Комментарий к Федеральному закону от 27.07.2006 N 152-ФЗ "О персональных данных" (в ред. Федеральных законов от 25.11.2009 N 266-ФЗ, от 27.12.2009 N 363-ФЗ, от 28.06.2010 N 123-ФЗ, от 27.07.2010 N 204-ФЗ, от 27.07.2010 N 227-ФЗ, от 29.11.2010 N 313-ФЗ, от 23.12.2010 N 359-ФЗ, от 04.06.2011 N 123-ФЗ, от 25.07.2011 N 261-ФЗ, от 05.04.2013 N 43-ФЗ)

Глава 1. Общие положения

Статья 1. Сфера действия настоящего Федерального закона

1. Комментируемая статья определяет сферу действия комментируемого закона в наиболее общей форме.

Как любой нормативно-правовой акт, комментируемый закон призван регулировать определенную группу относительно однородных общественных отношений. Комментируемым законом регулируются отношения, связанные с обработкой персональных данных. В соответствии с п. 3 ст. 3 комментируемого закона обработка персональных данных представляет собой любое действие (операцию) 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 (см. подробнее комментарий к ст. 3).

Часть первая комментируемой статьи говорит о двух способах обработки персональных данных, регулируемых комментируемым законом: обработка автоматизированная и неавтоматизированная.

Автоматизированная обработка персональных данных осуществляется с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях. В соответствии с п. 4 ст. 3 комментируемого закона автоматизированная обработка персональных данных - это обработка персональных данных с помощью средств вычислительной техники.

Несмотря на кажущуюся простоту определения автоматизированной обработки персональных данных, не любая компьютерная обработка или обработка с помощью электронных устройств персональных данных будет означать использование средств автоматизации. Для разграничения автоматизированной и неавтоматизированной обработки персональных данных на нормативном уровне используется критерий участия человека в данном процессе. Согласно п. 1 Положения об особенностях обработки персональных данных, утвержденного постановлением Правительства РФ от 15.09.2008 N 687, обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как

использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека. Укажем, что, исходя из этих формальных критериев, обработку персональных данных в подавляющем большинстве информационных систем в государственных и муниципальных учреждениях формально можно рассматривать как осуществляемую без использования средств автоматизации, несмотря на повсеместное применение компьютерной техники*(1) (подробнее об автоматизированной обработке данных см. п. 4 комментария к ст. 3).

Неавтоматизированная обработка персональных данных имеет место, соответственно, в том случае, когда человек непосредственно осуществляет значимые действия по обработке персональных данных. Для того чтобы неавтоматизированная обработка персональных данных (обработка без использования средств автоматизации) являлась предметом регулирования комментируемого закона, она должна соответствовать характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации. Определяя данный характер, законодатель, собственно, указывает на главный критерий, по которому отношения по обработке персональных данных относятся к предмету его регулирования. Процессам автоматизированной обработки данных такой характер присущ изначально, процессы же неавтоматизированной обработки обладают им не во всех случаях. Обработка персональных данных должна позволять 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.

На практике и в подзаконных нормативных актах выделяется также смешанная обработка персональных данных (сочетающая оба указанных типа обработки). Так, в п. 9 Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных, утв. приказом Роскомнадзора от 19.08.2011 N 706, говорится про неавтоматизированную обработку персональных данных, исключительно автоматизированную обработку персональных данных с передачей полученной информации по сети или без таковой и смешанную обработку персональных данных.

Пример: в суде было установлено, что банк осуществляет обработку персональных данных клиентов и работников оператора (банка) путем смешанной обработки персональных данных: как путем автоматической их обработки, так и неавтоматическим способом обработки. Автоматизированная обработка персональных данных банка обусловлена обработкой информации, полученной в ходе обработки персональных данных, передаваемых по внутренней сети оператора (операция доступна лишь для строго определенных сотрудников), при этом данная информация не передается с использованием сети общего пользования Интернет. Указанное свидетельствует, что Банк обрабатывает часть персональных данных автоматическим способом, без

непосредственного участия работника, что соответствует толкованию неавтоматической и автоматической обработки персональных данных, приведенному в постановлении Правительства РФ от 15.09.2008 N 687. При этом суд апелляционной инстанции указал, что обработка персональных данных без участия человека не подразумевает в данном случае того, что человек вообще исключен из участия данного процесса, поскольку любая автоматизированная обработка данных подразумевает участие человека, в частности ввод данных, обслуживание системы, ее настрой и т.п. Неавтоматизированная обработка персональных данных у банка состоит в ведении трудовых книжек, личных дел работников, учете и хранении договоров, заключенных с физическими лицами (см. решение Арбитражного суда Иркутской области от 14.05.2010 по делу N А19-25289/2009).

2. Субъектный состав правоотношений по обработке персональных данных также законодательно очерчен. Субъектами данных правоотношений являются:

1) государственные органы;

муниципальные органы;

юридические лица;

физические лица.

Рассмотрим их подробнее.

Задачи и функции государства осуществляются посредством деятельности его механизма, состоящего из соответствующих органов власти. Орган государственной власти - это часть государственного механизма, направленного на реализацию функций государства, обладающая определенными признаками:

- обладает определенной экономической и организационной обособленностью и самостоятельностью;
- наделен государственно-властными полномочиями;
- выполняет свойственные ему функции соответственно его компетенции;
- действует от имени государства и по его поручению;
- имеет установленную государством структуру и компетенцию*(2).

В соответствии со ст. 10 Конституции РФ органы государственной власти делятся на органы законодательной, исполнительной и судебной власти.

К федеральным органам государственной власти относятся:

а) Президент Российской Федерации (а также Совет Безопасности Российской Федерации; Администрация Президента Российской Федерации);

б) органы законодательной власти: Федеральное Собрание Российской Федерации (Совет Федерации Российской Федерации; Государственная Дума Российской Федерации);

в) органы исполнительной власти:

- Правительство Российской Федерации;
- федеральные министерства, федеральные службы и федеральные агентства, руководство деятельностью которых осуществляет Президент Российской Федерации, федеральные службы и федеральные агентства, подведомственные таким федеральным министерствам;
- федеральные министерства, федеральные службы и федеральные агентства, руководство которыми осуществляет Правительство Российской

Федерации, федеральные службы и федеральные агентства, подведомственные таким федеральным министерствам;

- организации при Президенте Российской Федерации, организации при Правительстве Российской Федерации, территориальные органы ряда министерств, организации при федеральных органах исполнительной власти, созданные Правительством Российской Федерации;

- организации при Правительстве Российской Федерации, не относящиеся к федеральным органам исполнительной власти, выполняющие некоторые функции исполнительной власти, определенные для них Президентом Российской Федерации или Правительством Российской Федерации, работающие на постоянной основе и являющиеся юридическими лицами;

- территориальные органы федеральных органов исполнительной власти; организации при федеральных органах исполнительной власти, созданные в соответствии с постановлениями Правительства Российской Федерации для решения задач по отдельным направлениям деятельности, отнесенной к ведению соответствующего федерального органа исполнительной власти;

г) органы судебной власти (Конституционный Суд Российской Федерации, система федеральных судов общей юрисдикции, система арбитражных судов в Российской Федерации, система Прокуратуры Российской Федерации, система Судебного департамента при Верховном Суде Российской Федерации);

д) иные государственные органы:

- Центральный банк Российской Федерации, Сберегательный банк Российской Федерации;

- Пенсионный фонд Российской Федерации;

- Федеральный фонд обязательного медицинского страхования, Фонд социального страхования Российской Федерации, Фонд содействия развитию малых форм предприятий в научно-технической сфере;

- Счетная палата Российской Федерации;

- Центральная избирательная комиссия Российской Федерации;

- Уполномоченный по правам человека в Российской Федерации;

- Российская академия наук;

- Общественная палата Российской Федерации;

К органам государственной власти субъектов Российской Федерации относятся:

а) органы представительной (законодательной) власти субъектов Российской Федерации;

б) органы исполнительной власти субъектов Российской Федерации;

в) правительства (администрации) и аналогичные по организационному уровню и функциям организации;

г) финансовые органы субъектов Российской Федерации и пр.

К муниципальным органам как субъектам рассматриваемых правоотношений комментируемая статья относит органы местного самоуправления и иные муниципальные органы. Местное самоуправление в Российской Федерации осуществляется гражданами как путем различных форм прямого волеизъявления, так и через органы местного самоуправления (ст. 130 Конституции РФ). В соответствии со ст. 132 Конституции РФ органы местного

самоуправления самостоятельно управляют муниципальной собственностью, формируют, утверждают и исполняют местный бюджет, устанавливают местные налоги и сборы, осуществляют охрану общественного порядка, а также решают иные вопросы местного значения. Органы местного самоуправления также могут наделяться законом отдельными государственными полномочиями с передачей необходимых для их осуществления материальных и финансовых средств. Реализация переданных полномочий подконтрольна государству;

Понятие юридического лица установлено в ст. 48 ГК РФ.

В соответствии со ст. 48 ГК РФ юридическим лицом признается организация, имеющая в собственности, хозяйственном ведении или оперативном управлении обособленное имущество и отвечающая по своим обязательствам этим имуществом, которая может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде.

Юридические лица также наделены правоспособностью (ст. 49 ГК РФ), которая возникает в момент их создания и прекращается в момент внесения записи об их исключении из единого государственного реестра юридических лиц;

Участниками рассматриваемой нами группы правоотношений выступают также физические лица. Следует отметить, что комментируемый закон не содержит указания на участие в рассматриваемых правоотношениях именно граждан РФ, следовательно, участниками данных правоотношений могут выступать и иностранные граждане - лица, не являющиеся гражданами РФ и имеющие гражданство (подданство) иностранного государства), а также лица без гражданства - лица, не являющиеся гражданами РФ и не имеющие доказательства наличия гражданства иностранного государства (ст. 3 Федерального закона от 31.05.2002 N 62-ФЗ "О гражданстве Российской Федерации"). Правовое положение указанных лиц регулируется Федеральным законом от 25.07.2002 N 115-ФЗ "О правовом положении иностранных граждан в Российской Федерации". Физическое лицо как субъект правоотношений обладает правоспособностью (возможность иметь права и нести обязанности) и дееспособностью (способность своими действиями приобретать и осуществлять гражданские права, создавать для себя обязанности и исполнять их). Наличие дееспособности - признак, свойственный только физическим лицам.

К физическим лицам относятся индивидуальные предприниматели, которые приобрели трудовую правосубъектность с момента их регистрации в качестве таковых и осуществляющие предпринимательскую деятельность без образования юридического лица. Согласно ст. 23 ГК РФ гражданин вправе заниматься предпринимательской деятельностью без образования юридического лица с момента государственной регистрации в качестве индивидуального предпринимателя. Кроме того, глава крестьянского (фермерского) хозяйства, осуществляющего деятельность без образования юридического лица (ст. 257), признается предпринимателем с момента государственной регистрации крестьянского (фермерского) хозяйства. Также, согласно ст. 20 ТК РФ, к физическим лицам - работодателям относятся частные нотариусы, адвокаты, учредившие адвокатские кабинеты, и иные лица, чья профессиональная деятельность в соответствии с федеральными законами подлежит

государственной регистрации и (или) лицензированию, вступившие в трудовые отношения с работниками в целях осуществления указанной деятельности. Физические лица, осуществляющие в нарушение требований федеральных законов указанную деятельность без государственной регистрации и (или) лицензирования, вступившие в трудовые отношения с работниками в целях осуществления этой деятельности, не освобождаются от исполнения обязанностей, возложенных ТК РФ на работодателей - индивидуальных предпринимателей.

Кроме индивидуальных предпринимателей, к физическим лицам - работодателям, на которых распространяется законодательство о персональных данных, относятся лица, которые в целях обеспечения своих личных потребностей (ведения домашнего хозяйства, управления личным автомобилем, охраны имущества и т.п.), творческой или научной деятельности используют чужой труд.

3. Часть вторая комментируемой статьи устанавливает перечень отношений, на которые не распространяется действие комментируемого закона:

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

Например, гражданин может вести домашнюю адресно-телефонную книгу, где указываются фамилии, имена, отчества, даты рождения, адреса, телефоны и иные сведения о его друзьях, родных и близких. В настоящее время хранение данной информации зачастую осуществляется в сети Интернет - в записных электронных книгах электронных почтовых ящиках, а также в записных книгах мобильных телефонов;

2) организация 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.

Отношения в сфере организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов независимо от их форм собственности, а также отношения в сфере управления архивным делом в Российской Федерации в интересах граждан, общества и государства регулируются Федеральным законом от 22.10.2004 N 125-ФЗ "Об архивном деле в Российской Федерации", а также принимаемыми в соответствии с ним иными нормативными правовыми актами Российской Федерации и субъектов Российской Федерации. Отличие данного вида правоотношений от правоотношений по обработке персональных данных заключается в том, что в соответствии с Федеральным законом от 22.10.2004 N 125-ФЗ обработке подвергается не информация, а только документы как носители информации, при этом не любые документы, а их отдельные категории, а именно:

архивные документы - материальные носители с зафиксированной на них информацией, которые имеют реквизиты, позволяющие их идентифицировать, и подлежат хранению в силу значимости указанных носителя и информации для граждан, общества и государства;

документы по личному составу - архивные документы, отражающие трудовые отношения работника с работодателем;

документы Архивного фонда Российской Федерации - архивные документы, прошедшие экспертизу ценности документов, поставленные на государственный учет и подлежащие постоянному хранению;

особо ценные документы - документы Архивного фонда Российской Федерации, которые имеет непреходящую культурно-историческую и научную ценность, особую важность для общества и государства и в отношении которых установлен особый режим учета, хранения и использования;

уникальные документы - особо ценные документы, не имеющие себе подобных по содержащейся в них информации и (или) их внешним признакам, невосполнимые при утрате с точки зрения их значения и (или) автографичности.

Кроме того, обработка указанных документов ограничена, допустимы не любые действия, а только действия по организации хранения, комплектования, учета и использования;

3) обработка персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

Отношения по обработке персональных данных, отнесенных к сведениям, составляющим государственную тайну, регулируются Законом РФ от 21.07.1993 N 5485-I "О государственной тайне".

Согласно ст. 2 указанного закона государственная тайна - это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Перечень сведений, составляющих государственную тайну, представляет совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством. Перечень сведений, составляющих государственную тайну, указан в ст. 3 Закона РФ от 21.07.1993 N 5485-I.

Таким образом, если персональные данные субъекта являются информацией, относящейся к перечню сведений, составляющих государственную тайну, их обработка осуществляется в соответствии со специальными нормами Закона РФ от 21.07.1993 N 5485-I;

4) предоставление уполномоченными органами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом от 22.12.2008 N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации".

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 Российской Федерации, 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 (п. 2 ст. 1 Федерального закона от 22.12.2008 N 262-ФЗ).

Доступ к информации о деятельности судов обеспечивается следующими способами:

присутствие граждан (физических лиц), в том числе представителей организаций (юридических лиц), общественных объединений, органов государственной власти и органов местного самоуправления, в открытом судебном заседании;

обнародование (опубликование) информации о деятельности судов в средствах массовой информации;

размещение информации о деятельности судов в информационно-телекоммуникационной сети Интернет;

размещение информации о деятельности судов в занимаемых судами, Судебным департаментом, органами Судебного департамента, органами судейского сообщества помещениях;

ознакомление пользователей информацией с информацией о деятельности судов, находящейся в архивных фондах;

предоставление пользователям информацией по их запросу информации о деятельности судов.

Информация о деятельности судов может предоставляться в устной форме и в виде документированной информации, в том числе в виде электронного документа, а также может быть передана по сетям связи общего пользования (ст. 6, 7 Федерального закона от 22.12.2008 N 262-ФЗ). Одними из основным принципов предоставления указанной информации являются открытость и доступность информации о деятельности судов, за исключением случаев, предусмотренных законодательством Российской Федерации, а также свобода поиска, получения, передачи и распространения информации о деятельности судов любым законным способом, тогда как при обработке персональных данных свобода поиска возможна только в отношении общедоступных источников персональных данных.

Статья 2. Цель настоящего Федерального закона

В комментируемой статье определена цель комментируемого закона, заключающаяся в обеспечении защиты прав и свобод гражданина при обработке его персональных данных в соответствии с основными правами и свободами, провозглашенными Конституцией Российской Федерации (ст. 17).

Природа прав субъекта персональных данных, его личной свободы, неприкосновенность частной жизни - объемная многогранная проблема, уходящая корнями в различные научные направления: философию, историю, юриспруденцию. В советский период и первое десятилетие современной российской истории исследования по вопросам личной свободы, частной жизни были ограничены отраслевыми рамками науки гражданского права. Современные исследователи придерживаются более широкой концепции природы персональных данных, что может быть достаточно наглядно представлено на кратком перечне работ. Наряду с традиционными

частноправовыми подходами (Н.И. Шахов*(3)), имеют место работы в рамках теории права, конституционного права (Э.А. Цадыкова*(4), И.В. Балакшина*(5)), международного права (И.А. Вельдер*(6)) и других отраслей права, в том числе информационного права (О.Б. Просветова*(7)). Научное направление, вбирающее все проблемы регулирования отношений по поводу персональных данных, концентрирующее научные исследования - отдельный институт защиты персональных данных в рамках информационного права. Тем не менее фактическое участие индивидуумов во всех отношениях, регулируемых всеми отраслями законодательства, а также техническими нормами, необходимость периодической идентификации, накопление и хранение сведений об индивидуумах, - это факторы, которые способствуют развитию различных исследовательских направлений. Они генерируют интерес к проблеме во всех научных отраслях, которые будут окружать и подпитывать развитие информационного права. Одна из основных идей, которая имеет место во многих исследовательских работах, такова: права субъекта персональных данных - это юридическая конструкция, производная от прав человека, сконцентрированная в источниках международного права. Многими исследователями конкретных правоотношений данная связь прослеживается от норм международного права до отраслевых. Например, О. Волкова, исследуя трудовые отношения, вопрос регламентации уровней доступа к персональным данным начинает с изучения Всеобщей декларации прав человека от 10.12.1948, далее отслеживает нормы, введенные Конвенцией о защите прав человека и основных свобод от 04.11.1950, и только потом обращается к Конституции России и российскому законодательству*(8). Действительно, основные, базовые нормы о персональных данных и о правах субъектов персональных данных впервые в современной истории появляются во Всеобщей декларации прав человека (1948), Европейской конвенции о защите прав человека и основных свобод (1950), Международном пакте о гражданских и политических правах (1976), Конвенции Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных (1981), Конвенции Содружества Независимых Государств о правах и основных свободах человека (1995) и других международных документах.

Одним из наиболее детализированных международных документов является Директива 95/46/ЕС Европейского парламента и Совета ЕС от 24.10.1995 о защите физических лиц в отношении обработки персональных данных и свободного обращения таких данных. Статья 10 Директивы предусматривает, какая информация в случаях получения данных от субъекта данных должна быть ему представлена, - это информация о наименовании оператора (его представителя); цели обработки, для которых предназначены данные. Кроме того, субъекту должны быть представлены другие сведения, например, о том, являются ли ответы на вопросы обязательными или добровольными, как и возможные последствия отсутствия ответа; существует ли право доступа и право исправлять относящиеся к нему данные, - насколько такая дополнительная информация необходима с учетом конкретных обстоятельств, в которых собираются данные, чтобы гарантировать их справедливую обработку в отношении субъекта данных.

В случае получения данных не от субъекта данных при возможном их раскрытии третьему лицу ст. 11 Директивы предусматривает обязанность оператора (его представителя) предоставить субъекту информацию о личности оператора (его представителя); целях обработки, а также дополнительную информацию (категории данных, получатели или категории получателей, существование права доступа и права исправлять относящиеся к нему данные) - насколько такая дополнительная информация необходима с учетом конкретных обстоятельств, в которых обрабатываются данные, чтобы гарантировать их справедливую обработку в отношении субъекта данных.

Право субъекта данных на доступ к данным предусматривает ст. 12 Директивы. Это право получать от оператора без ограничения, в разумные интервалы и без чрезмерной задержки или расходов:

подтверждение того, осуществляется или нет обработка относящихся к нему данных, и информацию по меньшей мере о целях обработки, категориях данных и получателях или категориях получателей, которым раскрываются данные;

право на сообщение ему в понятной форме данных, подвергающихся обработке, и любой имеющейся информации об их источнике;

знание об алгоритмах, задействованных в автоматической обработке касающихся его данных, по меньшей мере, в случае автоматизированных решений.

Данное право также включает право на исправление, стирание или блокирование, по мере необходимости, данных, обработка которых не соответствует нормам Директивы, в частности из-за неполноты или неточности самих данных, а также право на уведомление третьих лиц, которым были раскрыты данные, о любом исправлении, стирании или блокировании данных.

Российское законодательство частично воспроизводит основные положения названных актов. Например, согласно положениям ст. 23 и 24 Конституции РФ каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени; сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается, а органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Конституция ограничена определенным объемом и обусловлена определенным стилем изложения. Она не вмещает и в момент разработки не должна была вмещать все положения о правах субъекта персональных данных. Тем не менее развитие технологий в информационном обществе, проблема идентификации и самоидентификации субъекта персональных данных во всех жизненных сферах (публичной, частной, профессиональной, коммуникативной, иных) приобретают все большую значимость. Самым основным правом субъекта в информационном пространстве является набор персональных данных, гарантирующих его идентификацию, и требование (субъективное право) субъекта персональных данных о сохранении его персональных данных является приоритетным во всех сферах. Отсутствие надлежащей идентификации личности, его правового

статуса, правовой фиксации этих процедур делает все остальные права ничтожными. Внесение поправок в части усиления защиты персональных данных, особенно в части прав субъектов персональных данных, - вопрос, который рано или поздно будет связан с необходимостью внесения поправок в Конституцию России. Комментируемый закон является логическим продолжением Конституции России и более детально регламентирует нормы о правах субъекта персональных данных. Поскольку данный субъект является основным субъектом правоотношений - "главным действующим лицом", а его права являются основным объектом правоотношений, логичным представляется решение законодателя выделить права субъекта персональных данных в отдельную главу. Исторически в федеральном законодательстве понятие персональных данных - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность, - было впервые закреплено в первой редакции Федерального закона от 20.02.1995 N 24-ФЗ "Об информации, информатизации и защите информации", который в настоящее время утратил силу. Современная формулировка - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, - получила закрепление в комментируемом законе. Расширение контекста персональных данных и включение в основное понятие сведений о социальном, имущественном, образовательном ином состоянии способствовало более широкому восприятию данной категории и в исследовательской среде. Так, одним из представителей направления социальных исследований проблем прав субъекта персональных данных, идентификации субъекта в социальной сфере является Н.Н. Ходус. Автор отмечает, что в современную эпоху человек конструирует собственное Я, персональную идентичность, что позволяет говорить о том, что проблема защиты персональных данных не может быть решена без участия субъекта, без его активной позиции, если в целом полагаться только на государство или на оператора, то можно и не обеспечить полноценную защиту персональных данных*(9). Нормы о защите субъектов персональных данных и о защите персональных данных сосредоточены в соответствующих кодексах. Например, нормы об административной ответственности за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных), незаконную деятельность в области защиты, разглашение информации с ограниченным доступом закреплены в главе 13 КоАП РФ. Основной массив норм сосредоточен в комментируемом законе.

Критический анализ комментируемого закона проводит О.В. Борисенко. Она констатирует, что при лимите проверок 6 тысяч в год необходимо контролировать 7 миллионов операторов. Далее автор приводит аргументы в пользу замены действующей системы органов контроля за оборотом персональных данных (ФСТЭК, ФСБ, Минкомсвязь - Роскомнадзор) системой гражданских организаций-регуляторов, которые могли бы создаваться

различными структурами, работающими в сфере использования информации (операторами сотовой связи, медицинскими учреждениями, страховыми компаниями)*(10). Идея построения гражданского общества - формирование системы защиты циркулирующей в нем информации от неправильного использования - основной концепт автора. Аргументы О.В. Борисенко, действующего специалиста в системе Роскомнадзора, действительно заслуживают особого внимания и специального изучения. Вопрос защиты персональных данных и совершенствования законодательного механизма в сфере оборота персональных данных должен быть предметом внимания не только академических исследователей. Практическим специалистам, непосредственно работающим с персональными данными, предстоит продолжить начатые исследования.

О.С. Соколова, исследуя зарубежный опыт, констатирует, что практически во всех европейских государствах, а также в США, Австралии, Японии и ряде других стран действуют коллегиальные органы, являющиеся негосударственными структурами, в чьи функции входит защита прав субъектов правоотношений по поводу персональных данных и рассмотрение конфликтных ситуаций в этой сфере; регулярно проводятся международные совещания уполномоченных по защите персональных данных, возглавляющих эти органы*(11). Автор делает посыл о возможном учете и внедрении в России зарубежного опыта работы в сфере оборота персональных данных. Однако следует отметить, что в России предпринята попытка создания подобного органа. Роскомнадзор создал соответствующую структуру, деятельность которой носит формальный совещательный характер. Вопросы об адекватности контроля за оборотом и сохранностью персональных данных в России, возможности в современных условиях передать контрольные функции в сфере оборота персональных данных представляют серьезную проблему, к изучению которой основательно научное сообщество еще не приступало.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

1. Прежде всего, персональные данные, определение которых приводится первым в комментируемой статье, представляют собой информацию. Согласно Федеральному закону от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" информация - это сведения (сообщения, данные) независимо от формы их представления. Из содержания ст. 1 комментируемого закона следует, что в сферу действия закона попадает лишь информация, зафиксированная на материальном носителе, то есть документированная информация. Это соответствует принятому в информатике понятию "данные" (информация, зафиксированная на материальном носителе).

Кроме того, данная информация должна относиться к конкретному лицу, которое может быть прямо или косвенно определено пользователем персональных данных. Субъектом персональных данных может быть только физическое лицо.

В первоначальной редакции комментируемого закона под персональными

данными понималась "любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация". Конкретно указанные в законе атрибуты позволяли правоприменителям приходить к выводу, что простое сообщение фамилии, имени и отчества лица вне зависимости от контекста является распространением персональных данных. Новое определение более точно соответствует положению ст. 2 Конвенции Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных (ETS N 108) (заключена в г. Страсбурге, 28 января 1981 г.), согласно которому персональной информацией признана любая информация, касающаяся конкретного или могущего быть идентифицированным лица (субъекта данных).

