органами исполнительной власти, в число которых федеральные службы не входят. Исключение составляют службы, руководство деятельностью которых осуществляет Президент РФ или Правительство РФ.

Проекты актов или предложения о принятии нормативных правовых актов в случае внесения их в Правительство РФ руководителями органов, которые не указаны в этом регламенте, подлежат направлению в федеральные министерства в соответствии со сферами ведения соответствующих федеральных органов исполнительной власти.

Данные министерства проводят проработку обращений и принимают в пределах своей компетенции соответствующие решения, при необходимости вносят в Правительство РФ в установленном порядке проекты актов, по которым требуется решение Правительства РФ (п. 10, 11 указанного регламента).

> **Таким образом**, существующая система правового регулирования правотворческих процедур не предусматривает возможность реализации права Роскомнадзора направлять предложения по совершенствованию нормативно-правового регулирования защиты прав субъектов персональных данных в Правительство РФ, несмотря на то, что в п. 8 ч. 3 ст. 23 Закона о персональных данных за Роскомнадзором закреплено право вносить предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных.

Пункт 9 ч. 3 комментируемой статьи устанавливает полномочие Роскомнадзора привлекать к административной ответственности лиц, виновных в нарушении рассматриваемого закона.

В настоящее время гл. 13 КоАП РФ «Правонарушения в области связи и информации» содержит состав административных правонарушений, объектом которых являются отношения, связанные с оборотом и защитой персональных данных граждан.

Один из составов — «*Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)*» (ст. 13.11 КоАП РФ). Ответственность наступает в виде предупреждения или наложения штрафа на граждан — в раз-

мере от 300 до 500 руб., на должностных лиц — от 500 до 1 тыс. руб., на юридических лиц — от 5 до 10 тыс. руб.

Указанная норма сформулирована чрезмерно широко: ответственность наступает за нарушение установленного законом порядка сбора, хранения, использования или распространении информации о гражданах (персональных данных). Под это определение подпадают любые незаконные действия с персональными данными, вне зависимости от статуса субъекта административного правонарушения. Максимальное наказание в ст. 13.11 КоАП РФ предусмотрено для юридических лиц — это штраф в размере 10 тыс. руб.

Следует обратить особое внимание на то, что согласно п. 9 ч. 3 ст. 23 Закона о персональных данных уполномоченный орган имеет право привлекать к административной ответственности лиц, виновных в нарушении требований данного закона. Однако п. 58 ч. 2 ст. 28.3 КоАП РФ не наделяет Роскомнадзор полномочиями по составлению протоколов об административных правонарушениях, предусмотренных ст. 13.11 КоАП РФ. Данный состав относится к исключительной компетенции прокурора (ст. 28.4 КоАП РФ). В связи с этим Роскомнадзор при выявлении указанных правонарушений направляет материалы для возбуждения дела об административном правонарушении в прокуратуру.

Вместе с тем усовершенствовать систему защиты прав и законных интересов субъектов персональных данных, а также повысить эффективность осуществления государственного контроля (надзора) в области персональных данных помогут изменения в административное законодательство в части консолидации административных полномочий в рамках одного ведомства — Роскомнадзора.

В настоящее время проходит обсуждение законопроект «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» в части передачи полномочий по возбуждению дел об административном правонарушении в сфере персональных данных от прокуратуры к Роскомнадзору, а также дифференциации составов административных правонарушений в области персональных данных и увеличения санкций за указанные правонарушения.

В отдельные составы могут быть выделены правонарушения оператора персональных данных, обработка персональных данных без согласия субъекта персональных данных, незаконная обработка специальных категорий персональных данных и несоблюдение условий трансграничной передачи персональных данных.

Законопроектом заявлено существенное увеличение размера штрафов за нарушение законодательства о персональных данных. Для не-

которых новых составов предлагается установить квалифицирующие признаки: повторное совершение правонарушения и причинение вреда жизни и (или) здоровью гражданина в результате незаконной обработки персональных данных. Так, на наибольшие суммы предлагается штрафовать юридических лиц, повторно привлекаемых к ответственности за аналогичные административные правонарушения. Например, за повторное несоблюдение условий трансграничной передачи персональных данных для юридического лица может быть установлен минимальный штраф в размере 700 тыс. руб.

Наибольшая ответственность будет предусмотрена за незаконную обработку специальных категорий персональных данных. К таким данным относятся следующие сведения о гражданине: расовая, национальная принадлежность, политические взгляды, религиозные или философские убеждения, информация о состоянии здоровья, интимной жизни. Минимальный размер штрафа для юридических лиц составит 300 тыс. руб.