Тем не менее остается вопрос о том, каким должен быть объем информации, чтобы можно было считать ее персональными данными. Так, заслуживает интерес точка зрения С.П. Гришаева, который предлагает считать персональными данными фотографию (изображение) человека, поскольку "именно по фотографии идентифицируется человек"*(12). На наш взгляд, для того чтобы считать изображение персональными данными, необходима, во-первых, оценка его идентифицирующих свойств в каждом конкретном случае (однозначно идентифицировать человека на фотографии низкого качества может быть невозможно), а во-вторых, оценка информационного наполнения самой фотографии. Если кроме того факта, что на снимке запечатлено конкретное лицо, он не позволяет извлечь никаких сведений, относиться к нему как к персональным данным нельзя, точно так же как нельзя считать персональными данными фамилию, имя и отчество лица, использованные вне какого-либо контекста.

Остается открытым вопрос о целях использования персональных данных, другими словами, - попадают ли под определение комментируемой статьи сведения, относящиеся к идентифицируемому на их основании лицу, если форма представления этих сведений не предусматривает их автоматизированной обработки (см. п. 1 ст. 1).

Суды по-разному отвечают на этот вопрос.

Примеры: Липецкий областной суд пришел к выводу, что предписание Ростехнадзора, вывешенное на доске объявлений кооператива и содержащее фамилию, имя, отчество, номер гаража и домашний адрес истца, не нарушает закона о персональных данных, поскольку сведения о персональных данных истца получены гаражным кооперативом не в связи с их обработкой (апелляционное определение Липецкого областного суда от 06.06.2012 по делу N 33-1235/2012).

В то же время Рязанский областной суд пришел к выводу, что, опубликовав в газете "Новая газета Еженедельный рязанский выпуск" от 01.04.2010 N 13Р в рубрике, отведенной для публикации читательской почты, письмо, содержащее персональные данные лица, а именно: фамилию, имя, отчество, домашний адрес, должность и место работы, - редакция нарушила закон о персональных

данных (несмотря на то, что публикация в газете не является автоматизированной обработкой данных) (см. определение Рязанского областного суда от 25.04.2012 N 33-686).

Судебная практика содержит множество примеров как первой, так и второй позиции.

На наш взгляд, необходимо различать два понятия - персональные данные и тайну частной жизни. Несмотря на то что тайна частной жизни (личная и семейная тайна) - достаточно широкое понятие, не получившее точного нормативного закрепления и, в принципе, охватывающее персональные данные, отдельно взятые факты о лице (такие как фамилия, имя, отчество, место работы, адрес и др., а также сведения о большинстве повседневных событий, связанных с этим лицом*(13)) вряд ли могут считаться тайной, поскольку по своему характеру эти сведения являются общедоступными и могут быть непроизвольно получены любым случайным лицом. Например, отвечая на вопрос, где находится мой коллега, я не могу быть обвиненным в разглашении личной тайны, даже если этот коллега заинтересован в неразглашении своего местонахождения. Институт личной тайны защищает личность от злонамеренного умышленного вмешательства в личную жизнь, зачастую связанного с использованием властных полномочий (не случайно в Конституции РФ неприкосновенность частной жизни объединена в одну статью с тайной переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений). Персональные данные впервые появляются в связи с их автоматизированной обработкой. Часть этих данных практически является общедоступной и может быть получена заинтересованным лицом из самых разных источников (на что зачастую и ссылаются суды, отказывая в удовлетворении исков субъектам персональных данных*(14)). Другие данные являются чисто "техническими" и не несут никакой семантической нагрузки, например, номер паспорта, ИНН, данные кредитной карты и др., но между тем именно они чаще всего и становятся объектом злоупотреблений, масштаб которых возрастает при возможностях автоматизированной обработки.

Анализируя общественную опасность нарушений в области обработки персональных данных в государственных автоматизированных системах, можно выделить две основные угрозы утечки персональных данных. Первое из них - предложение баз данных на черном рынке - представляет собой достаточно известное и широко обсуждаемое явление. Общественная опасность обуславливается массовостью нарушений прав человека, поскольку пострадавшим является каждый, сведения о ком были преданы огласке. Так, в марте 2007 г. в продаже оказалась база данных о ВИЧ-инфицированных жителях Тольятти, содержащая 7 338 фамилий с адресами. Базы данных объектов недвижимости и налоговых платежей затрагивают права и законные интересы на порядок большего числа людей, но более серьезную опасность представляет второй вариант преступного деяния, связанного с нарушением конфиденциальности персональных данных. Он связан с тенденцией интеграции государственных АИС и слияния государственных баз данных. Лицо, имеющее доступ к интегрированной АИС (например, коррумпированный сотрудник

исполнительных органов), может получить исчерпывающую информацию о конкретном, интересующем его человеке. В отличие от первого случая, когда общественная опасность выражается в степени охвата незаконно полученной информации, здесь общественная опасность выражается в степени полноты информации. Исчерпывающую информацию о человеке легко использовать в целях шантажа, оказания давления на политического оппонента, "кражи личности" и т.д. При этом степень латентности такого преступления возрастает в разы, поскольку на прилавках лотков не появятся базы данных, свидетельствующие о факте утечки информации*(15). Данная угроза возникает именно при автоматизированной обработке персональных данных.

Здесь уместно процитировать И.Л. Бачило: "Креативность и социальная активность индивида теснейшим образом связаны с информационной открытостью личности перед обществом и государством. Это неравнозначно раскрытию информации о частной жизни человека, которая при всех условиях принадлежит только ему и составляет его ресурс. Данный ресурс становится достоянием общественности или государственных органов только при добровольном его предоставлении и раскрытии в интересах самого индивида. Здесь важно также подчеркнуть значение различий между персональными стандартными данными, которые нужны государственным структурам, равно как и самому гражданину, и сугубо личной, частной информацией, которая включается в другие информационные поля только по желанию индивида и под его контролем"*(16).

Таким образом, понятие персональных данных по смыслу закона включает их представление на материальном носителе в виде, пригодном для автоматизированной обработки (или в аналогичной по возможностям информационной системе - картотеке, других систематизированных собраниях). Однако следует учитывать, что закон позволяет расширительное толкование и суды могут придерживаться иной точки зрения.

Понятие персональных данных содержится также в ТК РФ. Согласно ст. 85 персональные данные работника - это информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Данное определение конкретизирует общее понятие персональных данных применительно к сфере трудовых отношений и не противоречит ему.

2. Вводя специального субъекта правоотношений, связанных с обработкой персональных данных,- оператора персональных данных, законодатель указывает две категории таких субъектов.

Состав первой категории определяется однозначно. Любое физическое или юридическое лицо, государственный или муниципальный орган, выполняющий любые действия с персональными данными (включая перечисленные в п. 3 комментируемой статьи), является оператором персональных данных. В частности, оператором персональных данных будет выступать:

а) любая организация, ведущая кадровый учет своих сотрудников (а также нанимающая работников по договорам гражданско-правового характера). Специальные требования для таких операторов персональных данных устанавливаются в ст. 86 ТК РФ. В частности, работодатель обязан:

обрабатывать персональные данные работника исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

все персональные данные работника получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие;

не обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

не обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных настоящим ТК РФ или иными федеральными законами;

б) любая организация, собирающая данные о своих клиентах (в том числе кредитно-финансовые учреждения, операторы сотовой связи, организации розничной торговли, предлагающие участие в персональных бонусных программах и т.д.);

в) организация, использующая автоматизированные информационные системы для управления информацией о взаимодействии с контрагентами, если в числе последних выступают юридические лица;

г) ассоциации, объединения, союзы, хранящие персональные данные своих членов - физических лиц;

д) медицинские и образовательные учреждения, диссертационные советы и т.д.

Не до конца ясно, что подразумевал законодатель под второй категорией - лица, непосредственно не выполняющие обработку данных, но определяющие цели обработки, состав обрабатываемых персональных данных, конкретные операции, совершаемые с персональными данными. Возможно, речь здесь идет о государственных и муниципальных органах, издающих в пределах своей компетенции локальные нормативно-правовые акты, регулирующие обработку персональных данных в подведомственных организациях. В отношении таких персональных данных эти органы также будут считаться операторами; в том числе, на них распространяется обязанность применения правовых мер по обеспечению безопасности таких данных, осуществления аудита соответствия обработки персональных данных комментируемому закону и т.д.

3. Любое действие с персональными данными, независимо от того, используются ли при совершении данного действия средства автоматизации или нет, является обработкой персональных данных.

Здесь важно еще раз отметить, что по смыслу закона им регулируется автоматизированная обработка персональных данных, а также обработка персональных данных без использования вычислительной техники, если она соответствует характеру действий, совершаемых с ее использованием.

Законодатель исходит из той предпосылки, что автоматизированная обработка персональных данных позволяет осуществлять накопление большого количества таких данных и легко осуществлять поиск (выборку) нужных сведений в этом информационном массиве, что увеличивает общественную опасность утечки (кражи) персональных данных и, собственно, влечет необходимость специального правового регулирования соответствующих отношений. Помимо автоматизированных информационных систем, такие возможности открывают и большие систематизированные картотеки (в качестве исторического примера уместно вспомнить знаменитую картотеку НКВД).

Однако если рассматривать технологический процесс обработки персональных данных, то среди этапов этого процесса встречаются отдельные действия, которые даже при использовании автоматизированных информационных систем будут полностью выполняться вручную. Например, часто вручную осуществляется сбор персональных данных (так, организация, оказывающая услуги, может получить данные клиента по телефону). В связи с этим возникает вопрос, следует ли считать это отдельное действие обработкой персональных данных, а лицо, записывающее персональные данные, - представителем оператора, связанным обязанностью следить за безопасностью полученных данных, на который комментируемый пункт отвечает утвердительно, в то время как более общее положение п. 1 ст. 1 - отрицательно. На наш взгляд, ответ на этот вопрос может быть дан лишь в контексте всего технологического процесса. Если технологический процесс, этапом которого является сбор персональных данных, предполагает последующее включение этих данных в состав информационной системы (автоматизированной или картотеки), хранение, систематизацию и поиск в рамках такой системы, то следует считать такое действие обработкой персональных данных в контексте комментируемого закона. Если же процесс заключается в том, чтобы получить такие данные (например, в телефонном разговоре) для однократного использования (например, организации встречи с клиентом), то это действие не следует рассматривать как обработку персональных данных (даже если клиент сообщил в телефонном разговоре достаточно подробную информацию о себе).

4. Законодатель включил в новую редакцию ст. 3 комментируемого закона понятие автоматизированной обработки персональных данных - обработка персональных данных с использованием средств вычислительной техники.

Новому положению противоречит п. 1 постановления Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", согласно которому обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Предыдущее определение не вполне отражало специфику предметной

области. Как справедливо отмечал А. Вифлеемский, оно позволяло констатировать, что "подавляющее большинство информационных систем в государственных и муниципальных учреждениях формально можно рассматривать как осуществляемые без использования средств автоматизации (включая значительную часть бухгалтерского программного обеспечения). Ведь все лицевые карточки в этих системах правятся в соответствующих окнах вручную. Для уничтожения лицевых карточек также необходимо их выделение в списке оператором и нажатие специальной клавиши для удаления данных. Даже архивация осуществляется специальной программой, которая запускается человеком"*(17). Отделяя автоматизированную обработку персональных данных от неавтоматизированной, законодатель не учитывал, что на самом деле существует три возможных режима обработки данных: ручной (когда обработка осуществляется исключительно человеком), автоматизированный (с помощью средств вычислительной техники при участии человека) и автоматический (без участия человека). В рассматриваемом постановлении речь шла скорее о неавтоматической обработке персональных данных, причем ключевым действием, затронутым в законе, являлось использование. Ранняя редакция комментируемого закона понимала под использованием персональных данных действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц. Речь шла о том, что действия, выполняемые информационной системой в автоматическом режиме, могли получить статус юридических фактов, то есть создавать права и обязанности для субъектов персональных данных. В текущей редакции закона определение использования изъято, хотя обозначенная проблема не исчезла и может проявиться уже в 2014 г., когда начнется повсеместное внедрение универсальных электронных карт граждан.

В настоящее время Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, противоречит в части ключевого определения федеральному закону и должно быть пересмотрено.

5. Новая редакция закона разделила понятия распространения и предоставления персональных данных. В первом случае речь идет о раскрытии персональных данных неопределенному кругу лиц (например, посредством СМИ, интернет-сайтов, продажи баз с персональными данными и т.д.), а во втором - их раскрытии конкретному лицу или кругу лиц. В настоящее время различия в правовом регулировании этих действий практически нет. Распространение, предоставление и доступ объединяются общим понятием "передача персональных данных", которая регулируется, к примеру, специальной статьей ТК РФ (ст. 88). Понятие доступа в законе не раскрывается. Под ним, на наш взгляд, следует понимать предоставление возможности самостоятельного получения персональных данных из информационной системы оператора персональных данных (возможно, не любых, а в соответствии с заданными ограничениями).

6. Термин "блокирование" применительно к данным впервые в федеральном законодательстве появился в главе 28 УК РФ "Преступления в сфере компьютерной информации". Состав преступлений, ответственность за которые предусмотрена ст. 272 (неправомерный доступ к компьютерной информации), 273 (создание, использование и распространение вредоносных компьютерных программ), 274 (нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей), включает блокирование компьютерной информации (то есть данных) в качестве одного из возможных квалифицирующих последствий неправомерного деяния. При этом определения понятия "блокирование" УК РФ не давал, что служило поводом к критике главы 28. Давая комментарий к названным положениям УК РФ, авторы предлагали следующие варианты определения:

"блокирование информации - обеспечение недоступности к ней, невозможности ее использования в результате запрещения дальнейшего выполнения последовательности команд либо выключения из работы какого-либо устройства, а равно выключения реакции какого-либо устройства ЭВМ, системы или сети ЭВМ при сохранении самой информации"*(18);

"под блокированием понимается временная или постоянная невозможность доступа к информации со стороны законного пользователя"*(19);

"блокирование информации заключается в создании различного рода временных или постоянных препятствий по правомерному доступу к ней, невозможности использования информации (полностью или частично) при ее полной сохранности"*(20);

"блокирование информации - это невозможность ее использования при сохранности такой информации"*(21).

Последнее определение представляется нам наиболее точным. В комментируемом законе законодатель определил блокирование персональных данных как временное прекращение обработки, то есть каких-либо действий с персональными данными. При этом блокирование - обратимая операция (см. ч. 2 ст. 21 комментируемого закона: блокирование может быть снято, например, после уточнения неточных персональных данных), таким образом, обеспечивается сохранность информации.

Следует, однако, отметить техническую небрежность в изменениях, внесенных Федеральным законом от 25.07.2011 N 261-ФЗ. Ранее блокирование определялось как "временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи". Заменив конкретный перечень действий с персональными данными обобщающим термином "обработка", законодатель расширил их такими действиями, как хранение и блокирование. Буквальное толкование нормы закона ведет к логическому противоречию (блокирование подразумевает временное прекращение блокирования), а также позволяет заключить, что блокирование обязывает оператора персональных данных временно прекратить их хранение, что, очевидно, не соответствует намерениям законодателя. На самом деле духу закона больше соответствует предыдущая формулировка.

7. Способы уничтожения персональных данных законодатель делит на две

категории:

физическое уничтожение носителя;

безвозвратное уничтожение информации с носителя.

Конкретный способ определяется в регламенте обработки персональных данных и может зависеть как от вида носителя, так и от характера персональных данных. В частности, информация на бумажном носителе уничтожается путем уничтожения носителя (шреддирование, термическая обработка).

8. Обезличивание персональных данных означает сохранение содержательной части информации, но устранение возможности определить на основании такой информации субъекта персональных данных, к которому она относится.

Обезличивание данных - это операция, порождающая новую (результатную) информацию на основании уже имеющейся (исходной). Само по себе обезличивание не означает уничтожение исходной информации, на наш взгляд, обезличенные персональные данные и исходные (не обезличенные) могут обрабатываться совместно, для различных целей. Однако по смыслу комментируемого закона обезличивание предполагает уничтожение исходной информации.

Закон содержит оговорку "без использования дополнительной информации", не уточняя, каким должен быть объем этой дополнительной информации. Очевидно, такая дополнительная информация не должна относиться к данным открытого доступа (хотя, на наш взгляд, законодателю стоит уточнить этот момент).

Обезличенные персональные данные могут использоваться в статистических или иных исследовательских целях без дополнительных ограничений (п. 9 ст. 6).

9. Под информационной системой Федеральный закон от 27.07.2006 N 149-ФЗ понимает совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Комментируемый закон уточняет это определение, конкретизируя характер информации в базах данных - персональные данные. Базой данных, согласно ст. 1260 ГК РФ, является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).

10. В определении трансграничной передачи используется термин "передача", подразумевающий доступ, предоставление и распространение. Представляется, что любое распространение персональных данных по своей природе включает трансграничную передачу данных (поскольку в неопределенный круг лиц включаются и иностранные лица), то есть действия по доступу и предоставлению персональных данных иностранному лицу, органу власти иностранного государства либо российскому лицу, находящемуся на территории иностранного государства. Представляется, что любая операция по передаче данных посредством глобальных компьютерных сетей (маршрут прохождения пакетов по которым физически может проходить где угодно), хотя и

не является в строго формальном смысле трансграничной передачей, должна рассматриваться как таковая в контексте необходимых мер защиты (сквозное шифрование, безопасные протоколы и т.д.).

Статья 4. Законодательство Российской Федерации в области персональных данных

1. Комментируемая статья устанавливает систему нормативных правовых актов, регулирующих правоотношения в сфере обработки персональных данных.

Часть первая комментируемой статьи непосредственно провозглашает законодательную основу регулирования отношений в сфере обработки персональных данных. Согласно ей законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации.

Конституция РФ принята на всенародном голосовании 12 декабря 1993 г. и является основным законом Российской Федерации. Конституция имеет высшую юридическую силу, прямое действие и применяется на всей территории РФ. Законы и иные правовые акты, принимаемые в РФ, не должны противоречить Конституции. Органы государственной власти, органы местного самоуправления, должностные лица, граждане и их объединения обязаны соблюдать Конституцию и законы. Важное место Конституция РФ отводит человеку, его правам и свободам, которые являются высшей ценностью. Обязанность государства по признанию, соблюдению и защите прав и свобод человека и гражданина закреплена в ст. 2 Конституции РФ.

В контексте комментируемого закона Конституция РФ выступает основным гарантом реализации комментируемого закона и соблюдения прав граждан в процессе его реализации (см. подробнее об этом комментарий к ст. 2).

Международные договоры Российской Федерации согласно ст. 5 Федерального закона от 15.07.1995 N 101-ФЗ "О международных договорах Российской Федерации" наряду с общепризнанными принципами и нормами международного права являются составной частью правовой системы Российской Федерации. Международные договоры Российской Федерации заключаются, выполняются и прекращаются в соответствии с общепризнанными принципами и нормами международного права, положениями самого договора, Конституцией Российской Федерации, Федеральным законом от 15.07.1995 N 101-ФЗ.

Международный договор Российской Федерации означает международное соглашение, заключенное Российской Федерацией с иностранным государством (или государствами), с международной организацией либо с иным образованием, обладающим правом заключать международные договоры, в письменной форме, и регулируемое международным правом, независимо от того, содержится такое соглашение в одном документе или в нескольких связанных между собой документах, а также независимо от его конкретного наименования.

Выполнение международных договоров регулируется ст. 31 Федерального закона от 15.07.1995 N 101-ФЗ, согласно которой они подлежат добросовестному выполнению в соответствии с условиями самих международных договоров, нормами международного права, Конституцией РФ, указанным законом, иными

актами законодательства Российской Федерации. Российская Федерация до вступления для нее международного договора в силу воздерживается с учетом соответствующих норм международного права от действий, которые лишили бы договор его объекта и цели. Международный договор подлежит выполнению Российской Федерацией с момента вступления его в силу для Российской Федерации.

В соответствии со ст. 38 Федерального закона от 15.07.1995 N 101-ФЗ в случае прекращения международного договора Российская Федерация освобождается от всякого обязательства выполнять договор в дальнейшем, если договором не предусматривается иное, а также если не имеется иной договоренности с другими его участниками и договор не влияет на права, обязательства или юридическое положение Российской Федерации, возникшие в результате выполнения договора до его прекращения.

Положения официально опубликованных международных договоров Российской Федерации, не требующие издания внутригосударственных актов для применения, действуют в Российской Федерации непосредственно. Для осуществления иных положений международных договоров Российской Федерации принимаются соответствующие правовые акты.

Основными международными актами в области защиты персональных данных являются следующие:

- Всеобщая декларация прав человека, принятая на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 A (III) от 10.12.1948, которая провозглашает, что никто не может подвергаться произвольному вмешательству в личную и семейную жизнь; каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств (ст. 12);

- Международный пакт о гражданских и политических правах (Нью-Йорк, 19.12.1966);

- Конвенция Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных (ETS N 108) (заключена в г. Страсбурге, 28 января 1981 г.).

В Конвенции определяется порядок сбора и обработки данных о личности, принципы хранения и доступа к этим данным, способы физической защиты данных. Конвенция гарантирует соблюдение прав человека при сборе и обработке персональных данных, а также запрещает обработку данных о расе, политических взглядах, здоровье, религии без соответствующих юридических оснований. Данная Конвенция была ратифицирована Федеральным законом от 19.12.2005 N 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных" с отдельными заявлениями, а именно, Российская Федерация заявила, что не будет применять Конвенцию к персональным данным:

а) обрабатываемым физическими лицами исключительно для личных и семейных нужд;

б) отнесенным к государственной тайне в порядке, установленном законодательством Российской Федерации о государственной тайне;

в) которые не подвергаются автоматизированной обработке, если применение Конвенции соответствует характеру действий, совершаемых с

персональными данными без использования средств автоматизации.

Кроме того, Российская Федерация оставила за собой право устанавливать ограничения права субъекта персональных данных на доступ к персональным данным о себе в целях защиты безопасности государства и общественного порядка.

- Директива 95/46/ЕС Европейского парламента и Совета ЕС от 24.10.1995 о защите физических лиц в отношении обработки персональных данных и свободного обращения таких данных.

Согласно положениям данной Директивы персональные данные означают любую информацию, связанную с идентифицированным или идентифицируемым физическим лицом (субъектом данных). Идентифицируемым лицом является лицо, которое может быть идентифицировано прямо или косвенно, в частности посредством ссылки на идентификационный номер или на один или несколько факторов, специфичных для его физической, психологической, ментальной, экономической, культурной или социальной идентичности.

Обработка персональных данных означает любую операцию или набор операций, выполняемых над персональными данными, как автоматическими средствами, так и без таковых. Это сбор, запись, организация, хранение, актуализация или изменение, извлечение, консультирование, использование, раскрытие посредством передачи, распространения или предоставления иного доступа, группировка, блокирование, стирание или удаление.

Директива вводит понятие "контролера персональных данных" - это физическое или юридическое лицо, официальный орган, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных. В случае, когда цели или средства обработки определяются национальным законодательством или законами или нормами Сообщества, контролер или особые критерии его назначения могут устанавливаться национальным законом или законом Сообщества;

- Директива 97/66/ЕС Европейского парламента и Совета ЕС от 15.12.1997, касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций;

- Директива 2002/58/ЕС Европейского парламента и Совета ЕС от 12.07.2002 об обработке персональных данных и защите информации о частной жизни в сфере электронных коммуникаций (Директива о конфиденциальности информации о частной жизни в сфере электронных коммуникаций).

Часть 4 комментируемой статьи устанавливает приоритет международных договоров Российской Федерации в области регулирования отношений по обработке персональных данных, а именно, если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены комментируемым законом, применяются правила международного договора. Указанная норма дублирует ч. 2 ст. 5 Федерального закона от 15.07.1995 N 101-ФЗ.

2. Собственно законодательство Российской Федерации в области обработки персональных данных включает в себя следующие нормативные правовые акты в порядке приоритета:

1) комментируемый закон, осуществляющий непосредственное прямое

регулирование правоотношений в области обработки персональных данных;

2) иные федеральные законы, определяющие случаи и особенности обработки персональных данных, а именно:

Федеральный закон от 15.11.1997 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

Федеральный закон от 03.04.1995 N 40-ФЗ "О федеральной службе безопасности";

Федеральный закон от 07.07.2003 N 126-ФЗ "О связи";

Федеральный закон от 12.08.1995 N 144-ФЗ "Об оперативно-розыскной деятельности";

Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне";

Федеральный закон от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации";

Федеральный закон от 25.01.2002 N 8-ФЗ "О Всероссийской переписи населения";

Федеральный закон от 29.11.2010 N 326-ФЗ "Об обязательном медицинском страховании в Российской Федерации";

Федеральный закон от 22.10.2004 N 125-ФЗ "Об архивном деле в Российской Федерации";

другие федеральные законы.

Часть норм, определяющих отдельные случаи регулирования обработки персональных данных, содержатся в кодексах, которые также являются федеральными законами. Так, СК РФ содержит перечень персональных данных, подлежащих установлению в отношении лиц. желающих усыновить ребенка, установить в отношении него опеку / попечительство, либо взять ребенка в приемную семью (ст. 123 СК РФ). Статьи 85-90 ТК РФ регулируют защиту персональных данных работника. Статья 85.1 ВК РФ регулирует порядок передачи персональных данных пассажиров воздушных судов в автоматизированные централизованные базы персональных данных о пассажирах.

Ряд норм, содержащихся в кодексах, устанавливают ответственность за нарушение законодательства в области обработки персональных данных. Например, нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц - от пятисот до одной тысячи рублей; на юридических лиц - от пяти тысяч до десяти тысяч рублей в соответствии со ст. 13.11 КоАП РФ.

Кроме того, административная ответственность предусмотрена за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14 КоАП РФ).

Нецелевая обработка персональных данных может повлечь также уголовную ответственность. Так, ст. 137 УК РФ предусматривает уголовную

ответственность за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Статья 272 УК РФ устанавливает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, в том числе баз персональных данных.

3. 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. Указанные нормативные правовые акты по своей юридической силе являются подзаконными. 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. Среди данной категории нормативных правовых актов, регулирующих отношения сфере обработки персональных данных, можно выделить следующие:

1) указы и распоряжения Президента Российской Федерации:

Указ Президента РФ от 06.03.1997 N 188 "Об утверждении перечня сведений конфиденциального характера";

Указ Президента РФ от 30.05.2005 N 609 "Об утверждении положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела";

Указ Президента РФ от 17.03.2008 N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";

распоряжение Президента РФ от 10.07.2001 N 366-РП "О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных" и пр.;

2) акты Правительства Российской Федерации:

- постановление Правительства РФ от 03.11.1994 N 1233 "Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти";

постановление Правительства РФ от 06.07.2008 N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";

постановление Правительства РФ от 15.09.2008 N 687 "Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

распоряжение Правительства РФ от 15.08.2007 N 1055-Р "О плане

подготовки проектов нормативных актов, необходимых для реализации Федерального закона "О персональных данных";

постановление Правительства РФ от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и пр.;

3) нормативные правовые акты органов федеральных органов исполнительной власти:

приказ Министерства связи и массовых коммуникаций от 21.12.2011 N 346 "Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги "Ведение реестра операторов, осуществляющих обработку персональных данных";

приказ ФСТЭК России от 05.02.2010 N 58 "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных";

приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных";

приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 19.08.2011 N 706 "Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществить обработку) персональных данных";

приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 20.06.2012 N 621 "О Консультативном совете при уполномоченном органе по защите прав субъектов персональных данных";

приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 03.12.2012 N 1255 "Об утверждении Положения об обработке и защите персональных данных в центральном аппарате Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций", и пр.;

4) а также акты органов местного самоуправления в пределах их полномочий.

Порядок опубликования и вступления в силу указов и распоряжений Президента Российской Федерации, постановлений и распоряжений Правительства Российской Федерации, а также нормативных правовых актов федеральных органов исполнительной власти регулируется Указом Президента РФ от 23.05.1996 N 763 "О порядке опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти".

Так, по общему правилу, установленному данным указом, акты Президента Российской Федерации, имеющие нормативный характер, и акты Правительства Российской Федерации, затрагивающие права, свободы и обязанности человека и гражданина, устанавливающие правовой статус федеральных органов исполнительной власти, а также организаций, вступают в силу одновременно на всей территории Российской Федерации по истечении семи дней после дня их

первого официального опубликования. Акты Президента Российской Федерации и акты Правительства Российской Федерации в течение 10 дней после дня их подписания подлежат официальному опубликованию в "Российской газете", Собрании законодательства Российской Федерации и на "Официальном интернет-портале правовой информации" (www.pravo.gov.ru), функционирование которого обеспечивает Федеральная служба охраны Российской Федерации.

Нормативные правовые акты федеральных органов исполнительной власти вступают в силу одновременно на всей территории Российской Федерации по истечении десяти дней после дня их официального опубликования, если самими актами не установлен другой порядок вступления их в силу. Нормативные правовые акты федеральных органов исполнительной власти подлежат официальному опубликованию в "Российской газете" в течение десяти дней после дня их регистрации, а также в Бюллетене нормативных актов федеральных органов исполнительной власти государственного учреждения - издательства "Юридическая литература" Администрации Президента Российской Федерации, который издается еженедельно. Официальным также является указанный Бюллетень, распространяемый в электронном виде федеральным государственным унитарным предприятием "Научно-технический центр правовой информации "Система" Федеральной службы охраны Российской Федерации, а также органами государственной охраны.

4. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами Российской Федерации с учетом положений комментируемого закона.

В настоящее время особенности обработки персональных данных, осуществляемой без использования средств автоматизации, регулируются постановлением Правительства Российской Федерации от 15.09.2008 N 687 "Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков). При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных

категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Глава 2. Принципы и условия обработки персональных данных

Статья 5. Принципы обработки персональных данных

Комментируемая статья устанавливает основные принципы обработки персональных данных. Необходимо отметить, что персональные данные являются категорией, способной непосредственно влиять на жизнь, в том числе личную, общественную, трудовую и пр., конкретного человека. Нарушение правил обработки персональных данных гражданина может сделать его частную жизнь достоянием гласности. Несомненно, что разные специальные категории персональных данных подлежат соответствующей специальной обработке. Однако в целях обеспечения защиты прав и свобод человека и гражданина при обработке персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, комментируемым законом устанавливаются основные начала, идеологическая база обработки персональных данных - принципы, изложенные ниже.

1) принцип законности.

Законность, как известно, является понятием достаточно широким, емким и, наверное, наиболее часто встречающимся в российском законодательстве.

Принцип законности означает верховенство закона и безусловное его исполнение гражданами и должностными лицами. Кроме того, законность характеризуется наличием специальных механизмов, гарантирующих безопасность и защиту личности от произвола, беспрепятственное осуществление гражданских прав и свобод.

Принцип законности пронизывает всю правовую систему в целом. Законность в качестве принципа провозглашена в ряде статей Конституции

России, и в большинстве законов.

Применительно к комментируемому закону принцип законности означает, что обработка персональных данных производится при строгом соблюдении норм комментируемого закона как со стороны операторов обработки персональных данных, так и со стороны граждан, предоставляющих персональные данные, а также уполномоченного органа по защите прав субъектов персональных данных. Принцип законности обработки персональных данных заключается в следующем:

приоритет комментируемого закона при обработке персональных данных в отношениях по обработке персональных данных;

единое толкование и применение комментируемого закона на всей территории России;

всеобщность комментируемого закона, а именно распространение его действия на всех лиц, находящихся на территории РФ, а также за ее пределами в соответствии с международными договорами Российской Федерации о реадмиссии;

гарантированность основных прав и свобод человека и гражданина при осуществлении обработки персональных данных;

равенство всех лиц при осуществлении обработки их персональных данных независимо от их расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни и пр. специальных категорий персональных данных;

неотвратимость наказания за нарушения комментируемого закона операторами персональных данных и иными лицами;

2) принцип справедливости.

Обработка персональных данных должна осуществлять на справедливой основе. Справедливость - понятие не менее, если не более, емкое, чем законность. Понятие справедливости носит скорее философский, чем правовой характер, и тем не менее многие нормы права основываются, прежде всего, на принципе справедливости, который применительно к конкретному типу правоотношений варьируется в своем значении. Например, принцип справедливости закреплен в ст. 6 УК РФ и означает, что наказание и иные меры уголовно-правового характера, применяемые к лицу, совершившему преступление, должны быть справедливыми, то есть соответствовать характеру и степени общественной опасности преступления, обстоятельствам его совершения и личности виновного. Статья 1101 ГК РФ содержит норму о том, что при определении размера компенсации морального вреда должны учитываться требования разумности и справедливости, где требование справедливости значит, что компенсация морального вреда должна соответствовать характеру причиненных потерпевшему нравственных и физических страданий с учетом степени вины причинителя вреда.

Принцип справедливости применительно к правоотношениям по обработке персональных данных означает, что действия по обработке персональных данных должны носить системный характер, т.е. обработка персональных данных должна осуществлять в строгом соответствии с установленным порядком (например, в порядке очередности в зависимости от даты поступления сведений

о персональных данных лица, в алфавитном порядке), без учета личной заинтересованности оператора (например, если среди лиц, чьи персональные данные обрабатываются, имеются работники оператора, то в процессе обработки их персональные данные не должны носить приоритет по отношению к персональным данных других лиц);

3) принцип целевой обработки персональных данных.

Комментируемый закон устанавливает принцип целевой обработки персональных данных. Поскольку, как указывалось выше, персональные данные могут носить сугубо личный характер, нецелевое использование персональных данных может являться вмешательством в частную жизнь лица и причинить ему тем самым значительный вред. Поскольку цель комментируемого закона заключается в защите прав и свобод человека и гражданина (ст. 2 комментируемого закона), в том числе права на неприкосновенность частной жизни и пр., законодатель разумно определил в качестве основного принципа обработки персональных данных принцип цели.

Цели обработки персональных данных должны обладать следующими характеристиками:

- цель должна быть конкретной, т.е. реально существующей, предметно определенной и четко обозначенной, например, цели переписи населения сформулированы в ст. 1 Федерального закона от 25.01.2002 N 8-ФЗ, а именно: формирование официальной статистической информации о демографических, об экономических и о социальных процессах;

- цель должна быть заранее определена, т.е. операторы обработки персональных данных должны оповещать о цели обработки персональных данных заблаговременно до процесса обработки, и каждое лицо, чьи персональные данные должны подвергнуться обработке, должно быть извещено о целях обработки. При этом озвученная цель обработки персональных данных уже не подлежит изменению;

- цель обработки персональных данных должна быть законной, как в общем (должна соответствовать принципу законности), так и в узком (не должна нарушать нормы права) смыслах.

Не допускается нецелевая обработка персональных данных, т.е. обработка, несовместимая с целями сбора персональных данных. Персональные данные должны обрабатываться только в тех целях, которые изначально были установлены как цели сбора и обработки персональных данных.

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой, т.е. не допускается смешение, соединение персональных данных, собранных и обрабатываемых в разных целях.

Обработке подлежат только персональные данные, которые отвечают целям их обработки. Например, при формировании электронной базы беременных, состоящих на учете в женской консультации, оператора персональных данных - консультацию не должны интересовать сведения о судимости как самой беременной, так и отца будущего ребенка.

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. Например, при формировании базы учащихся школы в разделе, содержащем сведения о родителях или иных законных представителях учащихся, не должны отражаться сведения о бабушках и дедушках учащихся, за исключением случаев, когда последние выступают в качестве опекунов/попечителей. Указание сведений о бабушках и дедушках учащихся в данном случае будет излишним.

Нецелевая обработка персональных данных является нарушением комментируемого закона и влечет за собой ответственность (ст. 24 комментируемого закона). Например, нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц - от пятисот до одной тысячи рублей; на юридических лиц - от пяти тысяч до десяти тысяч рублей в соответствии со ст. 13.11 КоАП РФ.

Кроме того, административная ответственность предусмотрена за разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14 КоАП РФ).

Нецелевая обработка персональных данных может повлечь также уголовную ответственность. Так, ст. 137 УК РФ предусматривает уголовную ответственность за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Статья 272 Уголовного кодекса РФ устанавливает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, в том числе баз персональных данных;

4) принцип точности, достаточности и актуальности персональных данных по отношению к целям их обработки.

Точность персональных данных означает полное соответствие содержания персональных данных заявленным целям их обработки. Персональные данные считаются достаточными, если их объем и содержание позволяют достигнуть целей обработки. Актуальность персональных данных означает, что в момент обработки персональных данных последние являются своевременными, достоверными и значимыми для достижения поставленной цели обработки персональных данных. Например, персональные данные, собранные после подведения итогов переписи населения, являются неактуальными, поскольку были собраны несвоевременно и утратили свою значимость по отношению к целям обработки.

Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

5) принцип срочного хранения.

Поскольку персональные данные по форме представляют собой информацию, содержащую сведения о субъекте и отдельных аспектах его жизни, представляется логичным урегулирование порядка и срока хранения указанной информации. Обработка персональных данных преследует достижение установленных целей обработки. По достижению указанных целей собранные персональные данные утрачивают свою актуальность. Возникает вопрос о дальнейшем использовании и хранении обработанных персональных данных. Комментируемая статья закрепляет принцип срочного хранения персональных данных, а именно хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных. Срок хранения персональных данных может быть установлен:

а) федеральным законом;

Так, в ст. 4 Федерального закона от 25.01.2002 N 8-ФЗ указано, что порядок хранения переписных листов и иных документов Всероссийской переписи населения определяется Правительством Российской Федерации. В частности, Правила хранения переписных листов и иных документов Всероссийской переписи населения 2010 года утверждены постановлением Правительства РФ от 26.07.2010 N 554. Согласно указанным Правилам хранение переписных листов Всероссийской переписи населения 2010 года в электронном виде осуществляется следующим образом:

один экземпляр хранится постоянно в Федеральной службе государственной статистики;

два экземпляра с программным обеспечением для просмотра переписных листов передаются до 01 января 2014 г. на постоянное хранение в Государственный архив Российской Федерации.

Переписные листы Всероссийской переписи населения 2010 года на бумажных носителях после завершения их автоматизированной обработки хранятся в Федеральной службе государственной статистики и ее территориальных органах в течение одного года со дня официального опубликования предварительных итогов Всероссийской переписи населения 2010 года.

Статья 87 ТК РФ устанавливает, что порядок хранения и использования персональных данных определяется работодателем самостоятельно. Таким образом, срок хранения персональных данных регулируется локальным нормативным актом (инструкцией, положением) о порядке работы с персональными данными работников. Разработка локального нормативного акта (инструкции, положения) о порядке работы с персональными данными работников является обязанностью работодателя, невыполнение которой влечет наложение административного штрафа по ст. 5.27 КоАП РФ;

б) договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Зачастую на практике передача субъектом своих персональных данных происходит при возникновении гражданско-правовых отношений, например, при заключении договоров об оказании услуг связи, договоров страхования, договоров оказания платных медицинских услуг, кредитных договоров и пр. Поскольку гражданско-правовые отношения основываются на принципах

свободы договора и диспозитивности, то процесс обработки, в т.ч. хранения, персональных данных урегулирован лишь общими нормами, а именно комментируемым законом. Специальное, детальное урегулирование зависит от волеизъявления сторон возникшего обязательства. В таких случаях срок хранения персональных данных субъекта может быть урегулирован в договоре.

Если срок хранения персональных данных не установлен ни законом, ни договором, то в данном случае хранение персональных данных должно осуществляться не дольше, чем этого требуют цели обработки 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. Например, в случае ликвидации религиозной организации персональные данные ее членов подлежат уничтожению в связи с утратой необходимости достижения цели обработки персональных данных.

Статья 6. Условия обработки персональных данных

1. Комментируемая статья устанавливает условия обработки персональных данных, т.е. обстоятельства, наличие которых позволяет осуществлять обработку персональных данных субъекта. В качестве общего условия обработки персональных данных законодатель указывает соблюдение принципов и правил, предусмотренных комментируемым законом. Принципы комментируемого закона закреплены в ст. 5 (см. подробнее об этом комментарий к ней). Общее условие обработке персональных данных, заключающееся в соблюдении принципов и правил, установленных комментируемым законом, является производной общеправового принципа законности, на котором основывается обработка персональных данных в целом.

Обработка персональных данных допускается в следующих случаях:

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

Согласие субъекта персональных данных на обработку его персональных данных должно быть выражено в письменной форме. Статья 9 комментируемого закона устанавливает требования к содержанию письменного согласия на обработку персональных данных (см. подробнее об этом комментарий к ней). Использование персональных данных субъекта без его письменного согласия влечет за собой административную (ст. 13.11, 13.14 КоАП РФ), уголовную (ст. 137, 272 УК РФ) либо гражданско-правовую (ст. 15, 1064, 1101 ГК РФ) ответственность в зависимости от степени общественной опасности деяния и тяжести наступивших последствий. Необходимость наличия письменного согласия субъекта для обработки персональных данных находит свое отражение в судебной практике.

Так, например, в постановлении Первого арбитражного апелляционного суда от 12.10.2011 N 01АП-4438/11, разрешившем спор, связанный с получением согласия на обработку персональных данных в сфере оказания услуг связи, отмечено, что получение согласия субъекта (абонента) на обработку персональных данных, за исключением установленных Правилами оказания услуг подвижной связи, утвержденных постановлением Правительства РФ от

25.05.2005 N 328, условий, является обязательным. При этом в соответствии с ч. 4 ст. 9 комментируемого закона письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя: фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе; наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных; цель обработки персональных данных; перечень персональных данных, на обработку которых дается согласие субъекта персональных данных; перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных; срок, в течение которого действует согласие, а также порядок его отзыва; собственноручную подпись субъекта персональных данных. Таким образом, положение данной нормы предусматривает обязательные требования к содержанию письменного согласия субъекта персональных данных на обработку своих 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.

В данном случае обработка персональных данных субъекта не требует письменного согласия и осуществляется в силу закона или международного договора Российской Федерации.

Письменное согласие субъекта персональных данных на обработку его персональных данных оператором не требуется, если обработка персональных данных необходима оператору в целях осуществления возложенных на него законом функций, полномочий и обязанностей.

Так, в соответствии со ст. 9, ч. 1 ст. 15 Федерального закона от 01.04.1996 N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования" страхователь вправе потребовать от работника представить ему сведения, подлежащие внесению в его индивидуальный лицевой счет застрахованного лица, при приеме на работу и при изменении данных сведений, а затем должен предоставить их в соответствующий орган Пенсионного фонда РФ. Таким образом, страхователь вправе осуществлять обработку персональных данных субъекта (работника) без его письменного согласия в целях исполнения возложенной на него обязанности по передаче сведений о работнике в Пенсионный фонд РФ.

Письменное согласие субъекта персональных данных на обработку его персональных данных оператором также не требуется, если обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии (Федеральный закон от 25.11.2009 N 266-ФЗ "О внесении изменений в Федеральный закон "О персональных данных" по вопросам реализации международных договоров Российской Федерации о реадмиссии") (см. подробнее об этом комментарий к ст. 10 комментируемого закона);

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.

Федеральным законом от 02.10.2007 N 229-ФЗ "Об исполнительном производстве" на судебных приставов возложена задача по своевременному исполнению судебных актов, актов других органов и должностных лиц, определены их права, обязанности и полномочия во взаимоотношениях с иными государственными органами, а также другими организациями, должностными лицами и гражданами.

Согласно п. 2, 17 ч. 1 ст. 64 Федерального закона от 02.10.2007 N 229-ФЗ в процессе исполнения требований исполнительных документов судебный пристав-исполнитель вправе запрашивать необходимые сведения у физических лиц, организаций и органов, находящихся на территории Российской Федерации, а также на территориях иностранных государств, в порядке, установленном международным договором Российской Федерации, получать от них объяснения, информацию, справки, а также совершать иные действия, необходимые для своевременного, полного и правильного исполнения исполнительных документов.

Таким образом, Федеральный закон от 02.10.2007 N 229-ФЗ дает право судебному приставу-исполнителю осуществлять обработку персональных данных лица (сбор, накопление, уточнение, использование и т.д.) без его письменного согласия в целях исполнения судебных актов.

Так, например, в постановлении Федерального арбитражного суда Уральского округа от 09.11.2010 N Ф09-9030/10-С1 по делу N А07-5328/2010 указано, что законные требования судебного пристава-исполнителя обязательны для всех государственных органов, органов местного самоуправления, граждан и организаций и подлежат неукоснительному выполнению на всей территории Российской Федерации (ст. 6 Федерального закона от 02.10.2007 N 229-ФЗ). Таким образом, судебный пристав-исполнитель, действуя в рамках возбужденного исполнительного производства в целях реализации задач службы судебных приставов, имеет право запрашивать информацию, имеющую непосредственное отношение к исполнению судебных актов, в частности, сведения об абонентах и о зарегистрированных за указанными абонентами абонентских номерах;

4) обработка персональных данных необходима 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 N 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.

Данная норма дублируется ч. 4 ст. 7 Федерального закона от 27.07.2010 N 210-ФЗ, согласно которой для обработки органами, предоставляющими государственные и муниципальные услуги, и иными органами, участвующими в

предоставлении государственных и муниципальных услуг, персональных данных в целях предоставления государственной или муниципальной услуги по запросу заявителя, а также для обработки персональных данных при регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг и на региональных порталах государственных и муниципальных услуг не требуется получение согласия заявителя как субъекта персональных данных.

Пункт 3 ч. 1 ст. 6 Федерального закона от 27.07.2010 N 210-ФЗ устанавливает обязанность органов, предоставляющих государственные и муниципальных услуги предоставлять в иные органы, предоставляющие государственные и муниципальные услуги, многофункциональные центры по межведомственным запросам таких органов и организаций документы и информацию, необходимые для предоставления государственных и муниципальных услуг, а также получать от иных органов, предоставляющих государственные и муниципальные услуги, многофункциональных центров такие документы и информацию.

Перечень указанных документов и информации установлен Перечнем сведений, находящихся в распоряжении государственных органов субъектов Российской Федерации, органов местного самоуправления, территориальных государственных внебюджетных фондов либо подведомственных государственным органам субъектов Российской Федерации или органам местного самоуправления организаций, участвующих в предоставлении государственных или муниципальных услуг, и необходимых для предоставления государственных услуг федеральными органами исполнительной власти и органами государственных внебюджетных фондов Российской Федерации, утвержденным распоряжением Правительства РФ от 29.06.2012 N 1123-р. К таким сведениям, в частности, относятся следующие персональные данные:

сведения о нахождении гражданина на регистрационном учете в государственном учреждении службы занятости населения в целях поиска подходящей работы в качестве ищущего работу и признанного безработным, о назначенных безработному гражданину социальных выплатах, периодах участия в оплачиваемых общественных работах, переезде по направлению органов службы занятости в другую местность для трудоустройства;

сведения о неполучении ежемесячного пособия по уходу за ребенком в органах социальной защиты населения по месту жительства отца, матери ребенка (для одного из родителей в соответствующих случаях, а также для лиц, фактически осуществляющих уход за ребенком вместо матери (отца, обоих родителей) ребенка) в случае, если отец (мать, оба родителя) ребенка не работает (не служит) либо обучается по очной форме обучения в образовательных учреждениях начального профессионального, среднего профессионального и высшего профессионального образования и учреждениях послевузовского профессионального образования;

сведения, содержащиеся в направлении на медико-социальную экспертизу, выдаваемом органом социальной защиты населения, и пр.

Однако, в случае 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 представителя на обработку персональных данных указанного лица. Действие настоящей части не распространяется на лиц, признанных безвестно отсутствующими, и на разыскиваемых лиц, место нахождения которых не установлено уполномоченным федеральным органом исполнительной власти (ч. 3 ст. 7 Федеральным законом от 27.07.2010 N 210-ФЗ);

5) обработка персональных данных необходима 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.

По смыслу этой нормы одной из сторон договора должно являться лицо, осуществляющее в соответствии с указанным договором в дальнейшем обработку персональных данных субъекта, выступающего в договоре либо также в качестве стороны, либо выгодоприобретателем (например, договоры страхования), либо поручителем (например, кредитные договоры). В данном случае согласие субъекта на обработку его персональных данных не требуется.

Примером применения указанной нормы на практике может являться определение СК по гражданским делам Московского городского суда от 06.04.2012 N 33-8687, в котором подтверждена правильность выводов суда первой инстанции о том, что ответчиком не нарушаются нормы комментируемого закона при обработке персональных данных субъектов без их согласия в порядке, предусмотренном пп. 3, 5, 7 ч. 1 ст. 6 ФЗ комментируемого закона, для исполнения договоров, стороной которых являлись субъекты персональных данных.

На основании указанной нормы права и в соответствии с гл. 14 ТК РФ работодатель осуществляет обработку персональных данных работника как стороны трудового договора. Общие требования при обработке персональных данных работника и гарантии их защиты регулируются ст. 86 ТК РФ, где, в частности, указано, что работодатель вправе запрашивать только те персональные данные, обработка которых работодателю необходима для осуществления работником его трудовых обязанностей;

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

В данном случае обработка персональных данных субъекта без его согласия возможна только в случае невозможности получения последнего, если субъект, например, находится в бессознательном состоянии и при этом существует реальная угроза его жизни, здоровью или жизненно важным интересам;

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.

Так, например, ст. 2 Федерального закона от 07.08.2001 N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" установлено, что указанный закон регулирует отношения граждан Российской Федерации, иностранных граждан и лиц без гражданства, организаций, осуществляющих операции с денежными средствами или иным имуществом, а также государственных органов, осуществляющих контроль на территории Российской Федерации за проведением операций с денежными средствами или иным имуществом, в целях предупреждения, выявления и пресечения деяний, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма.

Пунктом 1 ч. 1 ст. 7 Федерального закона от 07.08.2001 N 115-ФЗ установлено, что организации, осуществляющие операции с денежными средствами или иным имуществом (в контексте комментируемого закона - операторы), обязаны идентифицировать клиента, представителя клиента и (или) выгодоприобретателя, за исключением случаев, установленных пп. 1.1 и 1.2 данной статьи, и установить сведения, указанные в статье.

К указанным сведениям в отношении физических лиц закон прямо относит фамилию, имя, а также отчество (если иное не вытекает из закона или национального обычая), гражданство, дату рождения, реквизиты документа, удостоверяющего личность, данные миграционной карты, документа, подтверждающего право иностранного гражданина или лица без гражданства на пребывание (проживание) в Российской Федерации, адрес места жительства (регистрации) или места пребывания, идентификационный номер налогоплательщика (при его наличии).

Кредитные организации, организации федеральной почтовой связи, которым поручено проведение идентификации, несут ответственность за несоблюдение установленных требований по идентификации в соответствии с Федеральным законом от 07.08.2001 N 115-ФЗ. Банковские платежные агенты несут ответственность за несоблюдение установленных требований по идентификации в соответствии с договором, заключенным с кредитной организацией;

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.

В соответствии со ст. 48 Закона РФ от 27.12.1991 N 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 N 1055. В данном случае в отношении иностранного журналиста предоставляются следующие персональные данные: биография, справка о журналистской деятельности корреспондента, две фотографии.

Примером применения указанной нормы на практике может служить решение Верховного суда Республики Коми от 28.11.2007 N 3-41-2007, оставленное в силе определением СК по гражданским делам Верховного Суда РФ от 27.02.2008 N 3-Г08-3, в котором отмечено, 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 комментируемого закона необходимый для реализации требований ст. 48 Закона РФ от 27.12.1991 N 2124-1 минимум персональных данных журналиста может передаваться в орган, осуществляющий его аккредитацию, и без согласия этого журналиста;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей продвижения товаров и услуг на рынке, а также целей политической агитации, при условии обязательного обезличивания персональных данных.