Особый порядок предлагается установить для расчета штрафов за обработку персональных данных с целью извлечения дохода без согласия субъекта таких данных или с нарушением формы подобного согласия, установленной законом о персональных данных. Штрафы в таком случае будут зависеть от выручки от реализации товаров, услуг, полученной с использованием таких персональных данных.

С 1 сентября 2015 г. вступает в силу Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях», согласно которому ч. 3 ст. 23 комментируемого закона будет дополнена новым пунктом следующего содержания: «*3.1) ограничивать доступ к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, в порядке, установленном законодательством Российской Федерации*».

4. Норма ч. 4 комментируемой статьи обязывает должностных лиц Роскомнадзора обеспечивать конфиденциальность персональных данных, ставших им известными в ходе осуществления своей деятельности по защите прав субъектов персональных данных.

Аналогичное положение содержится в п. 2 ст. 15 Конвенции 1981 года, согласно которому каждое государство — участник этой конвенции взяло на себя обязательство по обеспечению соблюдения сотрудниками уполномоченных органов по защите прав субъектов персональных данных режима конфиденциальности информации, к которой

они имеют доступ в связи с исполнением своих служебных обязанностей в данной сфере.

5. Часть 5 анализируемой статьи определяет обязанности уполномоченного органа по защите прав субъектов персональных данных.

Согласно п. 1 ч. 5 комментируемой статьи уполномоченный орган обязан организовывать защиту прав субъектов персональных данных. Эта обязанность выполняется посредством реализации всех полномочий и прав, предоставленных Роскомнадзору законодательством о персональных данных как инструменту защиты прав субъектов персональных данных.

Пункт 2 ч. 5 указанной статьи устанавливает обязанность Роскомнадзора рассматривать жалобы и обращения граждан или юридических лиц по вопросам, связанным с обработкой персональных данных, а также принимать в пределах своих полномочий решения по результатам рассмотрения указанных жалоб и обращений.

Напомним, что отношения, связанные с реализацией гражданином РФ права на обращение в государственные органы и органы местного самоуправления, регулирует Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации». Указанным законом также установлены обязанность и порядок рассмотрения обращений граждан государственными органами, органами местного самоуправления и должностными лицами.

Пунктом 3 ч. 5 ст. 23 Закона о персональных данных определена обязанность уполномоченного органа по ведению реестра операторов персональных данных. Рассматриваемая обязанность Роскомнадзора представляет собой государственную услугу, сроки и последовательность административных процедур и административных действий которой установлены Административным регламентом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных», утвержденным приказом Минкомсвязи России от 21.12.2011 № 346.

Кроме этого, ч. 5 анализируемой статьи предусматривает следующие обязанности уполномоченного органа:

- осуществлять меры, направленные на совершенствование защиты прав субъектов персональных данных;
- принимать в установленном законодательством РФ порядке по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, или фе-

дерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, меры по приостановлению или прекращению обработки персональных данных;

- информировать государственные органы, а также субъектов персональных данных по их обращениям или запросам о положении дел в области защиты прав субъектов персональных данных;
- выполнять иные предусмотренные законодательством РФ обязанности.

6. Часть 5.1 рассматриваемой статьи наделяет уполномоченный орган правом осуществлять сотрудничество с органами, уполномоченными по защите прав субъектов персональных данных в иностранных государствах, в частности, осуществлять международный обмен информацией о защите прав субъектов персональных данных.

Реализуя право на сотрудничество с иностранными уполномоченными органами, Роскомнадзор принимает участие в различных международных конференциях, совещаниях и переговорах, посвященных проблематике персональных данных. Примером такого сотрудничества является участие в мероприятиях *Ad hoc Committee on data protection* (*CAHDATA*).

В рамках осуществления международного обмена информацией о защите прав субъектов персональных данных Роскомнадзором ежегодно проводится Международная конференция «Защита персональных данных». В ноябре 2014 г. она была проведена в пятый раз. В конференции принимают участие представители уполномоченных органов иностранных государств. Сайт Международной конференции «Защита персональных данных»: *http://zpd-forum.com/events.html*.

Также ч. 5.1 комментируемой статьи называет Роскомнадзор в качестве органа государственной власти, уполномоченного утверждать перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных (*см. комментарий к ст. 12 Закона о персональных данных*).

7. Часть 6 анализируемой статьи устанавливает судебный порядок обжалования решений уполномоченного органа.