Обезличивание персональных данных представляет собой действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (п. 9 ст. 3 комментируемого закона). В данном случае при обезличивании персональных данных допустима их обработка в статистических и иных исследовательских целях без согласия субъектов. Например, ст. 97 Федерального закона от 21.11.2011 N 323-ФЗ предусматривает ведение статистического наблюдения в сфере здравоохранения. Официальная статистическая информация в сфере здравоохранения является общедоступной и размещается уполномоченным федеральным органом исполнительной власти в средствах массовой информации, в том числе в сети Интернет. Персональные данные, используемые для ведения медицинской статистики, не позволяют определить субъекта персональных данных (обезличены), в связи с чем письменное согласие субъекта на использование персональных данных для медицинской статистики не требуется;

10) обработка персональных данных, сделанных общедоступными субъектом персональных данных.

Под общедоступными источниками персональных данных следует понимать такие источники, доступ к которым предоставлен неограниченному кругу лиц (см. подробнее об этом комментарий к ст. 8). Здесь следует отметить, что для того чтобы персональные данные субъекта приобрели категорию общедоступных, необходимо письменное согласие субъекта указанных персональных данных. Однако на обработку общедоступных персональных

данных дополнительного согласия субъекта не требуется, поскольку, выразив однажды свою волю на предоставление доступа неограниченному кругу лиц к своим персональным данным, предполагается, что субъект одновременно предоставляет согласие каждому из неограниченного круга лиц обрабатывать указанные данные в любых не противоречащих закону целях.

Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта либо по решению суда или иных уполномоченных государственных органов;

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

Так, например, согласно ч. 1 ст. 8 Федерального закона от 25.12.2008 N 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, Пенсионном фонде Российской Федерации, Фонде социального страхования Российской Федерации, Федеральном фонде обязательного медицинского страхования, иных организациях, создаваемых Российской Федерацией на основании федеральных законов, размещаются в информационно-телекоммуникационной сети Интернет на официальных сайтах федеральных государственных органов, государственных органов субъектов Российской Федерации, органов местного самоуправления, государственных корпораций, Пенсионного фонда Российской Федерации, Фонда социального страхования Российской Федерации, Федерального фонда обязательного медицинского страхования, иных организаций, создаваемых Российской Федерацией на основании федеральных законов, и предоставляются для опубликования средствам массовой информации. Порядок предоставления указанных сведений для опубликования в средствах массовой информации и размещения в сети Интернет установлен Указом Президента РФ от 18.05.2009 N 561 "Об утверждении порядка размещения сведений о доходах, об имуществе и обязательствах имущественного характера лиц, замещающих государственные должности Российской Федерации, федеральных государственных служащих и членов их семей на официальных сайтах федеральных государственных органов и государственных органов субъектов Российской Федерации и предоставления этих сведений общероссийским средствам массовой информации для опубликования". В частности, предоставляются следующие сведения:

а) перечень объектов недвижимого имущества, принадлежащих лицу, замещающему государственную должность Российской Федерации (федеральному государственному служащему), его супруге (супругу) и несовершеннолетним детям на праве собственности или находящихся в их пользовании, с указанием вида, площади и страны расположения каждого из них;

б) перечень транспортных средств, с указанием вида и марки, принадлежащих на праве собственности лицу, замещающему государственную должность Российской Федерации (федеральному государственному

служащему), его супруге (супругу) и несовершеннолетним детям;

в) декларированный годовой доход лица, замещающего государственную должность Российской Федерации (федерального государственного служащего), его супруги (супруга) и несовершеннолетних детей.

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. Особенности обработки специальных категорий персональных данных регулируются ст.ст. 10, 11 комментируемого закона (см. подробнее комментарии к ним). Следует отметить, что обработка специальных категорий персональных данных субъекта осуществляется исключительно с его согласия, выраженного в письменной форме, за исключением случаев, установленных комментируемым законом.

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:

1) наличие согласия субъекта персональных данных на поручение обработки другому лицу;

2) наличие договора, в т.ч. 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.

Существенными условиями договора будут являться, а в акте государственного или муниципального органа соответственно должны быть закреплены:

перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;

цели обработки;

обязанность лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;

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 не допустима.

Так, Кировский областной суд, признавая законность привлечения управляющей компании к административной ответственности, предусмотренной ст. 13.11 КоАП РФ, отметил, что в нарушение ч. 3 ст. 6 комментируемого закона 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 получено согласия субъектов персональных данных на такую обработку. Агентский договор не содержит существенного условия, предусмотренного ч. 3 ст. 6 комментируемого закона, а именно отсутствуют требования к защите обрабатываемых персональных данных в соответствии со ст. 19 комментируемого закона (см. подробнее постановление Кировского областного суда от 24.04.2012 N 7-А-98/2012).

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.

Статья 7. Конфиденциальность персональных данных

Комментируемая статья устанавливает общее правило о конфиденциальности персональных данных.

Понятие конфиденциальности информации установлено п. 2 ст. 7 Федерального закона от 27.07.2006 N 149-ФЗ. Конфиденциальность информации - это обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Комментируемый закон не содержит определение конфиденциальности персональных данных, однако, по смыслу комментируемой статьи, с учетом положения п. 2 ст. 7 Федерального закона от 27.07.2006 N 149-ФЗ можно сделать вывод о том, что конфиденциальность персональных данных представляет собой обязательное для выполнения операторами и иными лицами, получившими доступ к персональным данным, требование не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Режим конфиденциальности распространяется на все персональные данные, исключения из этого режима установлены федеральным законом. Так, режим конфиденциальности не распространяется на общедоступные источники персональных данных (ст. 8 комментируемого закона) и обезличенные персональные данные (п. 9 ст. 3 комментируемого закона). Под общедоступными источниками персональных данных следует понимать такие источники, доступ к которым предоставлен неограниченному кругу лиц. Следует отметить, что информация, содержащаяся в общедоступных источниках персональных данных, во-первых, доступна любому лицу; во-вторых, может использоваться этим лицом по его усмотрению.

Обезличивание персональных данных представляет собой действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. Обезличивание персональных данных осуществляется, например, в статистических и иных исследовательских целях. Использование обезличенных персональных данных осуществляется без

согласия субъекта обезличенных персональных данных.

Таким образом, в отношении персональных данных действует режим конфиденциальности, который представляет собой совокупность норм права, регулирующих такой порядок обработки персональных данных, который препятствует доступу к указанной информации третьим лицам без согласия субъекта персональных данных. Нормы, обеспечивающие режим конфиденциальности персональных данных, содержатся в комментируемом законе, а также иных федеральных законах, регулирующих особенности обработки персональных данных в зависимости от специфики регулируемых указанными законами правоотношений.

Так, в соответствии со ст. 53 Федерального закона от 07.07.2003 N 126-ФЗ сведения об абонентах и оказываемых им услугах связи, ставшие известными операторам связи в силу исполнения договора об оказании услуг связи, являются конфиденциальной информацией и подлежат защите в соответствии с законодательством Российской Федерации. К таким сведениям относятся:

фамилия, имя, отчество или псевдоним абонента-гражданина;

наименование (фирменное наименование) абонента - юридического лица, фамилия, имя, отчество руководителя и работников этого юридического лица;

адрес абонента или адрес установки оконечного оборудования;

абонентские номера и другие данные, позволяющие идентифицировать абонента или его оконечное оборудование;

сведения баз данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента.

Предоставление третьим лицам сведений об абонентах-гражданах может осуществляться только с согласия в письменной форме абонентов, за исключением случаев, предусмотренных федеральными законами.

Согласно ст. 63 Федерального закона от 07.07.2003 N 126-ФЗ на территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи. Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами. Осмотр почтовых отправлений лицами, не являющимися уполномоченными работниками оператора связи, вскрытие почтовых отправлений, осмотр вложений, ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи и сетям почтовой связи, осуществляются только на основании решения суда, за исключением случаев, установленных федеральными законами.

Сведения о передаваемых по сетям электросвязи и сетям почтовой связи сообщениях, о почтовых отправлениях и почтовых переводах денежных средств, а также сами эти сообщения, почтовые отправления и переводимые денежные средства могут выдаваться только отправителям и получателям или их уполномоченным представителям, если иное не предусмотрено федеральными законами.

На основании ст. 64 Федерального закона от 07.07.2003 N 126-ФЗ

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.

Применение режима конфиденциальности в отношении персональных данных абонентов операторов связи на практике может вызывать вопросы, которые находят разрешение в судебных актах, например, это касается вопроса распространения такого режима на судебных приставов-исполнителей.

Пример: в постановлении Федерального арбитражного суда Северо-Кавказского округа от 29.07.2011 N Ф08-3920/11 по делу N А53-4656/2010 отмечено, что в силу ст. 64 Федерального закона от 07.07.2003 N 126-ФЗ операторы связи обязаны предоставлять информацию об абонентах только уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации. Органы, осуществляющие оперативно-розыскную деятельность, определены в ст. 13 Федерального закона от 12.08.1995 N 144-ФЗ. Поскольку судебный пристав-исполнитель в этот перечень не входит, на него также распространяется режим конфиденциальности персональных данных абонентов. Аналогичный вывод содержится в постановлении Федерального арбитражного суда Северо-Кавказского округа от 18.01.2012 N Ф08-7758/11 по делу N А53-4649/2010, в котором указано, что законы о судебных приставах и об исполнительном производстве не предоставляют судебным приставам-исполнителям права получать персональные данные, в том числе сведения о номере телефона абонента без его согласия, а также не предусматривают полномочия судебного пристава-исполнителя по обработке персональных данных.

Федеральный закон от 21.11.2011 N 323-ФЗ относит сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, к врачебной тайне (ст. 13). Режим врачебной тайны не допускает распространение сведений, составляющих врачебную тайну, даже после смерти человека. С письменного согласия гражданина или его законного представителя допускается разглашение сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается только в случаях, установленных в ч. 4 ст. 13 Федерального закона от 21.11.2011 N 323-ФЗ, а именно:

1) в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю, если

медицинское вмешательство необходимо по экстренным показаниям для устранения угрозы жизни человека и если его состояние не позволяет выразить свою волю или отсутствуют законные представители;

2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

3) по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

4) в случае оказания медицинской помощи несовершеннолетнему, больному наркоманией при оказании ему наркологической помощи или при медицинском освидетельствовании несовершеннолетнего в целях установления состояния наркотического либо иного токсического опьянения, а также несовершеннолетнему, не достигшему возраста пятнадцати лет, для больных наркоманией - шестнадцати лет, для информирования одного из его родителей или иного законного представителя;

5) в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

7) в целях расследования несчастного случая на производстве и профессионального заболевания;

8) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

9) в целях осуществления учета и контроля в системе обязательного социального страхования.

Пример: в постановлении Пятнадцатого арбитражного апелляционного суда от 21.02.2011 N 15АП-167/2011 отмечено, что состояние здоровья в соответствии с п. 1 ст. 10 Федерального закона от 21.11.2011 N 323-ФЗ относится к категории персональных данных, требующих особой защиты. В силу указанной нормы обработка таких данных не допускается, за исключением случаев, установленных ч. 2 ст. 10 комментируемого закона, в том числе, если субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных. Письменное согласие на обработку персональных данных должно предусматривать возможность обработки специальной категории персональных данных, в том числе данных о состоянии здоровья. В противном случае обработка персональных данных о состоянии здоровья будет являться нарушением комментируемого закона.

Обработка персональных данных гражданских служащих осуществляется с учетом положений Федерального закона от 27.07.2004 N 79-ФЗ "О государственной гражданской службе Российской Федерации". Указом Президента РФ от 30.05.2005 N 609 утверждено Положение о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела.

При обработке, хранении и передаче персональных данных гражданского служащего кадровая служба государственного органа обязана соблюдать следующие требования:

1) обработка персональных данных гражданского служащего осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, других законов и иных нормативных правовых актов, содействия гражданскому служащему в прохождении гражданской службы, обучении и должностном росте, обеспечения личной безопасности гражданского служащего и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества, учета результатов исполнения им должностных обязанностей и обеспечения сохранности имущества государственного органа;

2) персональные данные следует получать лично у гражданского служащего. В случае возникновения необходимости получения персональных данных гражданского служащего у третьей стороны следует известить об этом гражданского служащего заранее, получить его письменное согласие и сообщить гражданскому служащему о целях, предполагаемых источниках и способах получения персональных данных;

3) запрещается получать, обрабатывать и приобщать к личному делу гражданского служащего не установленные Федеральным законом от 27.07.2004 N 79-ФЗ и другими федеральными законами персональные данные о его политических, религиозных и иных убеждениях и частной жизни, о членстве в общественных объединениях, в том числе в профессиональных союзах;

4) при принятии решений, затрагивающих интересы гражданского служащего, запрещается основываться на персональных данных гражданского служащего, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;

5) защита персональных данных гражданского служащего от неправомерного их использования или утраты обеспечивается за счет средств государственного органа в порядке, установленном Федеральным законом от 27.07.2004 N 79-ФЗ и комментируемым законом;

6) передача персональных данных гражданского служащего третьей стороне не допускается без письменного согласия гражданского служащего, за исключением случаев, установленных федеральным законом. Условия передачи персональных данных гражданского служащего третьей стороне устанавливаются нормативными правовыми актами Российской Федерации.

Пример: в определении СК по гражданским делам Московского городского суда от 16.03.2011 N 33-4339 отмечена законность отказа управления федеральной налоговой службы в предоставлении гражданину паспортных

данных должностных лиц управления, поскольку согласно п. 6 ч. 1 ст. 42 Федерального закона от 27.07.2004 N 79-ФЗ при обработке, хранении и передаче персональных данных гражданского служащего кадровая служба государственного органа обязана соблюдать требования о том, что передача персональных данных гражданского служащего третьей стороне не допускается без письменного согласия гражданского служащего, за исключением случаев, установленных федеральным законом.

В отношении персональных данных гражданских служащих действует особый режим конфиденциальности, а именно: гражданский служащий, замещающий должность гражданской службы, включенную в перечень, установленный нормативными правовыми актами Российской Федерации, ежегодно, не позднее 30 апреля года, следующего за отчетным, представляет представителю нанимателя сведения о своих доходах, имуществе и обязательствах имущественного характера, а также о доходах, об имуществе и обязательствах имущественного характера членов своей семьи. Кроме того, в соответствии с ч. 5 ст. 20 Федерального закона от 27.07.2004 N 79-ФЗ сведения о доходах, имуществе и обязательствах имущественного характера федеральных гражданских служащих, назначение на должность и освобождение от должности которых осуществляются Президентом Российской Федерации или Правительством Российской Федерации, предоставляются для опубликования общероссийским средствам массовой информации по их обращениям с одновременным информированием об этом указанных гражданских служащих, а сведения о доходах, имуществе и обязательствах имущественного характера соответствующих гражданских служащих субъекта Российской Федерации предоставляются для опубликования общероссийским и региональным средствам массовой информации по их обращениям с одновременным информированием об этом указанных гражданских служащих.

Статьей 8 Федерального закона от 31.05.2002 N 63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации" установлен режим адвокатской тайны. Адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю. К сведениям, составляющим адвокатскую тайну, относятся любые сведения о лице, обратившемся к адвокату, в т.ч. сведения о личной жизни доверителя, о мотивах его действий (в т.ч. религиозные, политические и др.), полученные адвокатом в процессе оказания юридической помощи указанному лицу.

Так, в п. 4 определения Конституционного Суда РФ от 06.07.2000 N 128-О "По жалобе гражданина Паршуткина Виктора Васильевича на нарушение его конституционных прав и свобод пунктом 1 части второй статьи 72 УПК РСФСР и статьями 15 и 16 Положения об адвокатуре РСФСР" отмечено, что юридическая помощь адвоката (защитника) в уголовном судопроизводстве не ограничивается процессуальными и временными рамками его участия в деле при производстве расследования и судебного разбирательства, она включает и возможные предварительные юридические консультации, что вытекает, в частности, из ст. 19 Положения об адвокатуре РСФСР (действовавшего на момент рассмотрения жалобы), согласно которой адвокаты, осуществляя свою

профессиональную деятельность, дают консультации и разъяснения по юридическим вопросам, устные и письменные справки по законодательству, составляют заявления, жалобы и другие документы правового характера, осуществляют представительство, оказывают иную юридическую помощь.

Следует отметить, что законом не установлены исключения из режима конфиденциальности адвокатской тайны, т.е. отсутствуют нормы права, обязывающие адвоката сообщить сведения, составляющие адвокатскую тайну без согласия лица, сообщившего адвокату указанные сведения (подзащитного, доверителя, клиента). Адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием.

Статья 8. Общедоступные источники персональных данных

1. Комментируемая статья устанавливает исключение из общего правила о конфиденциальности персональных данных, а именно: в целях информационного обеспечения могут создаваться общедоступные источники персональных данных. В контексте комментируемого закона не совсем понятно, что законодатель подразумевает под информационным обеспечением. Анализ действующего законодательства (глава 8 Федерального конституционного закона от 28.06.2004 N 5-ФКЗ "О референдуме Российской Федерации", глава 7 Градостроительного кодекса Российской Федерации от 29.12.2004 N 190-ФЗ, раздел IV Федерального закона от 22.04.1996 N 39-ФЗ "О рынке ценных бумаг", глава 6 Федерального закона от 23.11.2009 N 261-ФЗ "Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации" и другие) позволяет сделать вывод о том, что под информационным обеспечением понимается предоставление информации, необходимой для осуществления какой-либо деятельности, проведения каких-либо мероприятий различного характера (экономического, правового, по безопасности и др.), оценки состояния различных систем, предупреждения нежелательных (опасных) ситуаций и др. Основными признаками информационного обеспечения являются:

полнота;

достоверность;

адресность;

своевременность.

В контексте нормы комментируемой статьи информационное обеспечение выступает в качестве цели создания общедоступных источников персональных данных. Таким образом, полагаем, что в рамках комментируемой статьи информационное обеспечение не является квалифицированным (т.е. имеющим специализированный, узко направленный характер), а носит общий характер, т.е. информационное обеспечение заключается в предоставлении максимально возможного объема информации на минимально информатизированный запрос (например, поиск в различных справочниках только по фамилии разыскиваемого лица), тогда как квалифицированное (специализированное) информационное обеспечение предполагает в запросе максимально возможный объем конкретизирующей информации.

Понятие общедоступности информации содержится в Федеральном законе от 27.07.2006 N 149-ФЗ. Согласно ст. 7 указанного закона к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Таким образом, под общедоступными источниками персональных данных следует понимать такие источники, доступ к которым предоставлен неограниченному кругу лиц. Следует отметить, что информация, содержащаяся в общедоступных источниках персональных данных, во-первых, доступна любому лицу; во-вторых, может использоваться этим лицом по его усмотрению. В связи с этим комментируемой статьей установлено наличие обязательного письменного согласия физического лица на включение его персональных данных в общедоступные источники. Согласно п. 4 ст. 9 комментируемого закона письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

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

3) цель обработки персональных данных;

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

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

6) срок, в течение которого действует согласие, а также порядок его отзыва.

Указанное согласие должно содержать собственноручную подпись субъекта персональных данных, либо, если согласие на обработку персональных данных выражено в форме электронного документа, то электронную подпись субъекта персональных данных в порядке, установленном Федеральным законом от 06.04.2011 N 63-ФЗ "Об электронной подписи". Таким образом, любое использование и обработка персональных данных физического лица, в том числе размещение персональных данных в общедоступных источниках, без его согласия является прямым нарушением закона и влечет за собой ответственность в соответствии со ст. 24 комментируемого закона. Неправомерность размещения персональных данных в различных общедоступных источниках без согласия субъекта персональных данных подтверждается также выводами судебной практики.

Пример: в постановлении Семнадцатого арбитражного апелляционного суда от 26.01.2011 N 17АП-13190/2010 отмечено, в частности, что сведения об абоненте, ставшие известными оператору связи в силу исполнения договора об

оказании услуг подвижной связи, могут использоваться оператором связи для оказания справочных и иных информационных услуг или передаваться третьим лицам только с письменного согласия этого абонента, за исключением случаев, предусмотренных федеральными законами. Согласие абонента-гражданина на обработку его персональных данных в целях осуществления оператором связи расчетов за оказанные услуги связи, а также рассмотрения претензий не требуется.

Письменное согласие может носить как адресный характер (то есть размещение персональных данных физического лица только в определенном общедоступном источнике), так и универсальный характер (использование персональных данных субъекта для размещения во всех общедоступных источниках, создаваемых данным оператором). Следует отметить, что письменное согласие на размещение персональных данных в определенном общедоступном источнике персональных данных не дает основания оператору размещать полученные в результате такого согласия персональные данные физического лица в других общедоступных источниках персональных данных.

Итак, в общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться следующие сведения:

фамилия, имя, отчество субъекта персональных данных;

год и место рождения;

адрес места жительства;

абонентский номер;

сведения о профессии;

иные персональные данные, сообщаемые субъектом персональных данных, а именно: сведения об образовании, наименование высшего учебного заведения и период обучения в нем (справочники выпускников ВУЗов).

Содержание и объем сведений о физическом лице, запрашиваемых для размещения в общедоступных источниках персональных данных, определяется исходя из целевого информативного характера конкретного общедоступного источника размещения персональных данных (например, для телефонного справочника это, как правило, фамилия, имя, отчество, адрес и абонентский номер телефона; для справочника руководителей определенного субъекта РФ - фамилия, имя, отчество, год и место рождения, данные о профессии и месте работы, также могут включаться сведения о ВУЗе и периоде обучения в нем, и т.д.).

К общедоступным источникам персональных данных можно отнести следующие:

различные справочники на любых носителях информации: бумажных, электронных, - в том числе размещаемые в информационно-телекоммуникационной сети Интернет (справочники телефонные, адресные, выпускников ВУЗов, руководителей и пр.);

различные информационные базы данных государственных, муниципальных органов, управлений, учреждений;

сборники, энциклопедии и пр.

2. Часть вторая комментируемой статьи устанавливает, что сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта либо по решению суда или иных уполномоченных государственных органов.

Физическое лицо, обнаружившее использование своих персональных данных в любом общедоступном источнике, в т.ч. в сети Интернет, вправе обратиться к владельцу этого источника с заявлением об исключении своих персональных данных из общедоступного источника. Комментируемая статья не устанавливает требования к форме такого заявления, но разумно предположить, что в интересах самого субъекта подать данное заявление владельцу общедоступного источника персональных данных в письменном виде. В заявлении должно быть указаны следующие сведения:

1) фамилия, имя, отчество заявителя;

2) адрес заявителя;

3) наименование общедоступного источника персональных данных, его выходные данные (например, если источник размещен на бумажном носителе, - год, издательство; если расположен в сети Интернет, - адрес сайта);

4) требование об исключении персональных данных заявителя из указанного источника.

По смыслу комментируемой статьи требование субъекта об исключении его персональных данных из общедоступного источника является безусловным, т.е. не требующим указания основания для исключения (например, отсутствие письменного согласия, получение угроз, ненужных писем и пр.). При этом ранее выданное письменное согласие на использование персональных данных физического лица теряет силу с момента получения владельцем или оператором общедоступного источника персональных данных требования об исключении персональных данных субъекта. В случае отказа владельца общедоступного источника персональных данных или оператора исключить персональные данные заявителя из указанного источника последний вправе обратиться в суд с исковым заявлением о понуждении владельца (оператора) общедоступного источника персональных данных исключить из указанного источника персональные данные истца. Указанная категория споров рассматривается судами общей юрисдикции (глава 3 ГПК РФ).

Субъект персональных данных может также защитить свои права, установленные комментируемых законом, обратившись с соответствующим заявлением в прокуратуру (Федеральный закон от 17.01.1992 N 2202-I "О прокуратуре Российской Федерации"). В случае если прокурором будет установлено нарушение комментируемого закона или нарушение прав заявителя, прокурором или его заместителем будет внесено соответствующее представление об устранении нарушений в орган или должностному лицу, которые полномочны устранить допущенные нарушения. В течение месяца со дня внесения представления должны быть приняты конкретные меры по устранению допущенных нарушений, их причин и условий, им способствующих; о результатах принятых мер должно быть сообщено прокурору в письменной форме.

И наконец, за защитой своих прав, установленных комментируемым

законом, и с требованием об исключении своих персональных данных из общедоступного источника субъект может обратиться в уполномоченный орган - Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), а именно в одно из ее управлений - Управление по защите прав субъектов персональных данных.

На основании постановления суда, вступившего в законную силу в установленном законом порядке, либо на основании актов иных уполномоченных органов (прокуратуры, Роскомнадзора) владелец общедоступного источника персональных данных обязан исключить персональные данные заявителя из указанного источника.

Статья 9. Согласие субъекта персональных данных на обработку его персональных данных

1. Статья 9 комментируемого закона содержит комплексную норму о волеизъявлении субъекта персональных данных по вопросу о его согласии на обработку персональных данных. Норма изложена в четырех логических компонентах и восьми частях:

1) первый - о праве субъекта дать и отозвать согласие на обработку персональных данных - соответствует ч. 1 и 2 комментируемой статьи;

второй - об условиях и порядке дачи такого согласия в специальных случаях обработки персональных данных - соответствует ч. 4 и 5 комментируемой статьи;

третий - о возможных заменах волеизъявления субъекта персональных данных уполномоченными лицами - соответствует ч. 6 и 7 комментируемой статьи;

четвертый - об обязанностях оператора персональных данных - соответствует ч. 3 и 8 комментируемой статьи соответственно.

В целом вопрос о волеизъявлении лица определенным образом соотносится с вопросом о правоспособности и дееспособности лица. Это соотношение определяется наличием автономии воли и возможностью ее реализации. Если лицо самостоятельно в принятии решения, способно к волеизъявлению, не имеет ограничений в принятии решения и закон признает это волеизъявление, то волеизъявление по общему правилу рассматривается как автономное. Наиболее полно вопросы о правоспособности и дееспособности разработаны в рамках гражданского законодательства для применения в хозяйственных, экономических отношениях. В иных сферах основные положения о правоспособности и дееспособности лиц применяются по подобию. Комментируемая статья представляет одно из первых решений вопроса правоспособности и дееспособности лиц в информационной сфере в рамках информационного законодательства. Существенное влияние на российское законодательство оказывает европейское законодательство о персональных данных и сложившаяся практика (например, обмен сведениями в процессе обращения в уполномоченные визовые центры за получением визы).

2. Часть 1 комментируемой статьи содержит общую норму о согласии на обработку персональных данных. Согласие субъекта является комплексной категорией, при оценке которой необходимо учитывать: наличие свободы

принятия субъектом решения; наличие собственной воли субъекта, т.е. отсутствие какого-либо давления на него со стороны; наличие интереса субъекта в связи передачей для возможной обработки собственных персональных данных. Комментируя данную норму, российские авторы, как правило, акцентируют внимание на гражданско-правовом принципе автономии воли. Последний подразумевает свободное и самостоятельное принятие решения, основанного исключительно на внутреннем убеждении субъекта, определяющего характер и содержание собственных действий. Одним из основных международных документов в данной области, который позволяет сравнить подходы при определении наличия/ отсутствия согласия, является Директива 95/46/ЕС Европейского парламента и Совета ЕС от 24.10.1995 о защите физических лиц в отношении обработки персональных данных и свободного обращения таких данных. Анализ положений, закрепленных в Директиве 95/46/ЕС, позволяет выявить несколько критериев для оценки свободы принятия решения субъектом. В соответствии со ст. 2 Директивы 95/46/ЕС "согласие субъекта данных означает любое свободно данное конкретное и сознательное указание на его желания, которым субъект данных выражает свое согласие на обработку относящихся к нему персональных данных". В соответствии со ст. 7 Директивы 95/46/ЕС согласие квалифицируется как "однозначно данное" согласие. В соответствии со ст. 8 Директивы 95/46/ЕС имеет место определение согласия как "явно выраженное согласие" на обработку. В соответствии со ст. 26 Директивы 95/46/ЕС передача персональных данных в третью страну может совершаться при условии, что субъект данных "однозначно дал свое согласие" на предполагаемую передачу данных.

Современные представления о защите персональных данных в Европе необходимо соотносить с последними из принятых документов. Одним из таких является Резолюция Европейского парламента от 06.07.2011 о комплексном подходе к защите персональных данных в Европейском союзе (2011/2025 (INI)). В ней отражаются основные тенденции, которые могут повлиять на отношения по поводу персональных данных в России. Документом провозглашается преемственность основных принципов Директивы 95/46/ЕС. Наличие разных подходов в государствах-членах ЕС не снимает обязанности ЕС обеспечить неприкосновенность частной жизни в отношении любой обработки персональных данных физических лиц в пределах и за пределами ЕС при любых обстоятельствах в современных условиях, вызванных глобализацией, в целях решения многочисленных задач. Особенно подчеркивается необходимость защиты данных в связи с расширением деятельности в Интернете.

В документе подчеркнуто, что право на свободу выражения мнения и информации и принцип прозрачности должны быть полностью учтены при обеспечении фундаментального права на защиту персональных данных. Далее отмечается необходимость комплексного подхода по защите персональных данных во всех областях, в которых обрабатываются персональные данные, в том числе в области полицейского и судебного сотрудничества по уголовным делам, области общей внешней политики и политики безопасности без ущерба для конкретных правил. Европейский парламент призывает Европейскую комиссию убедиться в том, что текущий пересмотр законодательства ЕС о

защите данных будет предусматривать: полное согласование на самом высоком уровне предоставления правовой определенности и единого высокого стандарта уровня защиты людей в любых обстоятельствах; оценку воздействия и тщательный учет затрат; укрепление существующих принципов и элементов, таких как прозрачность данных, минимизация и цели ограничения, наличие предварительного и явного согласия, данные о нарушениях прав и уведомление субъектов, особенно в отношении глобальной онлайновой среды; подчеркивается, что согласие должно считаться действительным только тогда, когда имеется однозначное сообщение, свободное, конкретное и четкое; когда имеется адекватный реализованный механизм для фиксации согласия или отзыва согласия пользователя*(22).

В условиях глобализации оператор обязан учитывать существующие мировые и европейские тенденции, при этом получение согласия не должно становиться тормозом на пути развития отношений. В существующей реальности представляется обоснованным рекомендовать придерживаться изложенной российской правовой трехкомпонентной концепции согласия субъекта, не ограничиваясь гражданско-правовым толкованием. Соответственно, оператор должен учесть наличие свободы принятия субъектом решения; наличие собственной воли субъекта, т.е. отсутствие какого-либо давления на него со стороны; наличие интереса субъекта в связи передачей для возможной обработки его собственных персональных данных. Представляется, что на современном этапе развития информационных отношений этого будет достаточно для соблюдения требований комментируемого закона.

3. Часть 2 комментируемой статьи предусматривает возможность отзыва согласия на обработку персональных данных. Поскольку согласие может быть дано лично и через представителя, возможно предположить, что отзыв может быть представлен в аналогичном формате. Одновременно возникает вопрос о том, может ли быть отзыв представлен через представителя, если согласие было представлено лично, и наоборот. Оператору персональных данных предстоит решать (устанавливать в локальных нормативных актах), каков должен быть порядок дачи согласия и отзыва согласия на обработку персональных данных субъектом.

В соответствии с ч. 2 и 8 комментируемой статьи обработка 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;

в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию;

в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в

целях устройства детей, для предоставления государственной или муниципальной услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

в связи реализацией обязательств по обязательным видам страхования;

в соответствии со страховым законодательством при обработке данных детей, оставшихся без попечения родителей;

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

при обработке персональных данных в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

при обработке персональных данных 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;

если обработка персональных данных осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных;

если обрабатываются персональные данные, доступ к которым предоставлен субъектом персональных данных для неограниченного круга лиц;

если осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

если обработка персональных данных необходима для заключения (исполнения) договора, участником которого является субъект персональных данных;

если 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;

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

если обработка персональных данных осуществляется в соответствии с Федеральным законом от 25.01.2002 N 8-ФЗ;

если это персональные данные участников общественного объединения и обработка данных осуществляется в соответствии с учредительными документами в пределах организации.

4. Часть 4 комментируемой статьи содержит требование об обработке персональных данных исключительно с письменного согласия самого субъекта. К

названным случаям относятся все виды обработки персональных данных за исключением случаев, описанных в п. 3 комментария к настоящей статье (см. выше). В ч. 4 комментируемой статьи предусмотрен формат письменного согласия с указанием всех необходимых условий и сопутствующих обстоятельств. Частью 5 комментируемой статьи предусмотрен вариант предоставления согласия субъектом персональных данных на обработку его персональных в форме электронного документа. Данная ситуация предусмотрена Федеральным законом от 27.07.2010 N 210-ФЗ. В соответствии со ст. 21.2 Федерального закона от 27.07.2010 N 210-ФЗ Правительство Российской Федерации утверждает Правила использования простых электронных подписей при оказании государственных и муниципальных услуг. В соответствии с постановлением Правительства РФ от 25.01.2013 N 33 "Об использовании простой электронной подписи при оказании государственных и муниципальных услуг" субъект персональных данных (именуемый в тексте постановления - заявитель) должен указать фамилию, имя и отчество (если имеется), страховой номер индивидуального лицевого счета, а также дать согласие заявителя на обработку его персональных данных. Оператор, выдавая ключ, обязан установить личность заявителя. Таким образом, согласие в форме электронного документа предусматривает наличие простой электронной подписи и минимального количества персональных данных, необходимых для идентификации субъекта.

5. Часть 6 комментируемой статьи содержит норму о представителе субъекта персональных данных.

Представительство по вопросу оборота персональных данных несовершеннолетнего лица будут осуществлять его (субъекта) родители или лица их замещающие. Для лиц, ограничено дееспособных по медицинским показаниям, представителями могут выступать также должностные лица медицинского учреждения. В иных случаях представитель субъекта персональных данных будет осуществлять свою деятельность по доверенности.

Требования к форме и содержанию доверенности наиболее полно разработаны в сфере гражданских правоотношений. Тем не менее, начинают появляться отдельные рекомендации и комментарии на сайте Роскомнадзора, как уполномоченного субъекта по контролю за оборотом в сфере персональных данных. Доверенность, выданная представителю, должна содержать:

конкретное указание о том, кому она предоставлена в каких целях и на какой срок;

указание оператора, для каких целей дается согласие на обработку персональных данных;

указание на то, что данное действие не противоречит интересам субъекта персональных данных;

указание на то, что согласие на обработку персональных данных дается по воле субъекта персональных данных;

а также, что представляется важным, причину, по которой выдана доверенность, т.е. почему субъект персональных данных дает согласие на обработку персональных данных через представителя, а не лично.

Вопрос о том, каким образом оператором проверяются полномочия

представителя субъекта персональных данных, решаются оператором в каждом конкретном случае самостоятельно. Оператор для данного случая должен иметь соответствующие положения, закрепленные в документе, который входит в систему документов, именуемую в целом "политика обработки персональных данных". Вероятно, что для данного случая оператором будет разработана специальная инструкция либо специальный раздел в инструкции, регулирующий отношения в сфере оборота персональных данных. Оператор, как правило, являются юридическим лицом, что предполагает наличие физического лица, действующего от имени оператора. По сути, в данной ситуации мы наблюдаем ситуацию взаимодействия представителей: представителя субъекта персональных данных с одной стороны и оператора - с другой. Во всех случаях оператор либо его представитель обязаны проверить два момента: факт передачи права на обработку персональных данных субъектом персональных данных и наличие (соблюдение) формы доверенности о передаче субъектом персональных данных права на обработку персональных данных.

6. В ч. 7 комментируемой статьи содержится норма, устанавливающая порядок получения согласия на обработку персональных данных в случае смерти субъекта персональных данных. Действующим законодательством отношения по поводу вступления в наследство и исполнения последней воли субъекта регулируются в рамках ГК РФ. Субъектом, который будет решать вопрос о даче согласия на оборот персональных данных, вероятно, будет наследник по закону ли наследник по завещанию. В связи с развитием отношений по поводу оборота персональных данных прогнозируется, в специальных случаях, появление специального душеприказчика по вопросу информационного наследия, в том числе по вопросам оборота персональных данных.

7. Часть 8 комментируемой статьи содержит норму, которая связана с ч. 3 комментируемой статьи и содержит требование об обязанности оператора иметь согласие субъекта на обработку его персональных данных. Сама формулировка данной части не должна дезориентировать оператора. Возможность получения оператором персональных данных от лица, не являющегося их субъектом, не означает, что оператор освобождается от доказывания, что персональные данные получены законно. Отдельные исключения, предусмотренные ч. 2 комментируемой статьи и описанные в п. 3 настоящего комментария (см. выше), представляют ограниченное множество случаев. Во всех остальных случаях, которых, представляется, подавляющее большинство, оператор должен иметь согласие субъекта на обработку его персональных данных и при необходимости доказать, что персональные данные получены законным путем.

Европейская практика, влияние которой на российские отношения и законодательство по вопросу персональных данных трудно отрицать, свидетельствует о следующих тенденциях. Проект поправок в европейское законодательство о защите персональных данных предусматривает практически полное отделение отношений по поводу персональных данных от смежных гражданских и иных правоотношений. Директива 95/46/ЕС Европейского парламента и Совета ЕС от 24.10.1995 о защите физических лиц при обработке персональных данных и о свободном обращении таких данных обязывает операторов обеспечить надлежащий уровень защиты персональных данных.

Регламент Европейского парламента и Совета ЕС 45/2001 от 18.12.2000 о защите физических лиц при обработке персональных данных, осуществляемой учреждениями и органами Сообщества, и о свободном обращении таких данных - еще один документ, который направлен на обеспечение защиты персональных данных в учреждениях и органах Европейского союза. Документ включает положения о создании независимого надзорного органа для контроля. Исполнение перечисленных документов, а именно сочетание двух перечисленных факторов: независимый контроль и надлежащая защита - порой приводят к весьма значимым результатам.

Пример: в Объединенном Королевстве Великобритании и Северной Ирландии (UK) защитой личных данных занимается независимая Информационная комиссия (ICO). По данным от 15 февраля 2013 г. Управления Информационной комиссии Совет по сестринскому делу и акушерству был оштрафован на 150 000 английских фунтов. Из официального сообщения следует, что многие организации до настоящего времени не пересмотрели свою политику по защите персональных данных и их обработке. В результате нарушения этого типа встречаются снова и снова. В рассмотренном случае Совет потерял три DVD-диска, в которых содержались конфиденциальная личная информация и данные о детях. В ходе расследования Информационная комиссия обнаружила, что информация не была зашифрована, утрата связана с проступком медсестры. Было отмечено, что если бы был сделан простой шаг по шифрованию информации, ее утрата была бы менее опасной, а санкция не была бы столь значительной*(23).

Таким образом, операторам персональных данных требуется достаточно внимательно подходить к вопросу защиты персональных данных, начиная с подбора ответственного персонала и выполнения положений действующего законодательства. Вероятно, российский законодатель последует в направлении, которое будет учитывать европейскую практику, тем более что многие положения комментируемого закона заимствованы из европейского законодательство о защите персональных данных.

Статья 10. Специальные категории персональных данных

1. Часть первая комментируемой статьи устанавливает общее правило по обработке специальных категорий персональных данных. Так, согласно общему правилу, установленному комментируемой статьей, не допускается обработка следующих категорий персональных данных:

расовая принадлежность;
национальная принадлежность;
политические взгляды;
религиозные убеждения;
философские убеждения;
состояние здоровья;
интимная жизнь.

Статья 19 Конституции РФ провозглашает, что государство гарантирует

равенство прав и свобод человека и гражданина независимо от пола, расы, национальности, 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 (ч. 2 ст. 19 Конституции РФ). Таким образом, государство гарантирует не только формально-юридическое равенство прав и свобод человека и гражданина путем провозглашения последнего, но и обеспечивает претворение данной нормы в жизнь, в том числе устраняя любые возможные предпосылки для возникновения неравенства в зависимости от пола, расы, национальности, языка, происхождения, имущественного и должностного положения, места жительства, отношения к религии, убеждений, принадлежности к общественным объединениям, а также других обстоятельств. "Обезличенность" физического лица, лишение его индивидуальных характеристик (расовая, национальная принадлежность, состояние здоровья и пр.) в процессе обработки персональных данных направлены на получение максимально объективного результата обработки персональных данных, исключение малейшего влияния человеческого фактора в процессе обработки персональных данных, способного повлиять на результат обработки.

Расовая принадлежность указывает на принадлежность человека к одному из видов рас, выделенных антропологией в качестве основных, либо к промежуточным расам. Как отметил антрополог В.П. Алексеев, типологическая концепция расы "все больше приобретает характер анахронизма и отходит в историю антропологической науки"*(24). Действительно, значение расовой принадлежности человека в конце XX - начале XXI века нивелировано, поскольку подавляющее большинство государств не поддерживает политику расовой сегрегации населения. В современной России расовая принадлежность человека, вследствие подавляющего большинства среди населения представителей европеоидной расы, не играла такого существенного значения, как, например, в США или ЮАР. В частности, при проведении переписи населения в США респондент указывает свою расовую принадлежность, тогда как в Российской Федерации при проведении Всероссийской переписи населения в 2002 и 2010 годах в переписных листах имелся лишь вопрос о национальной принадлежности, вопрос о расовой принадлежности респондента отсутствовал.

Национальная принадлежность в Российской Федерации имеет несоизмеримо большее значение, поскольку Российская Федерация является многонациональным государством, что нашло отражение в преамбуле Основного закона - Конституции РФ: "Мы, многонациональный народ Российской Федерации, соединенные общей судьбой на своей земле...". Согласно ч. 1 ст. 26 Конституции РФ каждый вправе определять и указывать свою национальную принадлежность. Никто не может быть принужден к определению и указанию своей национальной принадлежности. Таким образом, в Конституции закреплен принцип свободы волеизъявления при определении национальной принадлежности: с одной стороны, человек вправе указывать свою национальность либо не указывать ее вообще (указание национальности), с

другой стороны, человек вправе указать любую национальность, к которой, по его мнению, он себя относит (определение национальности). В советский период документирование национальности полагалось принципиально значимым и обязательным. В паспорте гражданина СССР существовала графа "Национальность". Современные стандарты прав и свобод человека исключают возможность такого публичного отнесения не только гражданина, но и любого человека к какой-либо национальности. Согласно Положению о паспорте гражданина РФ, утвержденному постановлением Правительства РФ от 08.07.1997 N 828, не только не предусматривается фиксация в паспорте сведений о национальной принадлежности гражданина, но и запрещается вносить в паспорт не предусмотренные прямо сведения, отметки и записи (п. 6 Положения).

Политические взгляды человека представляют собой систему убеждений и взглядов на политику, экономику, устройство государства и общества, право, правосудие и прочие категории государственности и права в целом. Статья 29 Конституции РФ гарантирует каждому свободу мысли и слова при запрете на пропаганду или агитацию, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Свобода политических убеждений, взглядов означает и свободу участия в любых политических партиях, общественных объединениях, движениях. В Российской Федерации не допускается выдача другим государствам лиц, преследуемых за политические убеждения.

Религиозные убеждения отражают отношение человека к религии, а также обуславливают его специфическое (культовое) поведение. Статья 28 Конституции РФ провозглашает, что каждому в Российской Федерации гарантируются свобода совести, свобода вероисповедания, включая право исповедовать индивидуально или совместно с другими любую религию или не исповедовать никакой, свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними. Право человека и гражданина на свободу совести и свободу вероисповедания может быть ограничено федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов человека и гражданина, обеспечения обороны страны и безопасности государства. Правоотношения в области прав человека и гражданина на свободу совести и свободу вероисповедания, а также правовое положение религиозных объединений регулируются также Федеральным законом от 26.09.1997 N 125-ФЗ "О свободе совести и о религиозных объединениях". Пункт 5 ст. 3 указанного закона устанавливает, что никто не обязан сообщать о своем отношении к религии и не может подвергаться принуждению при определении своего отношения к религии, к исповеданию или отказу от исповедания религии, к участию или неучастию в богослужениях, других религиозных обрядах и церемониях, в деятельности религиозных объединений, в обучении религии.

Философские убеждения представляют собой совокупность взглядов человека на мир, его создание, цели его существования, место человека в мире, смысл человеческой жизни и пр. Философские убеждения, как правило, тесно

связаны с религиозными убеждениями человека и также оказывают существенное влияние на его мышление и поведение в целом. Свобода философских убеждений также является производной свободы мысли и слова, гарантированной ст. 29 Конституции РФ.

В соответствии с п. 1 ст. 2 Федерального закона от 21.11.2011 N 323-ФЗ под здоровьем понимается состояние физического, психического и социального благополучия человека, при котором отсутствуют заболевания, а также расстройства функций органов и систем организма. Отношения, возникающие в сфере охраны здоровья граждан в Российской Федерации, регулируются Федеральным законом от 21.11.2011 N 323-ФЗ. Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну и не допускаются к разглашению, за исключением случаев, установленных законом (ст. 13 Федерального закона от 21.11.2011 N 323-ФЗ). Гражданин самостоятельно принимает решение о разглашении сведений о состоянии своего здоровья за исключением случаев, установленных ст. 13 Федерального закона от 21.11.2011 N 323-ФЗ, например, при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений. Запрещено ставить возможность осуществления гражданских прав и свобод человека и гражданина в зависимость от состояния здоровья человека за исключением случая признания гражданина недееспособным (ст. 29 ГК РФ) или ограниченно дееспособным (ст. 30 ГК РФ).

Право на свободу интимной жизни гарантировано ст. 23 Конституции РФ, которая устанавливает право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый также имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

2. Часть 2 комментируемой статьи устанавливает исключения из общего правила, указанного в ч. 1 комментируемой статьи. Так, обработка специальных категорий персональных данных допускается в следующих случаях (и только в них):

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

Статья 9 комментируемого закона устанавливает требования к содержанию письменного согласия на обработку персональных данных (см. подробнее об этом комментарий к ст. 9). В любом случае, согласие на обработку персональных данных должно быть конкретным, информированным и осознанным и должно содержать весь перечень сведений, указанных в ч. 4 ст. 9 комментируемого закона, т.е. из согласия должно следовать, от кого и когда оно исходило и на обработку каких данных оно давалось.

Следует отметить, что специальные категории персональных данных, на обработку которых требуется письменное согласие субъекта, могут быть указаны в самом согласии.

Для обработки персональных данных, которые содержатся в самом согласии (фамилия, имя, отчество, дата рождения, место жительства и проч.),

данном субъектом в письменной форме, дополнительного согласия не требуется;

2) персональные данные сделаны общедоступными субъектом персональных данных.

Порядок и форма предоставления персональных данных субъектом в общедоступные источники персональных данных регулируется ст. 8 комментируемого закона (см. подробнее об этом комментарий к ней). Включение любых персональных данных субъекта, в том числе специальных категорий персональных данных, в общедоступные источники персональных данных возможно только с письменного согласия субъекта персональных данных. В любое время по требованию субъекта сведения о его персональных данных должны быть исключены из общедоступного источника персональных данных;

3) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии.

На данный период Правительством Российской Федерации заключено двенадцать соглашений о реадмиссии с иностранными государствами, одно из которых, заключенное с Правительством Республики Казахстан, в настоящее время в силу не вступило.

Реадмиссия представляет собой 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 заключенным между государствами соглашением.

Соглашения о реадмиссии содержат перечень документов и сведений, необходимых для реадмиссии. В частности, Приложение N 3 к Соглашению между Правительством Российской Федерации и Правительством Королевства Норвегия о реадмиссии (Москва, 08.06.2007) содержит список документов, предоставление которых рассматривается как косвенное наличие гражданства. Такими документами могут быть:

водительские удостоверения или их фотокопии;

любой другой официальный документ, выданный властями запрашиваемого государства;

служебные удостоверения или их фотокопии;

письменные заявления, сделанные соответствующим лицом, и язык, на котором он/она говорит, включая результаты официального тестирования.

Все указанные документы содержат персональные данные субъекта, подлежащего реадмиссии, и на основании Соглашения, заключенного между Российской Федерацией и Королевством Норвегия, могут быть использованы для установления действия указанного Соглашения в отношении конкретного лица. Следовательно, одному государству персональные данные лица необходимы для того, что бы установить подлежит ли данное лицо депортации с территории данного государства, а другому государству - чтобы принять указанное лицо на своей территории.

В данном случае обработка специальных категорий персональных данных субъекта осуществляется без его письменного согласия;

4) обработка персональных данных осуществляется в соответствии с

Федеральным законом от 25.01.2002 N 8-ФЗ.

В соответствии со ст. 1 Федерального закона от 25.01.2002 N 8-ФЗ 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 соответствии с официальной статистической методологией в целях формирования официальной статистической информации о демографических, об экономических и о социальных процессах. Сведения, полученные в ходе Всероссийской переписи населения, не могут быть использованы в целях причинения имущественного и морального вреда человеку и гражданину, затруднения реализации его прав и свобод.

Согласно ст. 6 Федерального закона от 25.01.2002 N 8-ФЗ при проведении Всероссийской переписи населения у лиц, проживающих на территории России, могут запрашиваться следующие персональные данные:

пол;

возраст (дата рождения);

гражданство (состояние в гражданстве, наличие двойного гражданства, наименование государства или государств, гражданином которых является опрашиваемое лицо);

национальная принадлежность;

владение языками (родной язык, русский язык, другой язык или другие языки);

образование (дошкольное, начальное общее, основное общее, среднее (полное) общее, начальное профессиональное, среднее профессиональное, высшее профессиональное, послевузовское профессиональное);

состояние в браке;

количество детей;

отношения с членами домохозяйства;

место рождения (наименование государства, субъекта Российской Федерации);

место жительства и (или) место пребывания (наименование государства, субъекта Российской Федерации, муниципального образования, городского, сельского поселения);

жилищные условия (тип жилого помещения, время постройки дома, размер общей и жилой площади, количество жилых комнат, виды благоустройства жилого помещения);

источники средств к существованию (доход от трудовой деятельности или иного занятия, пенсия, в том числе пенсия по инвалидности, стипендия, пособие, другой вид государственного обеспечения, иной источник средств к существованию);

занятость либо безработица (наличие работы или иного занятия, являющихся источниками средств к существованию, либо их отсутствие);

миграция (продолжительность проживания или пребывания, прежнее место жительства или пребывания, продолжительность пребывания на территории иностранного государства, причина въезда в Российскую Федерацию, передвижение от места жительства или пребывания до места

работы).

Сбор иных сведений, как и принуждение опрашиваемых лиц предоставить о себе указанные сведения, в соответствии с Федеральным законом от 25.01.2002 N 8-ФЗ не допускаются.

Согласно ст. 8 Федерального закона от 25.01.2002 N 8-ФЗ сведения о населении, содержащиеся в переписных листах, являются информацией ограниченного доступа, не подлежат разглашению или распространению и используются только в целях формирования официальной статистической информации. Обработка сведений о населении, содержащихся в переписных листах, осуществляется в условиях, обеспечивающих их защиту от несанкционированного доступа и предотвращение их хищения, утраты, подделки или иного искажения.

Обработка персональных данных, полученных при переписи населения, осуществляется только при наличии письменного согласия субъекта;

5) обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях.

В данном случае предоставление и обработка специальных категорий персональных данных осуществляется в интересах самого субъекта персональных данных, поскольку предоставление государством социальной помощи зависит, в частности, от предоставления лицом сведений о состоянии его здоровья. Так, в соответствии с Федеральным законом от 17.07.1999 N 178-ФЗ "О государственной социальной помощи" право на получение государственной социальной помощи в виде набора социальных услуг имеют, в частности, инвалиды и дети-инвалиды (персональные данные о состоянии здоровья), члены семей погибших (умерших) инвалидов войны, участников Великой Отечественной войны и ветеранов боевых действий, члены семей погибших в Великой Отечественной войне лиц из числа личного состава групп самозащиты объектовых и аварийных команд местной противовоздушной обороны, а также члены семей погибших работников госпиталей и больниц города Ленинграда (персональные данные о составе семьи, о смерти членов семьи). То же можно сказать и в отношении предоставления персональных данных относительно трудового стажа, места работы, размера заработной платы с целью получения трудовой пенсии (Федеральный закон от 15.12.2001 N 166-ФЗ "О государственном пенсионном обеспечении в Российской Федерации").