Вместе с тем следует отметить, что данная норма является корреспондирующей к положениям ст. 46 Конституции РФ и гл. 25 ГПК РФ, согласно которым граждане и организации вправе обратиться в суд за защитой своих прав и свобод с заявлением об оспаривании решений, действий (бездействия) органов государственной власти и должностных лиц, в результате которых были нарушены их права и свободы или

созданы препятствия к осуществлению ими прав и свобод либо на них незаконно возложена какая-либо обязанность или они незаконно привлечены к ответственности.

Порядок судопроизводства по делам об оспаривании указанных выше решений, а также действий (бездействия) уполномоченного органа по защите прав субъектов персональных данных определен гл. 25 ГПК РФ. К оспариваемым решениям относятся акты органов государственной власти, их должностных лиц, принятые единолично или коллегиально, содержащие властное волеизъявление, порождающие правовые последствия для конкретных граждан и организаций.

При этом согласно постановлению Пленума Верховного Суда РФ от 10.02.2009 № 2 «О практике рассмотрения судами дел об оспаривании решений, действий (бездействия) органов государственной власти, органов местного самоуправления, должностных лиц, государственных и муниципальных служащих» оспариваемое решение может быть выражено как в письменной, так и в устной форме.

Письменное решение принимается как в установленной законодательством определенной форме (например, акт проверки деятельности юридического лица), так и в произвольной (например, письменное сообщение об отказе должностного лица в удовлетворении обращения гражданина).

8. Часть 7 комментируемой статьи обязывает уполномоченный орган ежегодно составлять отчет о своей деятельности. Данный отчет подлежит направлению Президенту РФ, в Правительство РФ и Федеральное Собрание, а также публикуется в СМИ. Ознакомиться с ежегодными отчетами о деятельности уполномоченного органа по защите прав субъектов персональных данных можно на официальном сайте Роскомнадзора (*http://rkn.gov.ru/personal-data/reports/*).

9. Часть 8 рассматриваемой статьи определяет, что финансирование уполномоченного органа по защите прав субъектов персональных данных осуществляется за счет средств федерального бюджета. Федеральный бюджет в соответствии со ст. 11 БК РФ разрабатывается и утверждается в форме федерального закона. Бюджет на 2015 год утвержден Федеральным законом от 01.12.2014 № 384-ФЗ «О федеральном бюджете на 2015 год и на плановый период 2016 и 2017 годов».

10. Согласно ч. 9 анализируемой статьи при уполномоченном органе по защите прав субъектов персональных данных создается на общественных началах консультативный совет.

Порядок формирования и порядок деятельности консультативного совета определены в Положении о Консультативном совете при упол-

номоченном органе по защите прав субъектов персональных данных, утвержденном приказом Роскомнадзора от 20.06.2012 № 621. Согласно указанному положению Консультативный совет — консультативно-совещательный орган при Роскомнадзоре, осуществляющий свою деятельность на общественных началах. Консультативный совет не является экспертным учреждением, однако его члены могут выступать в качестве экспертов в порядке, предусмотренном действующим законодательством РФ.

К основным функциям Консультативного совета относятся:

- участие в формировании программ и планов деятельности Роскомнадзора в области защиты персональных данных;
- рассмотрение вопросов о необходимости включения определенных категорий операторов персональных данных в план проведения плановых проверок на текущий год при его формировании;
- изучение и оценка информации о состоянии дел в области персональных данных на основе научных и социологических исследований и разработок, профессиональных знаний и международного опыта;
- изучение, обобщение и распространение опыта организации деятельности по защите прав субъектов персональных данных;
- выработка и рассмотрение предложений по внесению изменений и дополнений в действующее законодательство РФ в области персональных данных;
- рассмотрение перечня проектов нормативных правовых актов и иных документов в области защиты персональных данных, включая перспективные, разрабатываемые Роскомнадзором, которые не могут быть приняты без предварительного обсуждения на заседании Консультативного совета;
- обсуждение проектов законодательных и иных нормативных правовых актов в области персональных данных;
- содействие реализации мер, направленных на защиту прав субъектов персональных данных;
- содействие реализации мер, направленных на расширение международного сотрудничества по вопросам защиты прав субъектов персональных данных.

Состав Консультативного совета утверждается приказом Роскомнадзора и состоит из председателя, заместителя председателя, ответственного секретаря и членов Консультативного совета. С действующим составом Консультативного совета, сформированным 11 декабря

2014 г., можно ознакомиться на официальном сайте Роскомнадзора (*www.rsoc.ru*) и на портале персональных данных (*pd.rsoc.ru*).

Также открытой для общественности является деятельность Консультативного совета, в связи с чем информация о проводимых заседаниях Консультативного совета, принимаемых решениях, деятельности постоянных и временных рабочих групп размещается на официальном сайте Роскомнадзора и на портале персональных данных.