Обработка данной категории персональных данных осуществляется при наличии письменного согласия субъекта;

6) 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.

Например, согласно Федеральному закону от 21.11.2011 N 323-ФЗ состояние здоровья гражданина составляет врачебную тайну (ст. 13). Однако предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается, в частности:

в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю;

при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

в случае оказания медицинской помощи несовершеннолетним для информирования одного из его родителей или иного законного представителя;

в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

в целях расследования несчастного случая на производстве и профессионального заболевания.

В указанных случаях обработка специальной категории персональных данных гражданина, в частности о состоянии его здоровья, необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц, при этом получение согласия субъекта персональных данных невозможно в силу физического состояния гражданина, либо в силу его несовершеннолетия;

7) 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.

Обработка персональных в целях, указанных в данном пункте, также осуществляется в соответствии с Федеральным законом от 21.11.2011 N 323-ФЗ. Особенность обработки персональных данных в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг заключается в том, что обработка персональных данных в этом случае осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

В соответствии с п. 10 ст. 2 Федерального закона от 21.11.2011 N 323-ФЗ под медицинской деятельностью понимается профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях.

По смыслу данного закона к перечню лиц, профессионально занимающихся медицинской деятельностью, относятся:

медицинская организация;

медицинские работники;

лечащие врачи;

8) 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.

Операторами обработки персональных данных членов (участников) общественного объединения или религиозной организации являются общественные объединения и религиозные организации, членами (участниками) которых являются субъекты персональных данных.

В соответствии со ст. 6 Федерального закона от 26.09.1997 N 125-ФЗ религиозным объединением в Российской Федерации признается добровольное объединение граждан Российской Федерации, иных лиц, постоянно и на законных основаниях проживающих на территории Российской Федерации, образованное в целях совместного исповедания и распространения веры и обладающее соответствующими этой цели признаками:

вероисповедание;

совершение богослужений, других религиозных обрядов и церемоний.

обучение религии и религиозное воспитание своих последователей.

Религиозные объединения могут создаваться в форме религиозных групп (ст. 7 Федерального закона от 26.09.1997 N 125-ФЗ) и религиозных организаций (ст. 8 Федерального закона от 26.09.1997 N 125-ФЗ).

Деятельность общественных объединений регулируется Федеральным законом от 19.05.1995 N 82-ФЗ "Об общественных объединениях".

Согласно ст. 7 Федерального закона от 19.05.1995 N 82-ФЗ общественные объединения могут создаваться в одной из следующих организационно-правовых форм:

общественная организация;

общественное движение;

общественный фонд;

общественное учреждение;

орган общественной самодеятельности;

политическая партия.

Обработка персональных данных членов (участников) общественного объединения или религиозной организации соответствующими операторами осуществляется только при наличии следующих условий одновременно:

для достижения законных целей, предусмотренных учредительными документами религиозных и общественных объединений;

при наличии письменного согласия субъектов персональных данных;

9) обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия.

В данном случае обработка персональных данных субъекта необходима для установления правоспособности лица, в том числе дееспособности, объема гражданских прав, которыми наделен субъект. Обработка персональных данных субъекта производится при осуществлении правосудия. В частности, ст. 278 УПК

РФ устанавливает, что в ходе судебного следствия при допросе свидетеля перед допросом председательствующий устанавливает личность свидетеля, выясняет его отношение к подсудимому и потерпевшему, разъясняет ему права, обязанности и ответственность, предусмотренные ст. 56 УПК РФ, о чем свидетель дает подписку, которая приобщается к протоколу судебного заседания. Таким образом, суд вправе при допросе свидетеля в целях выяснения его отношения к подсудимому или потерпевшему установить, в частности, такие специальные категории персональных данных, как родственное или иное отношение к подсудимому или потерпевшему, например, состояние в браке с подсудимым или потерпевшим ранее или в настоящее время.

Письменного согласия субъекта персональных данных при данном виде обработке персональных данных не требуется;

10) 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-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации.

В данном случае обработка специальных категорий персональных данных осуществляется в целях государственной и общественной безопасности и осуществляется без согласия субъекта персональных данных;

11) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

Согласно ст. 7 Федерального закона от 29.11.2010 N 326-ФЗ и приказом Министерства здравоохранения и социального развития РФ от 25.01.2011 N 29н "Об утверждении Порядка ведения персонифицированного учета в сфере обязательного медицинского страхования" Федеральный фонд обязательного медицинского образования вправе обрабатывать данные персонифицированного учета о медицинской помощи, оказанной застрахованным лицам, а именно проводить сбор, обработку, передачу и хранение следующих сведений:

номер полиса обязательного медицинского страхования застрахованного лица;

медицинская организация, оказавшая соответствующие услуги;

виды оказанной медицинской помощи;

условия оказания медицинской помощи;

сроки оказания медицинской помощи;

объемы оказанной медицинской помощи;

стоимость оказанной медицинской помощи;

диагноз;

профиль оказания медицинской помощи;

медицинские услуги, оказанные застрахованному лицу, и примененные лекарственные препараты;

примененные медико-экономические стандарты;

специальность медицинского работника, оказавшего медицинскую помощь;

результат обращения за медицинской помощью;

результаты проведенного контроля объемов, сроков, качества и условий предоставления медицинской помощи;

12) 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.

Органы опеки и попечительства обязаны при определении возможности передачи ребенка на воспитание в семью проводить обработку персональных данных потенциальных усыновителей, опекунов/ попечителей, родителей приемных семей.

В частности, в отношении лиц, желающих усыновить ребенка, устанавливаются следующие специальные категории персональных данных:

семейное положение;

место жительства;

наличие судимости;

состояние здоровья;

сведения о лишении родительских прав, об отмене усыновления, об отстранении от обязанностей опекуна или попечителя;

сведения о дееспособности усыновителя и его супруга (ст. 127 СК РФ).

Кроме того, ст. 123 СК РФ содержит положение о том, что при устройстве ребенка на воспитание в семьи граждан должны учитываться его этническое происхождение, принадлежность к определенной религии и культуре, родной язык, возможность обеспечения преемственности в воспитании и образовании.

3. Часть третья комментируемой статьи устанавливает круг операторов обработки специальной категории персональных данных - сведений о судимости. Так, обработка персональных данных о судимости может осуществляться:

1) государственными или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством РФ.

Понятие судимости установлено ст. 86 УК РФ. Так, лицо, осужденное за совершение преступления, считается судимым со дня вступления обвинительного приговора суда в законную силу до момента погашения или снятия судимости. Порядок погашения и снятия судимости регулируется УК РФ и УПК РФ. Погашение или снятие судимости аннулирует все правовые последствия, связанные с судимостью.

Обработка сведений о судимости государственными или муниципальными органами осуществляется только в том случае, если права или обязанность по обработки данной категории персональных данных возложена законом.

Так, в соответствии с п. 39 ч. 1 ст. 12 Федерального закона от 07.02.2011 N 3-ФЗ "О полиции" полиция обязана предоставлять 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 предоставление таких сведений или документа, содержащего такие сведения, в указанные государственные органы или органы местного самоуправления. Таким образом, полиция осуществляет обработку сведений о судимости. Кроме того,

полиция при осуществлении своей деятельности вправе использовать банки данных других государственных органов и организаций, в том числе персональные данные граждан, если законом не установлено иное (п. 33 ч. 1 ст. 13 Федерального закона от 07.02.2011 N 3-ФЗ).

Согласно ст. 16 Федерального закона от 27.07.2004 N 79-ФЗ одним из ограничений, связанных с гражданской службой, является наличие не снятой или не погашенной в установленном федеральным законом порядке судимости. Таким образом, любой государственный орган, профессиональная служебная деятельность в котором является государственной гражданской службой, вправе обрабатывать сведения о судимости кандидатов на должности гражданской службы и гражданских служащих, а также должностных лиц;

2) иными лицами в случаях и в порядке, установленном федеральными законами.

Так, в ст. 23 Федерального закона от 29.07.1998 N 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 собирать и обрабатывать сведения о судимости своих членов - оценщиков.

4. Часть четвертая комментируемой статьи устанавливает основание для прекращения причин обработки специальных категорий персональных данных, осуществляемой в случаях, рассмотренных в п. 2 комментария к настоящей статье. Обработка специальных категорий персональных данных должна быть прекращена, если устранены причины, вследствие которых осуществлялась обработка. Например, обработка специальных категорий персональных данных должна быть прекращена в следующих случаях:

если субъект персональных данных отозвал письменное согласие, данное им ранее, на обработку своих персональных данных;

по окончании Всероссийской переписи населения и подведения ее итогов;

если отпала угроза инфекционных заболеваний, массовых отравлений и поражений;

при прекращении членства субъекта персональных данных в религиозном организации или общественном объединении;

в случае увольнения гражданина с государственной гражданской службы и пр.

Статья 11. Биометрические персональные данные

1. Частью 1 комментируемой статьи закрепляется норма об обязательном наличии согласия субъекта персональных данных при обработке оператором биометрических персональных данных. Более того, согласие субъекта персональных данных должно быть предоставлено в письменной форме. Данная конструкция статьи концентрирует наше внимание, в первую очередь, на понятии "биометрические персональные данные". В самой статье содержится краткое

определение биометрических персональных данных - это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность. Таким образом, в статье имеется указание на две основные группы биометрических персональных данных: физиологические и биологические особенности человека. Следует дополнительно учитывать, что биологические особенности человека введены в качестве отдельного вида биометрических персональных данных сравнительно недавно, в 2011 году, Федеральным законом от 25.07.2011 N 261-ФЗ "О внесении изменений в Федеральный закон "О персональных данных", который вступил в силу 01 июля 2011 г. Динамика изменения понятия биометрических персональных данных обусловлена высокими темпами развития всего комплекса наук, и в первую очередь наук на стыке информатики, биологии, физиологии и смежных научных направлений.

Что касается непосредственно физиологических персональных данных, то специалисты для дальнейшего использования в целях идентификации личности различают статические и динамические биометрические характеристики человека. К статическим относят характеристики, данные человеку от рождения и неизменяемые с течением времени: отпечатки пальцев, геометрия лица, геометрия руки, рисунок сетчатки глаза. К динамическим биометрическим характеристикам относят поведенческие характеристики, основанные на динамике подсознательных движений: рукописный почерк, клавиатурный почерк, голосовые особенности*(25). Как динамические, так и статические физиологические биометрические персональные данные обладают целым рядом позитивных признаков, которые позволяют их накапливать, классифицировать для дальнейшего использования. Основным потребительским признаком является высокая степень устойчивости характеристик, неизменяемость на протяжении всей жизни субъекта. Другая характеристика, уникальность, т.е. возможность выделить свойственные только отдельному субъекту признаки, что позволяет идентифицировать личность и формировать базы данных сведений о личности. Биометрические данные, являясь объектом защиты, с одной стороны, в силу их устойчивости, с другой стороны, становятся основой для формирования средств защиты информации, что повышает значимость защиты персональных данных*(26). В последние несколько лет применение биометрических персональных нашло место в сфере криптографической защиты данных. Так, например, исследователь О.В. Куликова полагает, что биометрические криптографические системы имеют преимущества по сравнению с обычными ключами, которые имеют ряд недостатков: могут быть легко потеряны, украдены, забыты и т.д. Как отмечает автор, "биометрические методы аутентификации личности имеют ряд преимуществ по сравнению с традиционными, а именно: 1) биометрические признаки очень трудно фальсифицировать; 2) в силу уникальности биометрических признаков достоверность аутентификации очень высока; 3) биометрический идентификатор нельзя забыть, как пароль, или потерять, как пластиковую карточку; 4) для биометрической аутентификации требуется присутствие владельца биометрических признаков"*(27). Таким образом, с одной стороны, биометрические персональные данные выступают как объект защиты, с другой

стороны, - как средство защиты.

Еще одно направление, связанное с оборотом биометрических персональных данных, основано на теории распределенных процессов, т.е. на независимых процедурах сбора и обработки биометрических персональных данных. Данное направление получило развитие в исследованиях российских ученых, предлагают перспективное направление, связанное с мультибиометрической идентификацией, т.е. применение логических классификаторов для идентификации по нескольким биометрическим характеристикам. В основу такого процесса положен принцип независимости процесса биометрической идентификации от используемых биометрических характеристик и выбранного биометрического метода. Синтез осуществляется на основе методов интеграции отдельных биометрических идентификаторов, которые используют множество разных источников информации. На современном этапе исследователи В.М. Белов, Е.М. Сесин предлагают выделять следующие "уровни интеграции: различные биометрические характеристики (изображение лица и отпечаток пальца); множественные биометрические характеристики (отпечатки различных пальцев, радужная оболочка левого и правого глаза); различные способы получения биометрических образцов (изображение лица в видимом и инфракрасном диапазоне); различные сканеры (две фотокамеры); несколько образцов одной биометрической характеристики; несколько алгоритмов сравнения биометрических образцов"*(28).

Практически все российские исследования построены на использовании физиологических биометрических персональных данных. Биологические биометрические персональные данные в российской практике - новая категория. Зарубежные исследователи и практические специалисты используют более широкое понятие биометрических персональных данных. В Индии биометрия является наукой установления личности индивида, основанной на физических, химических или поведенческих признаках человека*(29). Ряд американских исследователей сосредоточены на совместимости биометрических систем и комплексном подходе к биометрическим стандартам. Одно из направлений их работы связано с введением в тестирование двоичных данных*(30). Еще одно направление исследований ведется канадскими учеными, которые предлагают весьма обширную методику формирования биометрических персональных данных и вместе с тем открывают новые направления биометрии, которые могут иметь правовые последствия. В их числе: биометрия, не оставляющая след, - новый класс технологий повышения конфиденциальности, таких как биометрическое шифрование; анонимная биометрия - система, где биометрические данные не подключены к персональным данным; биометрические данные могут быть включены в другую систему для объединения с личной информацией; отзывная (приватная) биометрия - позволяет иметь несколько биометрических идентичностей; каждая идентичность может быть использована самостоятельно или анонимно*(31). Перечисленные направления биометрии, представляется, имеют в своем составе различные дополнительные направления. Полный перечень всех направлений и технологий может и должен быть описан специальными стандартами. Правоведы должны иметь общее представление о широком круге

технологий и не ограничиваться классическими технологиями (описанием внешних признаков и примет, снятием отпечатков папиллярных узоров и т.д.). В то же время отдельные передовые технологии, в том числе технологии хранения и поиска по базам данных персональных данных, должны стать предметом специальных учебных курсов. Вместе с тем практически все исследователи отмечают, что нет ни одной биометрической системы, которая может эффективно удовлетворять всем требованиям. Биометрия по общему признанию не является идеальной, но некоторые системы являются допустимыми.

Другой аспект использования биометрических персональных данных - это согласие субъекта персональных данных, которое должно быть в письменной форме. Данный аспект не зависит от технологий. Вне зависимости от способа получения согласия (письмом, электронным письмом) наличие согласия субъекта персональных данных является обязательным условием законной обработки оператором биометрических персональных данных.

2. Часть 2 комментируемой статьи содержит норму, которой предусмотрены исключения из общего правила обработки биометрических персональных данных, а именно сведения об обстоятельствах, при которых обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных:

1) не требуется согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии. Термин реадмиссия введен в российское законодательство Федеральным законом от 06.05.2008 N 60-ФЗ "О внесении изменений в Федеральный закон "О правовом положении иностранных граждан в Российской Федерации" и отдельные законодательные акты Российской Федерации". В действующем Федеральном законе от 25.07.2002 N 115-ФЗ данной административной процедуре посвящена глава VI Передача и прием иностранных граждан в соответствии с международными договорами российской федерации о реадмиссии (ст. 32.2, 32.3). Статьи главы содержат нормы, которыми установлены порядок передачи и приема иностранных граждан в соответствии с международными договорами Российской Федерации о реадмиссии и порядок осуществления личного досмотра иностранных граждан, подлежащих реадмиссии, и досмотра вещей, находящихся при указанных иностранных гражданах. Реадмиссия - "действие государства разрешающего повторный въезд лица (собственных граждан, иностранных граждан, лиц без гражданства), о котором стало известно, что оно (данное лицо) незаконно въехало, пребывает, проживает на территории другого государства"*(32), - понятие, раскрываемое в руководящей, справочной литературе, в некоторых деталях может отличаться от существующей международной практики. Соглашение о реадмиссии между Россией и Швейцарией содержит иную формулировку, а именно: "реадмиссия означает передачу компетентным органом запрашивающего государства и принятие компетентным органом запрашиваемого государства лиц (граждан запрашиваемого государства, граждан третьих государств или лиц без гражданства), чей въезд, пребывание или проживание в запрашивающем государстве признаны незаконными..."*(33).

В целом процедура носит административный характер, независимо от того

в рамках административного (миграционного) или судебного (уголовного) процесса она реализуется. Соответственно, согласие субъекта персональных данных, по мнению законодателя, запрашивать не требуется;

2) не требуется согласия субъекта персональных данных в связи с осуществлением правосудия и исполнением судебных актов.

Федеральным законом от 28.06.2010 N 123-ФЗ "О внесении изменений в статью 1 Федерального закона "О персональных данных" и статью 15 Федерального закона "Об обеспечении доступа к информации о деятельности судов в Российской Федерации" предусмотрена процедура обезличивания персональных данных в отдельных случаях. Так, при размещении в сети Интернет текстов судебных актов, вынесенных судами общей юрисдикции, за исключением текстов судебных актов, подлежащих в соответствии с законом опубликованию, в целях обеспечения безопасности участников судебного процесса из указанных актов исключаются персональные данные, кроме фамилий и инициалов истца, ответчика, третьего лица, гражданского истца, гражданского ответчика, осужденного, оправданного, лица, в отношении которого ведется производство по делу об административном правонарушении, секретаря судебного заседания, рассматривавших (рассматривавшего) дело судей (судьи), а также прокурора, адвоката и представителя, если они участвовали в судебном разбирательстве. Вместо исключенных персональных данных используются инициалы, псевдонимы или другие обозначения, не позволяющие идентифицировать участников судебного процесса.

Что касается исполнения судебных актов, то в соответствии со ст. 64 Федерального закона от 02.10.2007 N 229-ФЗ в процессе исполнительного производства, т.е. в процессе исполнения требований исполнительных документов, судебный пристав-исполнитель вправе запрашивать персональные данные у физических лиц, организаций и органов, находящихся на территории Российской Федерации, а также на территориях иностранных государств, в порядке, установленном международным договором Российской Федерации. Ограничительным условием использования полученных персональных данных является требование о том, что персональные данные обрабатываются им исключительно в целях исполнения исполнительных документов в необходимом для этого объеме с учетом требований, установленных комментируемым законом. Кроме того, в соответствии со ст. 12 Федерального закона от 21.07.1997 N 118-ФЗ "О судебных приставах" судебный пристав-исполнитель получает и обрабатывает персональные данные при условии, что они необходимы для своевременного, полного и правильного исполнения исполнительных документов, в необходимом объеме;

3) не требуется согласия субъекта персональных данных в случаях, предусмотренных законодательством Российской Федерации об обороне. В соответствии со ст. 8 Федерального закона от 28.03.1998 N 53-ФЗ "О воинской обязанности и военной службе" при осуществлении первичного воинского учета органы местного самоуправления поселений и органы местного самоуправления городских округов обязаны осуществлять сбор, хранение и обработку сведений, содержащихся в документах первичного воинского учета, в порядке, установленном законодательством Российской Федерации в области

персональных данных и Положением о воинском учете, утвержденным постановлением Правительства РФ от 27.11.2006 N 719. Пункт 19 Положения о воинском учете предусматривает содержание в документах следующих сведений о гражданах: фамилия, имя и отчество; дата рождения; место жительства; семейное положение; образование; место работы; годность к военной службе по состоянию здоровья; основные антропометрические данные и иное;

4) не требуется согласия субъекта персональных данных в случаях, предусмотренных законодательством Российской Федерации о безопасности. В соответствии со ст. 13 Федерального закона от 03.04.1995 N 40-ФЗ в перечень прав органов федеральной службы безопасности входят следующие права:

проверять у граждан и должностных лиц документы, удостоверяющие их личность, если имеются достаточные основания подозревать их в совершении преступления;

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 Российской Федерации к ведению органов федеральной службы безопасности.

Права, связанные с проверкой и задержанием, непосредственно связаны с установлением личности и получением персональных данных. Как административная процедура, регулируемая императивными (власти-подчинения) методами, она не предполагает получение согласия на обработку персональных данных. Что касается права получать биологический материал и осуществлять обработку геномной информации, то представляется очевидным, что данная процедура проводится преимущественно в связи отсутствием живых лиц и, соответственно, в связи с отсутствием возможности получить какое-либо согласие в принципе. Статья 8 Федерального закона от 28.12.2010 N 390-ФЗ "О безопасности" содержит полномочия Президента Российской Федерации в области обеспечения безопасности. В перечень полномочий входит:

определение основных направлений государственной политики в области обеспечения безопасности;

утверждение стратегии национальной безопасности Российской Федерации;

принятие в соответствии с законодательством Российской Федерации мер по защите граждан от преступных и иных противоправных действий. Полномочия перечисленных субъектов реализуются в рамках рассмотренного законодательства без согласия субъектов персональных данных;

5) не требуется согласия субъекта персональных данных в случаях, предусмотренных законодательством Российской Федерации о противодействии

терроризму. В соответствии со ст. 11 Федерального закона от 06.03.2006 N 35-ФЗ "О противодействии терроризму" правовой режим контртеррористической операции предполагает введение ряда ограничений, которые касаются, в том числе, персональных данных. Например, в целях пресечения и раскрытия террористического акта, минимизации его последствий и защиты жизненно важных интересов личности, общества и государства на территории, в пределах которой введен правовой режим контртеррористической операции, допускаются:

проверка у физических лиц документов, удостоверяющих их личность, а в случае отсутствия таких документов - доставление указанных лиц в органы внутренних дел Российской Федерации (иные компетентные органы) для установления личности;

проведение досмотра физических лиц и находящихся при них вещей (см. предыдущий подпункт комментария к настоящей статье);

6) не требуется согласия субъекта персональных данных в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности. Статья 11 Федерального закона от 09.02.2007 N 16-ФЗ "О транспортной безопасности" предусматривает сбор персональных данных в информационных системах, которые обеспечивают продажу проездных документов. При оформлении проездных документов (билетов) автоматизированные централизованные базы персональных данных о пассажирах накапливают следующие данные о пассажирах:

фамилия, имя, отчество;

дата и место рождения;

вид и номер документа, удостоверяющего личность, по которому приобретается проездной документ (билет);

пункт отправления, пункт назначения, вид маршрута следования (беспересадочный, транзитный);

дата поездки.