Статья 24. Ответственность за нарушение требований настоящего Федерального закона

1. Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность. *(в ред. Федерального закона от 25.07.2011 № 261-ФЗ)*

2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков. *(часть вторая введена Федеральным законом от 25.07.2011 № 261-ФЗ)*

1. Комментируемая статья содержит нормы, касающиеся вопросов ответственности за нарушения положений Закона о персональных данных. Так, ч. 1 этой статьи предусматривает, что лица, виновные в нарушении требований указанного закона, несут предусмотренную законодательством РФ ответственность.

Однако поскольку нормы комментируемой статьи являются отсылочными, то установление конкретных видов правонарушений, санкций, а также порядок привлечения к ответственности виновных лиц определены соответствующим отраслевым законодательством. При этом ни в одной отрасли права не выделены в отдельную группу правонарушения в области обработки персональных данных.

Так, несмотря на то что в уголовном законодательстве не предусмотрено составов преступлений, в которых содержится словосочетание «персональные данные», отдельные статьи УК РФ предусматривают ответственность за противоправные деяния с использованием персональных данных, либо объект посягательства которых тесно связан с персональными данными. К таким преступлениям можно отнести составы, установленные ст. 137, 272, ч. 2 ст. 173.2, 155 УК РФ (*см. комментарий к ст. 23 Закона о персональных данных*).

Вместе с тем основной формой ответственности за нарушение законодательства о персональных данных является административная ответственность.

Так, ст. 13.11 КоАП РФ предусмотрена ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (*см. комментарий к ст. 23 Закона о персональных данных*).

Уполномоченный орган также может привлечь оператора персональных данных к административной ответственности за непредставление сведений (информации) по запросу уполномоченного органа (ст. 19.7 КоАП РФ), неповиновение законному распоряжению должностного лица уполномоченного органа, осуществляющего государственный надзор (контроль) в области обработки персональных данных (ст. 19.4 КоАП РФ), за невыполнение в срок законного предписания уполномоченного органа (ст. 19.5 КоАП РФ).

Кроме этого, за нарушение положений Закона о персональных данных может наступить дисциплинарная ответственность в отношении должностных лиц или работников организации, осуществляющих обработку персональных данных, за ненадлежащее исполнение ими своих трудовых обязанностей, связанных с обработкой персональных данных.

Так, ст. 192 ТК РФ предусматривает следующие виды дисциплинарных взысканий за совершение дисциплинарного проступка: замечание; выговор; увольнение.

К дисциплинарным взысканиям относится, в частности, увольнение работника по основанию, предусмотренному пп. «в» п. 6 ч. 1 ст. 81 ТК РФ, т.е. за разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашение персональных данных другого работника.

Порядок привлечения операторов персональных данных к гражданско-правовой ответственности определен в Гражданском процессуальном кодексе РФ. В связи с этим субъекту персональных данных в первую очередь необходимо определить суд, в который следует подать исковое заявление о защите своих прав как субъекта персональных данных. По общему правилу согласно ч. 6.1 ст. 29 ГПК РФ иски о защите прав субъекта персональных данных, в том числе о возмещении убытков и компенсации морального вреда, могут предъявляться в суд по выбору истца: как в суд по месту жительства истца, так и в суд по месту жительства ответчика.

При этом в случае, если дело о защите прав субъектов персональных данных осложнено иностранным элементом, следует также учитывать правила, установленные в гл. 44 ГПК РФ. Так, согласно п. 10 ч. 3 ст. 402 ГПК РФ суды в Российской Федерации вправе рассматривать дела с участием иностранных лиц в случае, если по делу о защите прав субъекта персональных данных, в том числе о возмещении убытков и (или) компенсации морального вреда, истец имеет место жительства в Российской Федерации.

Следует отметить, что исполнение российского судебного решения на территории иностранного государства представляет собой довольно трудоемкую и длительную процедуру, правила которой определяются в соответствии с требованиями гл. 45 ГПК РФ, международными договорами РФ об оказании международной правовой помощи.

В случае если права субъекта персональных данных были нарушены в Интернете, например, посредством размещения данных в общем доступе, исполнить решение российского суда путем принуждения ответчика на территории иностранного государства к удалению персональных данных из Интернета будет невозможно. Так, ни один международный договор о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам не предусматривает возможность экзекватуры по делам о защите прав субъектов персональных данных путем ограничения доступа к данным в Интернете.