Такие базы формируются при осуществлении внутренних и международных воздушных перевозок; железнодорожных перевозок в дальнем следовании; международных перевозок морским, внутренним водным и автомобильным транспортом; перевозок железнодорожным, морским, внутренним водным и автомобильным транспортом по отдельным маршрутам. Одной из функций информационной системы является обеспечение безопасности перевозок, в том числе путем передачи данных, содержащихся в проездных документах (билетах), в автоматизированные централизованные базы персональных данных о пассажирах в соответствии с комментируемым законом. Контроль за соблюдением порядка передачи сведений, предусмотренных настоящей статьей, в автоматизированные централизованные базы персональных данных о пассажирах осуществляется федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере транспорта. Статья 85.1 главы XII "Авиационная безопасность" ВК РФ содержит норму о персональных данных пассажиров воздушных судов. Согласно названной норме перевозчики обеспечивают передачу персональных данных пассажиров воздушных судов в автоматизированные централизованные базы персональных данных о пассажирах в соответствии с комментируемым

законом и законодательством Российской Федерации о транспортной безопасности;

7) не требуется согласия субъекта персональных данных в случаях, предусмотренных законодательством Российской Федерации о противодействии коррупции. В соответствии со ст. 8.1 Федерального закона от 25.12.2008 N 273-ФЗ и ст. 2, 4, 8, 15 Федерального закона от 03.12.2012 N 230-ФЗ "О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам" государственные служащие и иные предусмотренные законом лица*(34) обязаны представить сведения о расходах, а также о расходах своих супруги (супруга) и несовершеннолетних детей. Сведения, опубликование которых предусмотрено нормами названных актов, размещаются в информационно-телекоммуникационной сети Интернет на официальных сайтах федеральных государственных органов, государственных органов субъектов Российской Федерации, органов местного самоуправления, Центрального банка Российской Федерации, государственных корпораций, Пенсионного фонда Российской Федерации, Фонда социального страхования Российской Федерации, Федерального фонда обязательного медицинского страхования, иных организаций, созданных Российской Федерацией на основании федеральных законов, и предоставляются для опубликования средствам массовой информации в порядке, определяемом нормативными правовыми актами Президента Российской Федерации, иными нормативными правовыми актами Российской Федерации и нормативными актами Центрального банка Российской Федерации, с соблюдением требований комментируемого закона;

8) не требуется согласия субъекта персональных данных в случаях, предусмотренных законодательством Российской Федерации об оперативно-розыскной деятельности. В соответствии со ст. 6 Федерального закона от 12.08.1995 N 144-ФЗ 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. Тем не менее закон не предусматривает процедуру получения согласия на обработку персональных данных. В то же время закон не вводит запрет на получение персональных данных в ходе оперативно-розыскных мероприятий. Норма, которая обеспечивает соблюдение прав субъекта персональных данных, предусмотрена ст. 5 Федерального закона от 12.08.1995 N 144-ФЗ. Согласно упомянутой норме полученные в результате проведения оперативно-розыскных мероприятий материалы в отношении лиц, виновность которых в совершении преступления не доказана в установленном законом порядке, хранятся один год, а затем уничтожаются, если служебные интересы или правосудие не требуют иного. За три месяца до дня уничтожения материалов, отражающих результаты оперативно-розыскных мероприятий, проведенных на основании судебного решения, об этом уведомляется соответствующий судья;

9) не требуется согласия субъекта персональных данных в случаях, предусмотренных законодательством Российской Федерации о государственной службе. В соответствии со ст. 14 Федерального закона от 27.05.2003 N 58-ФЗ "О

системе государственной службы Российской Федерации" персональные данные государственных служащих, сведения об их профессиональной служебной деятельности и о стаже (об общей продолжительности) государственной службы вносятся в личные дела и документы учета государственных служащих. Персональные данные, внесенные в личные дела и документы учета государственных служащих, являются персонифицированными и в случаях, установленных федеральными законами и иными нормативными правовыми актами Российской Федерации, относятся к сведениям, составляющим государственную тайну, а в иных случаях к сведениям конфиденциального характера. Обработка, хранение и передача персональных данных гражданского служащего и ведение его личного дела осуществляются в соответствии со ст. 42 Федерального закона от 27.07.2004 N 79-ФЗ. При этом кадровая служба государственного органа обязана получать персональные данные гражданского служащего лично у него самого. В случае возникновения необходимости получения персональных данных гражданского служащего у третьей стороны субъекта персональных данных следует известить об этом и получить его письменное согласие. Субъекту персональных данных сообщают о целях, предполагаемых источниках и способах получения персональных данных. В личное дело гражданского служащего вносятся его персональные данные и иные сведения, связанные с поступлением на гражданскую службу, ее прохождением и увольнением с гражданской службы и необходимые для обеспечения деятельности государственного органа. Положение о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела утверждено Указом Президента РФ от 30.05.2005 N 609. В соответствии с п. 16 Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела к личному делу гражданского служащего приобщается, в числе прочих документов, медицинское заключение установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на гражданскую службу или ее прохождению. Весь массив сведений о государственных служащих, сформированный на основе их персональных данных, сводится в реестры государственных служащих. Реестры государственных служащих ведутся, в том числе, на электронных носителях;

10) не требуется согласия субъекта персональных данных в случаях, предусмотренных уголовно-исполнительным законодательством Российской Федерации. 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 порядовка осуществления контроля за поведением условно осужденных. В соответствии с положениями поименованных статей уголовно-исполнительная инспекция по месту жительства осужденного к наказанию в виде ограничения свободы ставит его на персональный учет, а также осуществляет персональный учет условно осужденных. При постановке на учет осужденный подлежит дактилоскопической регистрации и фотографированию;

11) не требуется согласия субъекта персональных данных в случаях, предусмотренных законодательством Российской Федерации о порядке выезда

из Российской Федерации и въезда в Российскую Федерацию. Порядок выезда из Российской Федерации регулируется Федеральным законом от 15.08.1996 N 114-ФЗ "О порядке выезда из Российской Федерации и въезда в Российскую Федерацию". Согласно данному закону основными документами, удостоверяющими личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию, признаются: паспорт; дипломатический паспорт; служебный паспорт; паспорт моряка (удостоверение личности моряка). Основные документы, удостоверяющие личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию, могут содержать электронные носители информации с записанными на них персональными данными владельца паспорта, включая биометрические персональные данные. Более детально понятие паспорта, который содержит биометрические персональные данные, изложены в Указе Президента РФ от 29.12.2012 N 1709 "О паспорте гражданина Российской Федерации, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем на электронном носителе информации дополнительные биометрические персональные данные его владельца". В частности, данный правовой акт под таким документом понимает паспорт гражданина Российской Федерации, удостоверяющий личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащий на электронном носителе информации дополнительные биометрические персональные данные его владельца (изображение папиллярных узоров двух пальцев рук). Кроме того, в соответствии с названным Указом Правительству Российской Федерации предписано в 3-месячный срок разработать и внести в Государственную Думу Федерального Собрания Российской Федерации проект федерального закона о внесении в Федеральный закон от 15.08.1996 N 114-ФЗ изменений по вопросу закрепления полномочий по сканированию папиллярных узоров двух пальцев рук гражданина Российской Федерации за соответствующими федеральными органами исполнительной власти, а также обеспечить начиная с 01 июня 2013 г. года изготовление бланков паспорта гражданина Российской Федерации, удостоверяющего личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащего электронный носитель информации, предназначенный для записи дополнительных биометрических персональных данных гражданина Российской Федерации (изображения папиллярных узоров двух пальцев рук).

Порядок въезда в Российскую Федерацию, предусмотренный Федеральным законом от 18.07.2006 N 109-ФЗ "О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации" (ст. 9), включает следующее условие въездного контроля: при осуществлении миграционного учета осуществляются сбор, фиксация, хранение, обобщение и использование таких сведений об иностранном гражданине, как вид и реквизиты документа, удостоверяющего личность и признаваемого Российской Федерацией в этом качестве (наименование, серия, номер, дата и место выдачи, срок действия, а при наличии - биометрические данные, содержащиеся в указанном

документе). Учету подлежат также иные сведения (всего 17 видов).

Статья 12. Трансграничная передача персональных данных

1. Часть 1 комментируемой статьи содержит норму, которая определяет правила регулирования отношений по трансграничной передаче персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы. Законодатель не уточняет, каким именно документом в рамках законодательства Европейского союза следует руководствоваться, однако по смыслу нормы можно сделать заключение, что придерживаться следует действующей версии Директивы 95/46/ЕС Европейского парламента и Совета ЕС от 24.10.1995 о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, которая постоянно дорабатывается и совершенствуется. Наиболее полная современная редакция Директивы 95/46/ЕС изложена в Резолюции Европейского парламента от 06.07.2011 о комплексном подходе к защите персональных данных в Европейском союзе (2011/2025 (INI)). Документом провозглашается преемственность основных принципов Директивы 95/46/ЕС и осуществляется значительная доработка отдельных норм. Применительно к комментируемой статье это нормы о наличии предварительного и явного согласия на обработку персональных данных, особенно в отношении глобальной онлайновой среды*(35). Кроме того, следует учитывать отдельные положения норм, которые были исправлены ранее либо провозглашены специальными документами. К названным положениям относятся: обязанность операторов обеспечить адекватный уровень защиты данных*(36) и создание независимого надзорного органа для контроля*(37). Эти моменты, как правило, не учитываются отдельными авторами в процессе анализа европейского законодательства о трансграничной передаче данных. Основное их внимание сосредоточено на законодательстве 1995-2001 годов*(38). Тем не менее европейское законодательство находится в состоянии постоянной доработки и в ближайшее время российским законодателям и операторам придется учитывать также обновленные положения об особенностях обработки персональных данных в уголовном процессе*(39). Предложения о совершенствовании законодательства о персональных данных в Европе вносятся практически ежемесячно*(40). Относительно стабильную на период 2-3 года картину европейского законодательства, вероятно, следует ожидать к окончанию 2014 года.

Положения норм комментируемой статьи относятся к автоматизированной обработке персональных данных (см. комментарий к ст. 16). Соответственно, операторы, осуществляющие ручную обработку персональных данных, должны самостоятельно решать, как учитывать положения комментируемой статьи при трансграничной передаче данных. В связи с тем, что автоматизированная обработка при трансграничной передаче персональных данных преобладает, операторам рекомендуется учитывать положения комментируемой статьи и при ручной обработке и трансграничной передаче персональных данных.

Обратимся к самому понятию трансграничной передачи персональных данных. Трансграничная передача персональных данных - это передача персональных данных на территорию иностранного государства, органу власти

иностранного государства, иностранному физическому лицу или иностранному юридическому лицу (п. 11 ст. 3 комментируемого закона). Несмотря на то что понятие определено комментируемым законом, остается значительное число вопросов, ответ на которые не вместит ни один комментарий. Большинство этих вопросов связано с отдельными функциями программных продуктов (программ для компьютеров), которые не декларируются. Речь в данном случае идет о маркерах программ для поиска информации в информационных телекоммуникационных сетях (браузерах), для общения в социальных сетях и иных. Механизм действия и особенно правовые последствия достаточно подробно описаны в литературе*(41). Наша рекомендация оператору заключается в том, чтобы он четко представлял, какие функции реализует оборудование, на котором он производит обработку персональных данных. Вполне вероятна ситуация, при которой передача персональных данных может быть осуществлена и без его воли.

Понятие адекватной защиты прав субъектов персональных данных должно быть более четко определено законодательно либо на основе судебной и повседневной практики уполномоченного органа в сфере защиты персональных данных. С формально логической стороны адекватность может быть истолкована как совпадение, соответствие*(42). Применительно к комментируемой статье адекватная защита прав субъектов персональных данных - соответствующая, совпадающая защита персональных данных в России и в той стране, с которой производится сравнение. В этом смысле полной адекватности установить не удастся, поскольку законодательство и юридическая практика каждой страны по-своему уникальны. Минимальный уровень адекватности, как представляется, может быть обеспечен в сравниваемой стране путем принятием закона аналогичного тому, который является предметом настоящего комментария. Фактически имеет место обратная ситуация, поскольку Россия принимает законодательство о защите персональных данных, догоняя европейские страны. Таким образом, можно говорить о неполном соответствии европейскому современного российского законодательства о защите персональных данных либо о соответствии современного российского законодательства европейскому образца периода 1995-2001 годов. В этой связи адекватная защита прав субъектов персональных данных должна толковаться как защита в иностранной юрисдикции, соответствующая отечественной, но с большей степенью защиты и с дополнительными возможностями.

2. В ч. 2 комментируемой статьи содержится норма, которая детализирует функции государственного органа, который уполномочен осуществлять защиту прав субъектов персональных данных. Правительством Российской Федерации данная функция поручена Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзору)*(43). Министерством связи и массовых коммуникаций Российской Федерации, которому подведомствен Роскомнадзор, разработан документ, определяющий порядок осуществления указанных функций - Административный регламент 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 (приказ Минкомсвязи РФ от 14.11.2011 N 312). В соответствии с названным документом регламентируется практически вся деятельность Роскомнадзора, результаты которой доводятся до сведения заинтересованных лиц, в том числе, через официальной сайт *(44). Одним из документов, который ожидают увидеть на официальном сайте многочисленные операторы, является 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, о котором идет речь в комментируемой статье. На конец марта 2013 г. искомый перечень на сайте не был представлен. Документы на сайте Роскомнадзора*(45), которые могут быть использованы для оценки ситуации в Европейском Союзе, имеют возраст 10 и более лет. Соответственно, если следовать строго принципу сравнительного правоведения в части хронологической точности сравниваемых объектов (в данном случае это нормативные акты), то на сайте отсутствует информация, на основе которой возможно провести такое сравнение. С другой стороны, приведенные на сайте документы Европейского Союза (периода 2002 года) в максимальной степени соответствуют действующему российскому законодательству (2011-2013 годов). Европейские государства продвинулись дальше, и понятие "адекватная защита персональных данных" в России и Европе имеет временной люфт - 10 лет. Следует также учитывать, что практически все страны принимают собственные нормативные акты, которые могут в деталях отличаться от общеевропейского законодательства. В этом смысле очевидна нелегкая для Роскомнадзора задача формирования Перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Весьма вероятно, что данный перечень может быть сформирован Роскомнадзором совместно с полномочными структурами Министерства иностранных дел России, на основе двусторонних соглашений или консультаций по вопросам защиты персональных данных. В любом случае, операторам, которые ожидают появления данного Перечня, рекомендуется обращаться к законодательству и юридической практике соответствующего государства для уточнения всех деталей трансграничной передачи в каждом конкретном случае.

3. В ч. 3 комментируемой статьи закреплена норма об обязанностях оператора персональных данных убедиться в том, что страна, в которую будут направлены персональные данные, обеспечивает их адекватную защиту. Данное требование комментируемого закона может поставить многих операторов в затруднительное положение, что явствует из материалов многочисленных форумов и сайтов, посвященных данной тематике. Вместе с тем алгоритм действия оператора может быть весьма простым и состоять из следующих основных типов мероприятий:

первое, - привести собственную деятельность по обработке персональных данных в соответствие с комментируемым законом;

второе, - изучить требования законодательства страны получателя

отправляемых персональных данных и сравнить (провести сравнительно-правовое исследование), в чем отличия;

третье, - дать оценку и принять решение о возможности/невозможности осуществления трансграничной передачи данных. Данное мероприятие оператор может провести самостоятельно, при наличии соответствующих специалистов, либо обратиться в соответствующие научно-исследовательские организации. Кроме того, передачу персональных данных можно поручить соответствующей подготовленной организации. Более детальное описание процедуры можно посмотреть на соответствующих сайтах организаций, которые специализируются на оказании аудиторских услуг по обслуживанию персональных данных*(46).

Как правило, все рекомендации являются однотипными и весьма общими. Более детальное описание действий оператора возможно дать только при наличии сведений обо всех обстоятельствах трансграничной передачи данных. Представляется обоснованным полагать, что уполномоченный орган в рамках полномочий также будет ограничиваться общими рекомендациями. Это обусловлено ответственностью оператора за сохранность персональных данных.

4. Часть 4 комментируемой статьи содержит норму об осуществлении обязанностей оператора в случае трансграничной передачи персональных данных под юрисдикцию государства, которое не обеспечивает их адекватную защиту. В отношениях данного типа оператор должен уделить максимальное внимание отношениям с субъектом персональных данных (ситуации, предусмотренные пп. 1 и 4 комментируемой части статьи). Он должен проверить и учесть наличие свободы принятия субъектом решения; наличие собственной воли субъекта, т.е. отсутствие какого-либо давления на него со стороны; наличие интереса субъекта в связи передачей для возможной обработки его собственных персональных данных; получить и надлежащим образом (письменно или в электронной форме с соответствующими подписями) оформить полученное согласие. Только после этого он может приступать к трансграничной передаче персональных данных.

Согласно п. 2 комментируемой части статьи действующие соглашения с различными странами могут содержать особенности осуществления трансграничной передачи персональных данных применительно к соответствующей стране и конкретной ситуации (например, массовое перемещение гражданских лиц в случае природных катастроф, военных действий и т.д.). Консультации по данному вопросу оператор сможет получить в представительствах Министерства иностранных дел или консульских учреждениях за рубежом.

Пункт 3 комментируемой части транслирует на отношения по трансграничной передаче персональных данных норму-исключение, в соответствии с которой согласия на обработку персональных данных не требуется в случаях обеспечения безопасности субъектов персональных данных и иных лиц, например:

в случаях, предусмотренных законодательством Российской Федерации об обороне, в частности в соответствии со ст. 8 Федерального закона от 28.03.1998 N 53-ФЗ, согласно которой при осуществлении первичного воинского учета органы местного самоуправления поселений и органы местного самоуправления

городских округов обязаны осуществлять сбор, хранение и обработку сведений, содержащихся в документах первичного воинского учета, в порядке, установленном законодательством Российской Федерации в области персональных данных и Положением о воинском учете*(47);

в случаях, предусмотренных законодательством Российской Федерации о безопасности, например, ст. 13 Федерального закона от 03.04.1995 N 40-ФЗ, а также в случаях предусмотренных ст. 8 Федерального закона от 28.12.2010 N 390-ФЗ;

в случаях, предусмотренных законодательством Российской Федерации о противодействии терроризму, например, ст. 11 Федерального закона от 06.03.2006 N 35-ФЗ;

в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, а именно ст. 11 Федерального закона от 09.02.2007 N 16-ФЗ. (подробнее см. комментарий к ст. 11)

Пункт 5 комментируемой части статьи предусматривает ситуацию, в которой может не представиться возможность получить согласие субъекта персональных данных (например, в случаях крушений, катастроф и т.д.). Защита жизни и здоровья субъекта, находящегося в ситуации, когда его жизни и здоровью угрожает опасность в результате травмы или заболевания, также требует моментального принятия решения. В таком случает передача сведений, относящихся в категории медицинских данных (например, группа крови, перечень медицинских препаратов, вызывающих аллергическую реакцию, перечень медицинских противопоказаний, иных данных), должна осуществляться с последующим оформлением отношений по поводу трансграничной передачи данных.

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

1. Федеральный закон от 27.07.2006 N 149-ФЗ предлагает в ст. 13 классификацию информационных систем, согласно которым они подразделяются на государственные информационные системы, муниципальные информационные системы и иные информационные системы. При этом квалифицирующим признаком является не право собственности на информационные системы, а правовые основания их создания и функционирования. Государственные информационные системы - это федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов. Муниципальные информационные системы - системы, созданные на основании решения органа местного самоуправления.

При этом оператор операционной системы определяется уже на основании признака собственности. В п. 2 той же статьи устанавливается, что оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот

собственник заключил договор об эксплуатации информационной системы (если иное не установлено федеральными законами).

Государственные и муниципальные информационные системы, в том или ином объеме обрабатывающие персональные данные, внедряются в настоящее время во всех сферах государственного и муниципального управления. Перечислим основные области, в которых использование АИС является достаточно продолжительным и устоявшимся:

административный учет (АИС ЗАГС*(48), АИС "Паспортный стол" ЖЭО, государственная информационная система миграционного учета, АИС "Карта иностранного гостя"*(49), АИС "Регистрация", "АИС регистрации и учета АМТС и их владельцев"*(50));

социальная сфера (АИС "Электронный социальный регистр населения Санкт-Петербурга", АИС учета граждан, имеющих право на социальную поддержку при оплате жилых помещений и коммунальных услуг*(51), АИС "Молодежь", "распределенная автоматизированная система обработки информации по социальной защите населения г. Москвы");

налоговая сфера (АИС "Налог", АИС "Налог 2 Москва");

образование (АИС "Экзамен"*(52), используется в ряде регионов для проведения ЕГЭ, АИС ЕСП*(53));

здравоохранение (АС "Социально-гигиенический мониторинг"*(54));

государственные закупки (АИС "Государственный заказ", АИС "Госзакупки", АИС ЕРКТ);

избирательный процесс (ГАС "Выборы");

судопроизводство (ГАС "Правосудие", АИС "Арбитражный суд города Москвы", АИС "Ведение судебных дел").

В настоящее время наиболее масштабным проектом по автоматизации в сфере государственного и муниципального управления является выпуск универсальных электронных карт (УЭК).

Основной задачей универсальной электронной карты является идентификация пользователя и удостоверение его прав на получение государственных и муниципальных услуг, а также иных услуг, оказание которых осуществляется с учетом положений настоящей главы. Закон предполагает, в частности, использование универсальной электронной карты как средства аутентификации для совершения юридически значимых действий в электронной форме в случаях, предусмотренных законодательством РФ, юридически значимых действий в электронной форме.

В ст. 22 Федерального закона от 27.07.2010 N 210-ФЗ устанавливается, что на электронном носителе универсальной электронной карты подлежат фиксации следующие сведения, относящиеся к категории персональных данных:

фамилия, имя и (если имеется) отчество пользователя универсальной электронной картой;

фотография заявителя;

страховой номер индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования Российской Федерации;

дата, место рождения и пол пользователя универсальной электронной картой.

Кроме того, в области данных приложений универсальной электронной карты будут храниться и другие персональные данные (такие как номер полиса обязательного медицинского страхования застрахованного лица и т.д.).

Существует опасение, что концепция универсальной электронной карты нарушает один из основных принципов обработки персональных данных, а именно недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных. Здесь следует отметить, что универсальная информационная карта не является базой данных. На этой карте действительно объединяются данные из баз, созданных для несовместимых между собой целей, но речь идет именно об объединении отдельных данных, а не баз данных. Однако в рамках деятельности по выпуску универсальных электронных карт данные из различных баз данных, созданных для заведомо несовместных целей, будут поступать в центр персонализации и объединяться (пусть даже на временной основе) в автоматизированной информационной системе этого центра, что может привести к нарушению прав субъектов персональных данных.

2. Часть 2 комментируемой статьи содержит отсылку к федеральным законам, которыми могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных. В том числе, в этих федеральных законах могут устанавливаться различные способы обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.

К таким законам следует отнести Федеральный закон от 27.07.2004 N 79-ФЗ.

В ч. 1 ст. 42 устанавливаются специальные цели обработки персональных данных гражданского служащего. К ним относятся содействие гражданскому служащему в прохождении гражданской службы, обучении и должностном росте, обеспечение личной безопасности гражданского служащего и членов его семьи, а также обеспечение сохранности принадлежащего ему имущества, учет результатов исполнения им должностных обязанностей и обеспечение сохранности имущества государственного органа. Персональные данные гражданского служащего и иные сведения, связанные с поступлением на гражданскую службу, ее прохождением и увольнением с гражданской службы и необходимые для обеспечения деятельности государственного органа, заносятся в личное дело гражданского служащего. Кроме того, ст. 43 Федерального закона от 27.07.2004 N 79-ФЗ предусматривает обязанность представителя нанимателя вести реестр гражданских служащих, работающих в данном государственном органе. Реестр представляет собой систематизированные (в том числе на электронных носителях) сведения о прохождении государственной службы. Он ведется кадровой службой государственного органа на основе личных дел и карточек учета государственных служащих.

Закон обязывает получать персональные данные о гражданском служащем лично от него, а в случае, когда возникает необходимость получения таких

данных у третьей стороны, государственный гражданский служащий должен быть извещен о целях, источниках и способах их получения и дать на это свое согласие.

Статья 42 Федерального закона от 27.07.2004 N 79-ФЗ усиливает норму ч. 1 и 2 ст. 16 комментируемого закона. Она запрещает принятие решений, затрагивающих интересы гражданского служащего, на основе персональных данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей.

Аналогичные нормы содержит Федеральный закон от 30.11.2011 N 342-ФЗ "О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации", ст. 39 которого регламентирует обработку персональных данных сотрудников ОВД. По аналогии с нормами ст. 42 Федерального закона от 27.07.2004 N 79-ФЗ предусматривается, что в федеральном органе исполнительной власти в сфере внутренних дел, его территориальных органах, подразделениях ведутся личные дела, документы учета сотрудников ОВД, банки данных о сотрудниках и гражданах, поступающих на службу в ОВД, содержащие персональные данные сотрудников, сведения об их служебной деятельности и стаже службы, а также персональные данные членов семей сотрудников и граждан, поступающих на службу в ОВД.

В качестве примера приведем также Федеральный закон от 18.07.2006 N 109-ФЗ. Статья 10 этого закона содержит положение о государственной информационной системе миграционного учета, а ст. 9 - перечень сведений, хранящихся и обрабатываемых в такой информационной системе. К ним относятся:

1) вид и реквизиты документа, удостоверяющего личность и признаваемого Российской Федерацией в этом качестве (наименование, серия, номер, дата и место выдачи, срок действия, а при наличии - биометрические данные, содержащиеся в указанном документе);

2) вид и реквизиты документа, подтверждающего право на пребывание (проживание) в Российской Федерации;

3) фамилия, имя, отчество (последнее - при наличии);

4) дата и место рождения;

5) пол;

6) гражданство (подданство);

7) цель въезда в Российскую Федерацию;

8) профессия;

9) заявленные сроки пребывания (проживания) в Российской Федерации;

10) дата регистрации по последнему месту жительства и его адрес, даты регистрации и снятия с регистрации по предыдущим местам жительства и их адреса;

11) дата постановки на учет по последнему месту пребывания и его адрес, даты постановки на учет и снятия с учета по предыдущим местам пребывания и их адреса;

12) сведения о законных представителях (о родителях, об усыновителях, об опекунах, о попечителях);

13) сведения о депортации, об административном выдворении за пределы Российской Федерации или о реадмиссии (применялись или нет, если применялись, то когда и кем);

14) сведения о принятии решения о нежелательности пребывания (проживания) в Российской Федерации (принималось или нет, если принималось, то когда и кем);

15) сведения о привлечении в Российской Федерации к уголовной или административной ответственности либо к ответственности за совершение налоговых правонарушений;

16) дата и место смерти в Российской Федерации либо дата вступления в законную силу решения суда о признании безвестно отсутствующим или об объявлении умершим, наименование и место нахождения указанного суда;

17) основания постановки на миграционный учет и снятия с миграционного учета.

Наконец, приведем в качестве примера способа обозначения персональных данных идентификационный номер налогоплательщика (ч. 7 ст. 84 НК). Порядок и условия присвоения, применения, а также изменения идентификационного номера налогоплательщика установлены приказом МНС РФ от 03.03.2004 N БГ-3-09/178 "Об утверждении Порядка и условий присвоения, применения, а также изменения идентификационного номера налогоплательщика и форм документов, используемых при постановке на учет, снятии с учета юридических и физических лиц". Идентификационный номер налогоплательщика используется для идентификации персональных данных физических лиц в Едином государственном реестре налогоплательщиков. Согласно постановлению Правительства РФ от 26.02.2004 N 110 "О совершенствовании процедур государственной регистрации и постановки на учет юридических лиц и индивидуальных предпринимателей" реестр включает в себя государственные базы данных учета налогоплательщиков, ведется Федеральной налоговой службой и ее территориальными органами на основе единых методологических и программно-технологических принципов и документированной информации, поступающей в эти органы. Реестр ведется на бумажных и электронных носителях. При несоответствии сведений на бумажных носителях сведениям на электронных носителях приоритет имеют сведения на бумажных носителях. Ведение реестра осуществляется с использованием информационных технологий и включает в себя ведение государственных баз данных, формируемых по территориальному признаку, а также последующее автоматизированное объединение их в единый банк данных.

3. При обозначении принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных не допускается использования способов, оскорбляющих чувства граждан или унижающих человеческое достоинство. Формулируя эту норму, законодатель прежде всего имел в виду проблему, связанную с позицией представителей верующих, подвергавших резкой критике законопроект. По мнению критиков, присвоение числовых идентификаторов персональным данным граждан равносильно "нумерации" самих граждан, что является умалением их

человеческого достоинства. Не решив проблему до конца, законодатель переложил ее решение на разработчиков информационных систем. Поскольку в основе любой автоматизированной информационной системы персональных данных лежит база данных, а записи в базе данных должны каким-то образом идентифицироваться (причем этот идентификатор в любом случае будет иметь числовую природу), то каждая такая система не свободна от субъективных нападок. Следует согласиться с точкой зрения Н.И. Петрыкиной, что правовой порядок использования идентификаторов персональных данных не установлен, хотя их применение фактически легализовано, что может привести к злоупотреблениям и путанице в их использовании*(55).