Исполнение подобных решений осуществляется в порядке, предусмотренном ст. 15.1 Федерального закона «Об информации, информационных технологиях и о защите информации». Согласно этой статье одним из оснований для включения информации в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в сети „Интернет“ и сетевых адресов, позволяющих идентифицировать сайты в сети „Интернет“, содержащие информацию, распространение которой в Российской Федерации запрещено» в целях ограничения доступа к сайтам, является вступившее в законную силу решение суда.

После включения информации о сайте в указанный реестр доступ к сайту или странице сайта, посредством которых осуществляется незаконная обработка персональных данных, будет заблокирован. Посредством применения указанной нормы в 2014 году Роскомнадзором было исполнено девять судебных решений о блокировке 16 интернет-ресурсов[1].

[1] См.: http://rkn.gov.ru/news/rsoc/news30327.htm.

2. Часть 2 комментируемой статьи устанавливает основания взыскания морального вреда, причиненного субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Законом о персональных данных, а также требований к защите персональных данных. При этом указанная часть анализируемой статьи содержит отсылочную норму при определении правил возмещения морального вреда. Способ и размер компенсации морального вреда установлены в Гражданском кодексе РФ.

Глава 6
Заключительные положения

Статья 25. Заключительные положения

1. Настоящий Федеральный закон вступает в силу по истечении ста восьмидесяти дней после дня его официального опубликования.

2. После дня вступления в силу настоящего Федерального закона обработка персональных данных, включенных в информационные системы персональных данных до дня его вступления в силу, осуществляется в соответствии с настоящим Федеральным законом.

2.1. Операторы, которые осуществляли обработку персональных данных до 1 июля 2011 года, обязаны представить в уполномоченный орган по защите прав субъектов персональных данных сведения, указанные в пунктах 5, 7.1, 10 и 11 части 3 статьи 22 настоящего Федерального закона, не позднее 1 января 2013 года. *(часть вторая.1 введена Федеральным законом от 25.07.2011 № 261-ФЗ)*

3. Утратил силу. — *Федеральный закон от 25.07.2011 № 261-ФЗ.*

4. Операторы, которые осуществляют обработку персональных данных до дня вступления в силу настоящего Федерального закона и продолжают осуществлять такую обработку после дня его вступления в силу, обязаны направить в уполномоченный орган по защите прав субъектов персональных данных, за исключением случаев, предусмотренных частью 2 статьи 22 настоящего Федерального закона, уведомление, предусмотренное частью 3 статьи 22 настоящего Федерального закона, не позднее 1 января 2008 года.

5. Отношения, связанные с обработкой персональных данных, осуществляемой государственными органами, юридическими лицами, физическими лицами при предоставлении государственных и муниципальных услуг, исполнении государственных и муниципальных функций в субъекте Российской Федерации — городе федерального значения Москве, регулируются настоящим Федеральным законом, если иное не предусмотрено Федеральным законом «Об особенностях регулирования отдельных правоотношений в связи с присоединением к субъекту Российской Федерации — городу федерального значения Москве территорий и о внесении изменений в отдельные законодательные акты Российской Федерации». *(часть пятая введена Федеральным законом от 05.04.2013 № 43-ФЗ)*

1. Комментируемая статья содержит правила вступления в силу Закона о персональных данных и определяет срок его вступления в силу.

Так, согласно ч. 1 анализируемой статьи этот закон вступает в силу по истечении 180 дней после дня его официального опубликования. Учитывая, что официальным опубликованием считается первая публикация полного текста документа в «Парламентской газете», «Российской газете», «Собрании законодательства Российской Федерации» или первое размещение на официальном интернет-портале правовой информации (*www.pravo.gov.ru*), данный срок следует рассчитывать с 29 июля 2006 г., когда Закон о персональных данных был впервые опубликован в «Российской газете» (ст. 4 Федерального закона от 14.06.1994 № 5-ФЗ «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания»).

Вместе с тем дату начала течения срока вступления в силу следует определять также в соответствии с требованиями ст. 191 ГК РФ, согласно которой течение срока начинается на следующий день после календарной даты или наступления события, которыми определено его начало. Таким образом, поскольку днем официального опубликования является 29 июля 2006 г., а началом течения срока будет считаться 30 июля 2006 г., то днем вступления в силу комментируемого закона является 26 января 2007 г.

2. В соответствии с одним из основополагающих принципов правовой системы РФ — «закон обратной силы не имеет» комментируемый закон не распространяется на отношения, возникающие до его вступления в законную силу (ст. 54 Конституции РФ).

Закон о персональных данных не распространяет свое действие на те отношения по обработке персональных данных, которые возникли до его вступления в силу. Однако согласно ч. 2 анализируемой статьи под действие закона подпадают отношения по обработке персональных данных, включенных в информационные системы до дня его вступления в силу. То есть, если персональные данные были собраны и обработаны в информационной системе до 26 января 2007 г., то их дальнейшая обработка должна осуществляться в соответствии с требованиями комментируемого закона.

3. В ч. 4 рассматриваемой статьи установлена обязанность операторов, которые осуществляли обработку персональных данных до дня вступления в силу Закона о персональных данных и продолжают осуществлять такую обработку после дня его вступления в силу, направить в уполномоченный орган по защите прав субъектов персональных данных уведомление об обработке персональных данных не позднее 1 января 2008 г. Таким образом, законодатель определил «переходный

период», в течение которого операторы персональных данных могут реализовать обязанность по направлению уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных, не нарушая требования законодательства о персональных данных. Все операторы, которые начали осуществлять обработку персональных данных после дня вступления в силу Закона о персональных данных, должны уведомлять уполномоченный орган до начала такой обработки.

4. 25 июля 2011 г. в комментируемую статью были внесены изменения. Эти изменения были направлены на совершенствование порядка внесения сведений об операторах персональных данных в реестр операторов и дополнили уведомление об обработке персональных данных, которое подается в Роскомнадзор, новыми сведениями.

Учитывая, что уведомления операторов об обработке персональных данных, поданные до внесения соответствующих изменений в текст комментируемого закона, не содержали этих дополнительных сведений, в ч. 2.1 ст. 25 Закона о персональных данных было предусмотрено, что операторы, которые осуществляли обработку персональных данных до 1 июля 2011 г., были обязаны представить в уполномоченный орган по защите прав субъектов персональных данных сведения, указанные в п. 5, 7.1, 10, 11 ч. 3 ст. 22 названного закона, не позднее 1 января 2013 г.

Апелляционное определение Московского городского суда от 16 июля 2014 г. № 33-27539

1 инстанция: судья Грабовская Г.А.

Судебная коллегия по гражданским делам Московского городского суда в составе:

председательствующего Лукашенко Н.И.

и судей Иваненко Ю.С., Фроловой Л.А.,

при секретаре М.,

заслушав в открытом судебном заседании по докладу судьи Иваненко Ю.С.

дело по апелляционной жалобе В. на решение Басманного районного суда г. Москвы от 2 апреля 2014 г. по иску В. к ОАО НБ «ТРАСТ» о взыскании компенсации морального вреда, которым в удовлетворении исковых требований отказано,

установила:

В. обратилась в суд с иском к ОАО НБ «ТРАСТ» о взыскании компенсации морального вреда, мотивируя свои требования тем, что на протяжении более 5 лет на принадлежащие ей домашний и мобильный телефоны поступали звонки с требованиями о возврате денежных средств, полученных в ОАО НБ «ТРАСТ» в виде кредита, с использованием оскорблений и угроз физической расправы в случае их невозврата. ОАО НБ «ТРАСТ» незаконно использовал ее персональные данные, в связи с чем ее деловой репутации был нанесен ущерб, выразившийся в невозможности с 2008 года получить кредит, и, полагая, что действиями банка нарушены ее права в части предусмотренных ст. 150 ГК РФ нематериальных благ, истец В. просила суд взыскать с ответчика ОАО НБ «ТРАСТ» компенсацию морального вреда в размере [...] руб., а также судебные расходы в размере [...] руб.

В судебное заседание суда первой инстанции истец В. не явилась, ее представитель по доверенности К. исковые требования поддержал в полном объеме.

Представитель ответчика ОАО НБ «ТРАСТ» в судебном заседании суда первой инстанции исковые требования не признала.

Представитель третьего лица ООО «Морган энд стаут» в судебное заседание явился, представит письменный отзыв.

Решением суда в удовлетворении иска В. отказано.

Не согласившись с решением суда, истец В. обжаловала его в апелляционном порядке.

Руководствуясь ст. 167, 327 ГПК РФ, судебная коллегия полагает возможным рассмотреть дело при данной явке.

Проверив материалы дела, заслушав объяснения истца В., ее представителя по доверенности К., представителя ответчика ОАО НБ «ТРАСТ» по доверенности Б. и представителя третьего лица ООО «Морган энд стаут» по доверенности Ф., обсудив доводы апелляционной жалобы, судебная коллегия не находит оснований к от-

мене решения суда как принятого в соответствии с установленными по делу обстоятельствами и действующими нормами материального и процессуального права.

Установив по делу фактические обстоятельства, на которых основаны заявленные требования и которые явились предметом судебной проверки, что нашло отражение в мотивировочной части решения, суд пришел к выводу об отсутствии в данном случае оснований для удовлетворения исковых требований В.

Так, из материалов дела следует, что 23 августа 2010 г. между В., [...] года рождения, уроженки г. [...] и ОАО НБ «ТРАСТ» был заключен кредитный договор № [...].

Истец В., [...] года рождения, уроженка дер. [...], зарегистрированная по адресу: [...], в договорных отношениях с ОАО НБ «ТРАСТ» не состояла, заемщиком или поручителем в рамках кредитного договора № [...] от 23.08.2010 не являлась.

Сведения о телефонных номерах истца В. размещены в сети Интернет и являются общедоступными.

Указанные обстоятельства сторонами по делу в суде первой инстанции не оспаривались.

Проанализировав установленные по делу обстоятельства, суд первой инстанции, руководствуясь ст. 2 Конвенции от 28.01.1981 о защите физических лиц в отношении автоматизированной обработки данных личного характера, ст. 19, 151 ГК РФ и ст. 2, 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», пришел к выводу об отсутствии в действиях сотрудников ответчика ОАО НБ «ТРАСТ» нарушений установленного на законодательном уровне порядка использования персональных данных истца, на основании чего отказал в удовлетворении исковых требований В.

При этом суд обоснованно исходил из того, что сотрудники ответчика связывались с истцом по общедоступным телефонным номерам, размещенным в сети Интернет, и при этом высказывания работников банка не содержали персонифицированных и детализированных данных, поскольку ими не называлось ни адреса места проживания истца, ни года, месяца, даты и места ее рождения, не указывалось ее семейное, социальное, имущественное положение, образование, профессия, доходы, а также другой информации, по которой можно было бы идентифицировать конкретное лицо.

Согласно п. 1 ст. 151 ГК РФ, если гражданину причинен моральный вред действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину нематериальные блага, а также в других случаях, предусмотренных законом, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда.

Судебная коллегия соглашается с выводами суда об отсутствии оснований для взыскания с ОАО НБ «ТРАСТ» в пользу В. компенсации морального вреда, поскольку доказательств, свидетельствующих о том, что персональные данные истца В. были распространены либо разглашены сотрудниками ответчика третьим лицам, в материалы дела стороной истца в соответствии с требованиями ст. 56 ГПК РФ представлено не было.

В соответствии с ч. 4 ст. 198 ГПК РФ в мотивировочной части решения суда должны быть указаны обстоятельства дела, установленные судом; доказательства,

на которых основаны его выводы об этих обстоятельствах; доводы, по которым суд отвергает те или иные доказательства; законы, которыми руководствовался суд.

Решение суда первой инстанции полностью соответствует требованиям данной нормы процессуального права, и судебная коллегия считает его законным и обоснованным.

В соответствии со ст. 327.1 ГПК РФ судебная коллегия проверяет законность и обоснованность решения суда первой инстанции исходя из доводов, изложенных в апелляционных жалобе, представлении.

В апелляционной жалобе истец В. указывает на неправильное определение судом обстоятельств, имеющих значение для дела, поскольку, по ее мнению, суд не учел, что телефонные звонки и смс-сообщения истцу совершались безосновательно, так как в договорных отношениях с ответчиком она никогда не состояла.

Однако с данным утверждением судебная коллегия согласиться не может.

В соответствии с разъяснениями, данными в п. 1 Постановления Пленума Верховного Суда Российской Федерации от 20.12.1994 № 10 «Некоторые вопросы применения законодательства о компенсации морального вреда», суду в целях обеспечения правильного и своевременного разрешения возникшего спора необходимо по каждому делу выяснять характер взаимоотношений сторон и какими правовыми нормами они регулируются, допускает ли законодательство возможность компенсации морального вреда по данному виду правоотношений, и если такая ответственность установлена, когда вступил в силу законодательный акт, предусматривающий условия и порядок компенсации вреда в этих случаях, а также когда были совершены действия, повлекшие причинение морального вреда.

Суду следует также устанавливать, чем подтверждается факт причинения потерпевшему нравственных или физических страданий, при каких обстоятельствах и какими действиями (бездействием) они нанесены, степень вины причинителя, какие нравственные или физические страдания перенесены потерпевшим, в какой сумме он оценивает их компенсацию и другие обстоятельства, имеющие значение для разрешения конкретного спора.

В соответствии со ст. 24 Федерального закона «О персональных данных» моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации.

В силу вышеприведенных норм под моральным вредом понимаются нравственные или физические страдания, причиненные действиями (бездействием), посягающими на принадлежащие гражданину от рождения или в силу закона нематериальные блага (жизнь, здоровье, достоинство личности, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна и т.п.) или нарушающими его личные неимущественные права (право на пользование своим именем, право авторства и другие неимущественные права в соответствии с законами об охране прав на результаты интеллектуальной деятельности), либо нарушающими имущественные права гражданина.

Обязательными условиями наступления ответственности за причинение морального вреда являются противоправные действия причинителя вреда, наличие причинной связи между его действиями и вредными последствиями и вина причинителя в наступлении вредных последствий.

Совершение звонков и направление смс-сообщений на телефон истца не является осуществлением со стороны ОАО НБ «ТРАСТ» противоправных действий в отношении истца В.

Одни лишь утверждения истца В. о причинении морального вреда со ссылкой на требования о погашении кредита не могут быть основанием в данном случае для удовлетворения ее исковых требований.

Доказательств, подтверждающих доводы апелляционной жалобы, что в результате действий ОАО НБ «ТРАСТ» был нанесен ущерб деловой репутации В., а также что истцу по этой причине какой-либо организацией было отказано в предоставлении кредита, в материалы дела и с апелляционной жалобой стороной истца не представлено.

Ввиду отсутствия достаточных доказательств противоправного поведения со стороны ответчика либо нарушения его сотрудниками личных неимущественных прав истца оснований для удовлетворения исковых требований В. о взыскании с ОАО НБ «ТРАСТ» компенсации морального вреда у суда первой инстанции не имелось.

Таким образом, доводы апелляционной жалобы не могут быть положены в основу отмены по существу правильного судебного постановления, так как основаны на неправильном толковании положений законодательства, применяемого к спорным правоотношениям, сводятся к выражению несогласия с произведенной судом первой инстанции оценкой обстоятельств дела и представленных по делу доказательств.

При этом обстоятельств, которые нуждались бы в дополнительной проверке, доводы апелляционной жалобы не содержат.

Оснований для иной оценки имеющихся в материалах дела доказательств суд апелляционной инстанции не усматривает.

Предусмотренных ст. 330 ГПК РФ оснований для отмены решения суда по доводам апелляционной жалобы судебная коллегия не усматривает. Нарушений норм ГПК РФ, влекущих отмену решения, по делу не установлено.

На основании изложенного, руководствуясь ст. 328, 329 ГПК РФ, судебная коллегия

определила:

Решение Басманного районного суда г. Москвы от 02.04.2014 оставить без изменения, апелляционную жалобу В. — без удовлетворения.

Содержание

Федеральный закон
«О персональных данных»:
научно-практический комментарий

Под редакцией заместителя руководителя
Федеральной службы по надзору в сфере связи,
информационных технологий
и массовых коммуникаций А.А. Приезжевой

Редактор М.А. Архимандритова
Корректор Г.Н. Хотеева
Верстка И.Ю. Луканина

Подписано в печать 27.05.2015.
Бумага архангельская писчая. Формат 60x88 1/16.
Усл. печ. л. 11,0. Уч.-изд. л. 10,0. Тираж 2910 экз.
Заказ №
Цена в рознице — договорная

Свидетельство о регистрации журнала «Библиотечка «Российской газеты»
как средства массовой информации ПИ № 77-1915 от 15.03.2000

Учредители: ФГБУ «Редакция «Российской газеты» и ЗАО «Библиотечка РГ»

Издатель ФГБУ «Редакция «Российской газеты»
Генеральный директор ФГБУ «Редакция «Российской газеты» П.А. Негоица
Главный редактор «Российской газеты» В.А. Фронин

Адрес издателя: 125993, г. Москва, ул. Правды, 24, стр. 4

По вопросам публикации и размещения рекламы
обращаться по тел.: 8-499-257-52-64; 8-499-257-52-47;
e-mail: bibliotechka@rg.ru.
Шеф-редактор журнала И.А. Бусыгина

Информация о других выпусках журнала: www.bibliotechka.rg.ru

Подписные индексы:
по Объединенному каталогу «Пресса России» («АПР»): 38229 (на год);
73097 (на полгода); 40913, 40945, 41591 (в комплектах с «РГ»);
по каталогу российской прессы «Почта России»: 12420 (на полгода)

Отпечатано в Обособленном подразделении Академиздатцентра «Наука» —
Производственно-полиграфическом предприятии «Типография «Наука».
Адрес: 121099, г. Москва, Шубинский пер., 6; тел. 8-499-241-94-93

ISSN 1605-7449