Первое положение ч. 3 комментируемой статьи, а именно - недопустимость ограничения прав и свобод человека и гражданина 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, - можно толковать как в узком, так и в широком смысле. В узком смысле данная норма сводится к положению, уже рассмотренному выше, - сам способ идентификации персональных данных может нарушать право на свободу совести, оскорблять чувства верующих или наносить моральный вред субъектам персональных данных. В широком смысле конкретные способы обработки персональных данных, заложенные в алгоритме автоматизированной информационной системы, могут привести к нарушению прав субъекта персональных данных в различных (большей части административных) правоотношениях, для автоматизации которых используется данная государственная или муниципальная информационная система. В этом смысле комментируемая норма перекликается со ст. 16, в которой устанавливается, что 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 примером можно обратиться к одной из статей Д. Горелишвили, специализирующегося в области административного учета. Речь идет об учетной АИС для регистрации ПБОЮЛ, разработанной в начале 2000-х гг. (название системы в статье не приводится). Эта АИС не позволяла сделать запись о регистрации в базе данных в случае, если при вводе данных не заполнялось поле "зарегистрирован", содержащее сведения о регистрации по месту жительства. В результате гражданин без регистрации по месту жительства не мог зарегистрироваться в качестве ПБОЮЛ, так как программа не присваивала необходимый для выдачи свидетельства регистрационный номер. При этом нарушалось конституционное право на предпринимательскую деятельность (которое не ограничивалось для незарегистрированного по месту жительства гражданина действующим на тот момент законодательством*(56)). В суде не удалось доказать, "что компьютерная программа является приложением к инструкции для должностного лица, поскольку инструкция утверждается Председателем Регистрационной палаты, а компьютерная программа, как

выяснилось, никем не утверждается, а является коммерческим продуктом, разработанным каким-то сторонним разработчиком, который не назывался"*(57). Комментируемый закон устанавливает недопустимость подобной ситуации при обработке персональных данных в государственных и муниципальных информационных системах.

4. Впервые концепция создания государственного регистра населения была разработана в 2000 году Министерством РФ по связи и информатизации в соответствии с распоряжением Правительства РФ от 02.03.2000 N 323-р. На основе существующей системы регистрации граждан по месту жительства и по месту пребывания предполагалось создать единую автоматизированную информационную систему АС ГРН, решающую проблему информационного взаимодействия различных АИС учета населения (создаваемых федеральными органами исполнительной власти с целью решения возложенных на них задач, таких как выплата пенсий, социальных пособий, взимание налогов, проведение избирательных кампаний и т.д.).

По замыслу разработчиков концепции, АС ГРН должна содержать первичные персональные данные о гражданах, формирующиеся при регистрации граждан по месту жительства и при государственной регистрации актов гражданского состояния, а также сводные данные, формирующиеся в результате агрегирования первичных данных. Аналитические данные о различных категориях населения будут формироваться в федеральных автоматизированных информационных системах и в информационно-аналитических центрах администраций федеральных округов, регионов и муниципальных образований в соответствии с возложенными на эти органы функциональными задачами.

Разработка АИС ГРН в рамках федеральной целевой программы "Электронная Россия (2002-2010 годы) завершена не была, однако предпосылки создания такой системы были зафиксированы законодателем в комментируемом законе.

С 05 декабря 2005 г. введена в эксплуатацию автоматизированная информационная система "Государственный регистр населения Санкт-Петербурга", положение о которой утверждено постановлением Правительства Санкт-Петербурга от 07.09.2004 N 1472. АИС "ГРН Санкт-Петербурга" создана для решения следующих задач:

создание условий для развития и интеграции ГИР Санкт-Петербурга и ведомственных АС учета населения за счет использования единых стандартов на форматы представления данных, единой системы идентификации сведений о личности, единой объектно-адресной системы и общесистемных лингвистических средств;

создание условий для обеспечения единого государственного учета сведений о населении СПб, обеспечения совместимости и сопоставимости значений различных социально-экономических показателей при информационном взаимодействии федеральных органов государственной власти и органов государственной власти СПб;

обеспечение органов государственной власти СПб достоверной и актуальной социально-демографической информацией, охватывающей все

категории граждан.

В состав персональных данных, содержащихся в ГРН Санкт-Петербурга, входят следующие сведения: персональный идентификационный номер гражданина; Ф.И.О.; дата и место рождения; пол, гражданство; адрес регистрации по месту проживания; реквизиты документа, удостоверяющего личность (паспорта или др.); дата прибытия к месту проживания, место, откуда прибыл; дата выбытия с места проживания, место и причина выбытия (отъезд за пределы Санкт-Петербурга, смерть); семейное положение; информация о родителях (усыновителях, опекунах) для несовершеннолетних детей до 14 лет.

В связи с внедрением универсальных электронных карт и предоставлением государственных и муниципальных услуг в электронном виде возникла объективная необходимость централизованного хранения и обработки данных о получателях таких услуг. В постановлении Правительства РФ от 28.11.2011 N 977 "О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" устанавливается, что единая система идентификации и аутентификации помимо регистров юридических лиц, органов и организаций, их должностных лиц, информационных систем должна включать в себя регистр физических лиц. Государственный регистр населения, предусмотренный в комментируемом законе, вполне может быть построен на базе данной информационной системы (ранее планировалась положить в основу базу данных государственной автоматизированной системы "Выборы").

Глава 3. Права субъекта персональных данных

Статья 14. Право субъекта персональных данных на доступ к его персональным данным

1. Часть 1 комментируемой статьи содержит нормативную формулу юридической конструкции права субъекта персональных данных на доступ к его персональным данным, состоящего из комплекса определенных правомочий.

В состав правомочий субъекта персональных данных входят:

право на получение сведений;

право требовать от оператора уточнения его персональных данных;

право блокировать свои персональные данные;

право уничтожить свои персональные данные в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

право принимать предусмотренные законом меры по защите своих прав.

Права субъекта ограничены правами других лиц, в частности в случаях, предусмотренных ч. 8 комментируемой статьи. Права субъекта персональных данных являются производными от права человека на жизнь и права на информацию. В отдельных контекстах в информационной сфере, в зависимости

от конструкции конкретных правоотношений, права субъекта персональных данных можно рассматривать как производную часть или как составную часть от права на информацию. Такое понимание природы представляется современным, соответствующим всем основным тенденциям науки информационного права. Вместе с тем можно предположить наличие иных подходов к пониманию природы прав субъекта персональных данных.

Некоторые исследователи позиционируют себя как сторонники отраслевой природы прав субъектов персональных данных. Так, А.В. Дворецкий формулирует право персональных данных из двух основных правомочий: право субъекта знать собственные персональные данные, собранные работодателем, и право таить от иных лиц содержание сведений, составляющих персональные данные*(58). Автор не выходит за рамки трудового права и предлагает закрепить разработанные положения и принципы защиты персональных данных в ТК РФ. Другой автор, Л.К. Терещенко, ссылаясь на международные акты, отмечает, что право на неприкосновенность частной жизни и, как следствие, право на защиту персональных данных - это право относительное, а не абсолютное. При этом автор признает наличие тенденции рассматривать защиту персональных данных как самостоятельное право гражданина, т.е. отдельно от более широкого права на уважение частной и семейной жизни. Другое обстоятельство, подчеркнутое автором, - это отсутствие баланса интересов, закрепленных в комментируемом законе *(59).

Весьма основательным представляется исследование М.Н. Малеиной, которая представила аргументированное мнение по различным аспектам тайны персональных данных как объекта правового регулирования и субъективного права самого субъекта. В частности, она предлагает рассматривать тайну частной жизни как общую родовую категорию, включающую профессиональные и непрофессиональные тайны; тайна персональных данных - одна из видов тайн. Дискутируя с В.Б. Наумовым, она относит к персональным данным также сведения о сетевой активности субъекта. Основываясь на положениях комментируемого закона о возможности исключения персональных данных из общедоступных источников персональных данных по требованию субъекта, М.Н. Малеина утверждает, что доминирующим является режим тайны персональных данных, а исключения составляют режим общедоступности персональных данных и режим государственной тайны*(60).

2. Часть 2 комментируемой статьи содержит процедурную норму, которой определяется форма представления персональных данных субъекту-заявителю. В комментируемой статье не раскрывается термин "доступная форма". Вместе с тем общие требования к порядку рассмотрения обращений граждан обуславливают порядок, в соответствии с которым ответ необходимо формировать в той же форме, в какой получен запрос, если иное не предусмотрено законодательством или не указано в обращении заявителя. Готовность получить ответ в форме электронного сообщения письма или короткого текстового сообщения или сообщения в социальной сети должна быть обозначена в запросе. Если отправитель прямо указал, в какой форме он готов получить ответ, и эта форма не совпадает с первичным отправлением, возникает дилемма: отправить ответ в формате полученного письма обращения либо

отправить ответ в соответствии с требованием заявителя. Запрос лицом персональных данных для представления их третьему лицу (например, запрос о сроках трудовой занятости или сроках прохождения службы для оформления пенсии) может иметь определенные временные ограничения. Соответственно, пересылка заявителю двух экземпляров документа, для дальнейшей пересылки необходимого самим субъектом по назначению, есть действие не рациональное, а в отдельных случаях - просто вредное. Например, пожилой человек может оформить запрос с помощью родственника, который не сможет проконтролировать ответ и дальнейшую пересылку запрошенного документа. Дать однозначный ответ для всех случаев - невозможно. Отправка ответа в каждый адрес - также может быть ошибочной. Вероятно, необходимо сделать краткий анализ ситуации с участием штатного специалиста в области права (юрисконсульта). Ориентиром должна быть оценка сведений, которые предполагаются к отправке. Другое требование, изложенное в комментируемой части, - отсутствие дополнительных персональных данных, относящихся к другим субъектам. Это логичное требование, которое согласуется с общим правилом предоставления персональных данных только их субъекту. Исключения из данного правила также обусловлены законом. Логично предположить, что исключения возможны в отдельных весьма специфичных сферах, например, в сфере семейных отношений (получение сведений родителем о ребенке и т.д.).

3. Часть 3 комментируемой статьи содержит процедурную норму, которая включает основные способы подачи и удовлетворения запроса субъекта персональных данных. Субъект может обратиться лично либо через представителя, таким образом, ограничен субъектный состав. Это представляется логичным, поскольку не все субъекты персональных данным обладают полной правоспособностью (например, дети, или иные лица, в предусмотренных законом случаях), соответственно, реализация их права предусмотрена с помощью представителя. Специально законом не предусмотрено, но есть основания полагать, что данный субъектный состав соответствует и всем способам (в техническом отношении) подачи и получения запроса, а именно путем обращения (надо полагать, личного обращения, поскольку иное в законе не указано), путем подачи заявления (документальный запрос), путем подачи заявления в форме электронного документа (электронный запрос). Обращение в электронном виде требует наличия электронной подписи. В комментируемой статье не уточняется, каким именно из трех видов (простая, квалифицированная, усиленная) электронной подписи в соответствии с действующим законодательством об электронной подписи должно быть подписано обращение. Согласно сложившейся практике (приказы, инструкции) государственные органы рекомендуют принимать обращения, подписанные не ниже чем квалифицированной электронной подписью.

4. Часть 4 комментируемой статьи содержит норму, которая предусматривает право на повторное обращение к оператору персональных данных в срок не ранее чем через тридцать дней. Это минимальный срок между обращениями субъекта к оператору по поводу его (субъекта) персональных данных. Вероятно, не требует объяснения тот факт, что время, необходимое для

подготовки письменного (печатного) ответа, значительно превышает время для подготовки такого же ответа в электронной форме и срок не менее тридцати дней обусловлен именно временем для подготовки письменного (печатного) ответа. В течение предусмотренного срока оператором могут быть выполнены мероприятия по устранению нарушений в порядке обработки персональных данных, что, вероятно, и является причиной предусмотренного повторного обращения. В связи с ожидаемым в 2013-2018 годы переходом государственных органов на электронный документооборот (см. Государственную программу РФ "Информационное общество (2011-2020 годы)", утвержденную распоряжением Правительства РФ от 20.10.2010 N 1815-р), логично предположить, что срок повторного обращения может быть изменен. Соответственно, переход на электронный документооборот позволит реагировать на обращения в более короткие сроки. Возможность такой ситуации предусмотрена нормой, закрепленной в комментируемой части статьи. Изменение сроков на договорной основе является дозволением для участников гражданских правоотношений ввести иные сроки по усмотрению сторон. Законодательство не ограничивает субъектов предпринимательской деятельности в правах использовать электронные формы документооборота, что позволяет реализовать отношения в очень короткие сроки, логично, что сроки повторного обращения в таких случаях могут быть значительно сокращены.

5. Часть 5 комментируемой статьи содержит норму, согласно которой субъект персональных данных вправе обратиться к оператору повторно. Повторный запрос по существу носит уточняющий характер. Норма содержит условие, при котором правомерность повторного запроса считается обоснованной, а именно - при неполноте полученных в ответе на первоначальный запрос сведений. Норма о праве повторного запроса, кроме материальной правовой составляющей, содержит отдельные процедурные требования к запросу, а именно требование обосновать направление повторного запроса. Таким образом, закрепленная в ч. 5 комментируемой статьи норма содержит материально-правовые и процессуальные условия, направленные на обеспечение полноты прав субъекта персональных данных в части обеспечения его сведениями о том, в каком объеме оператор производит обработку данных.

6. Часть 6 комментируемой статьи содержит смешанную норму материально-правового и процессуального характера. Норма закрепляет частный случай в комплексе отношений оператора и субъекта персональных данных - это право оператора персональных данных на защиту от необоснованных запросов, которые не соответствуют требованиям, изложенным в ч. 4 и 5 комментируемой статьи. Право оператора соответствует его же обязанности обосновать причину отказа, т.е. самостоятельно представить аргументы, на основании которых оператор отказывает удовлетворить повторный запрос.

7. Часть 7 комментируемой статьи можно рассматривать через призму международных норм европейского права о защите персональных данных, тем более что Россия является участником многих соглашений по данному вопросу.

В отношении большинства положений ч. 7 комментируемой статьи действует общее правило, введенное Директивой 95/46/ЕС, которое

предусматривает минимальный объем требуемых сведений, т.е. минимальный уровень, ниже которого национальный законодатель (в том числе российский) не должен опускаться.

В целом сведения можно условно классифицировать следующим образом:

информация об операторе и доверенных лицах;

цели обработки;

объем сведений и порядок сбора.

В пределах юрисдикции каждое государство устанавливает необходимый объем требований по раскрытию субъекту сведений об операторе и объемах обработки данных. Так, в частности, требования о предоставлении сведений об операторе и/или его представителе (п. "а" ст. 10 Директивы 95/46/ЕС) практически полностью соответствуют тем требованиям, которые изложены в ч. 7 комментируемой статьи. Можно также отметить более высокую степень детализации требований в комментируемой статье по сравнению с требованиями ст. 10 Директивы 95/46/ЕС. Практически полностью соответствуют друг другу нормы о целях обработки персональных данных. Более широко в Директиве 95/46/ЕС представлены требования о порядке сбора персональных данных. Так, в частности, к другой информации, которая должна быть предоставлена по требованию субъекта персональных данных, относятся сведения о добровольности/обязательности представления персональных данных и последствиях отсутствия персональных данных. Комментируемый закон не содержит полного, исчерпывающего ответа на данный вопрос, но судебная практика формирует подходы к данной проблеме, которые в будущем, возможно, будут оформлены в качестве норм.

Пример: Советский районный суд по делу (Областной наркологический диспансер против прокуратуры) о нарушении законодательства о персональных данных вынес решение об отказе в удовлетворении заявления о признании законным требования дополнительных данных. В ходе рассмотрения дела было установлено, что Областной наркологический диспансер требовал от клиентов избыточные персональные данные по отношению к заявленным целям их обработки. На требования надзорного органа - Роскомнадзора - устранить нарушение диспансер реагировал неадекватно, нарушение не устранил. Представление прокуратуры об устранении нарушения законодательства диспансер не исполнил и обратился в суд с жалобой. Суд, исследовав все материалы, принял решение о признании представления об устранении нарушений законодательства о персональных данных по жалобе клиента законным, в удовлетворении жалобы Областного наркологического диспансера отказал (см. решение Советского районного суда г. Астрахани от 13.08.2012 по делу N 2-2739/2012).

8. Часть 8 комментируемой статьи содержит норму, которая предусматривает, что право субъекта персональных данных на доступ к его персональным данным может быть ограничено на основании федерального закона. Данное ограничение носит преимущественно характер исключения из общего правила - права субъекта персональных данных на доступ к его

персональным данным. Ограничение также можно рассматривать как предел (границу, край) права субъекта персональных данных на доступ к его персональным данным. Данная конструкция более применима к характеристике п. 4 ч. 8 комментируемой статьи. Пределом в этом случае является право иного лица - субъекта персональных данных - на доступ к его персональным данным. Разбор и исследование теоретических конструкций, заложенных в комментируемой статье закона, могут в отдельных случаях провоцировать непонимание. Тем не менее они имеют сугубо практическое значение. Например, подготовка локальных актов (положений, приказов, инструкций, иных документов), регулирующих отношения по поводу персональных данных, невозможна без учета всех положений комментируемого закона и иных федеральных законов в сфере оборота персональных данных. Часть 8 комментируемой статьи содержит также сведения о специальных нормах, закрепленных соответствующими нормативными актами, которыми права субъекта персональных данных могут быть ограничены.

Ограничения прав субъекта персональных данных возможны в случаях, предусмотренных законодательством Российской Федерации об оперативно-розыскной деятельности. В соответствии со ст. 6, 8-12 Федерального закона от 12.08.1995 N 144-ФЗ оперативно-розыскные мероприятия осуществляются в формах, предусмотренных законом. Процедура, порядок документирования и проверки оперативно-розыскных мероприятий строго регламентирован. Ограничение прав субъектов персональных данных возможно также в связи с реализаций отдельных разведывательных и контрразведывательных мероприятий, предусмотренных ст. 8, 17-23 Федерального закона от 10.01.1996 N 5-ФЗ "О внешней разведке". В соответствии со ст. 11 Федерального закона от 06.03.2006 N 35-ФЗ правовой режим контртеррористической операции предполагает введение ряда ограничений, которые касаются, в том числе, персональных данных. Например, в целях пресечения и раскрытия террористического акта, минимизации его последствий и защиты жизненно важных интересов личности, общества и государства на территории, в пределах которой введен правовой режим контртеррористической операции, допускается: проверка у физических лиц документов, удостоверяющих их личность, а в случае отсутствия таких документов - доставление указанных лиц в органы внутренних дел Российской Федерации (иные компетентные органы) для установления личности; проведение досмотра физических лиц и находящихся при них вещей. В соответствии с отдельными нормами в области обеспечения безопасности Федерального закона от 28.12.2010 N 390-ФЗ Президент Российской Федерации имеет полномочия по принятию мер по защите граждан от преступных и иных противоправных действий. Полномочия перечисленных субъектов реализуются в рамках рассмотренного законодательства без согласия субъектов персональных данных с ограничением отдельных прав.

В связи с мероприятиями по противодействию коррупции в случаях, предусмотренных Федеральным законом от 25.12.2008 N 273-ФЗ и Федеральным законом от 03.12.2012 N 230-ФЗ, возможны ограничения прав субъектов персональных данных (см. также комментарий к ст. 11).

Ограничение прав субъекта возможно в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в том числе отдельными положениями Федерального закона от 09.02.2007 N 16-ФЗ. Одной из функций транспортной информационной системы является обеспечение безопасности перевозок, в том числе путем передачи данных, содержащихся в проездных документах (билетах), в автоматизированные централизованные базы персональных данных о пассажирах в соответствии с комментируемым законом. Ограничение возможно также в связи с реализацией ст. 85.1, 103, 105 ВК РФ.

Современные представления о защите персональных данных в Европе необходимо соотносить с последними из принятых документов. Одним из таких является Резолюция Европейского парламента от 06.07.2011 о комплексном подходе к защите персональных данных в Европейском союзе (2011/2025 (INI)) (подробнее см. комментарий к ст. 9).

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. Часть 1 комментируемой статьи содержит два блока норм:

1) об особых условиях обработки персональных данных в целях рекламы с помощью средств связи;

2) об особых условиях обработки персональных данных в целях политической агитации.

Основное условие обработки в каждом из перечисленных случаев - получение предварительного согласия субъекта персональных данных. Часть 1 комментируемой статьи содержит также норму, которой вводится презумпция вины оператора за отсутствие согласия субъекта персональных данных на обработку персональных данных оператором, до тех пор пока оператор не докажет, что такое согласие было получено.

1.1. Нормы об особых условиях обработки персональных данных в целях продвижения товаров, работ, услуг на рынке (т.е. рекламы) путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи - это особый вид отношений, регулирование которых специально выделено Европейским Союзом. Основным документом, которым предлагается руководствоваться, является Директива 2002/58/ЕС Европейского парламента и Совета ЕС от 12.07.2002 об обработке персональных данных и защите информации о частной жизни в сфере электронных коммуникаций (Директива о конфиденциальности информации о частной жизни в сфере электронных коммуникаций), которая учитывает специфику и особые условия оказания услуг. В России отношения в данной сфере только начинают формироваться, многие нормы комментируемого закона, в том числе положения комментируемой статьи, принимались на перспективу. Одновременно, в феврале 2013 года, в связи инициативой отдельных российских министерств началось активное обсуждение нескольких проектов законов о регулировании отношений в информационно-телекоммуникационной сети Интернет. В условиях существующей действительности европейская законодательная практика служит

перспективной моделью для формирования российских правовых традиций. Директива конкретизирует и дополняет Директиву 95/46/ЕС Европейского парламента и Совета ЕС от 24.10.1995 о защите физических лиц в отношении обработки персональных данных и свободного обращения таких данных. Цель Директивы - обеспечить защиту персональных данных, не нарушая прав на свободную коммуникацию (общение) в сетях электронной коммуникации. Развитие информационного общества характеризуется введением новых услуг электронной связи. Доступ к цифровому мобильному Интернету стал возможным для широкой общественности, что порождает определенные требования к защите персональных данных и информации о частной жизни пользователя. Применительно к коммуникациям, осуществляемым посредством общедоступной телекоммуникационной сети, должны быть разработаны специальные законодательные, регулятивные и технические положения, с тем чтобы обеспечить защиту основных прав и свобод физических лиц и законных интересов юридических лиц. В особенности это имеет большое значение в связи с увеличивающейся способностью автоматизированного хранения и обработки персональных данных абонентов и пользователей. Директива не регулирует отношения в сфере телерадиовещательных услуг. Также она не применяется в отношении видов деятельности, касающихся общественной безопасности и обороны, государственной безопасности (включая экономическое благосостояние государства, когда речь идет о делах государственной безопасности) и в отношении деятельности государства в областях уголовного права. Директива вводит для дальнейшего применения целый ряд терминов (пользователь, данные трафика, сообщение, дополнительная услуга, электронная почта, повреждение системы безопасности персональных данных). Это сделано для того, чтобы максимально уточнить понимание термина в контексте директивы или сложившихся отношений. Так, например, термины "сообщение" и "электронная почта" понимаются гораздо шире, чем привыкли российские потребители. В новом контексте эти термины могут обозначать практически любое отображение информации, которое воспринимает потребитель. Естественно, в связи с этим расширилось понимание действий субъекта персональных данных, и в частности такое действие, как получение согласия. В новом контексте согласие может быть выражено нажатием на клавишу (клик). Данная директива должна применяться в отношении обработки персональных данных в связи с предоставлением общедоступных услуг электронной связи в сетях связи коллективного доступа в Сообществе, в том числе в сетях связи коллективного доступа, поддерживающих сбор данных и устройства идентификации. Поставщик услуг электронной связи должен предпринять необходимые технические и организационные меры для обеспечения безопасности предоставляемых услуг, в частности гарантировать, что доступ к персональным данным может быть предоставлен только уполномоченному персоналу в разрешенных законом целях. Он должен защищать персональные данные, гарантировать введение политики безопасности в отношении обработки персональных данных. При наличии определенной угрозы повреждения системы безопасности сети он должен информировать абонентов в отношении такой угрозы и т.д. Для сохранности

персональных данных директива предусматривает комплекс обязанностей оператора по поддержке конфиденциальности сообщений, сохранности трафика, технической возможности контроля фиксации номера вызывающего абонента и детализации счетов за оказанные услуги. Директивой установлено, что использование систем связи автоматического повтора вызова без человеческого вмешательства, факсимильных аппаратов (факсов) или электронной почты в целях прямого маркетинга допускается только в отношении абонентов или пользователей, давших свое предварительное согласие. Кроме того, директивой вводится прямой запрет на рассылки сообщений в целях прямого маркетинга электронной почты, маскирующей отправителя сообщений, с недействительного адреса, на который получатель не может отправить запрос о прекращении отправки таких сообщений.

Что касается действующего российского законодательства в сфере электронных коммуникаций, то оно представлено Федеральным законом от 07.07.2003 N 126-ФЗ. Статьей 53 Федерального закона от 07.07.2003 N 126-ФЗ закреплено понятие сведений об абонентах. Названные сведения являются информацией ограниченного доступа и подлежат защите в соответствии с законодательством Российской Федерации. К сведениям об абонентах отнесены фамилия, имя, отчество или псевдоним абонента-гражданина, наименование (фирменное наименование) абонента - юридического лица, фамилия, имя, отчество руководителя и работников этого юридического лица, а также адрес абонента или адрес установки оконечного оборудования, абонентские номера и другие данные, позволяющие идентифицировать абонента или его оконечное оборудование, сведения баз данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента. Категория сведений об абонентах по правой конструкции и правовому режиму имеет много общего с категорией персональных данных. Сравнив объем понятий этих понятий, можно предположить, что в рамках российской юрисдикции отношения к каждому из представленных видов данных (сведений) должно быть практически идентичное. В этой связи представляет интерес следующий пример.

Оператор связи при заключении договора в типовой форме договора ограничил одной графой для подписи абонента место для выражения абонентом согласия на использование сведений в системе информационно-справочного обслуживания и согласия, разрешающего обработку персональных данных. Получив предписание об устранении нарушения, оператор обжаловал его в арбитражный суд. Суд первой инстанции жалобу удовлетворил. Апелляционная инстанция решение отменила по той причине, что договор, заключенный с абонентом, не содержит отдельное поле для получения согласия абонента на обработку его персональных данных, поэтому предписание, выданное Управлением Роскомнадзора, правомерно. Сведения, представленные в договоре оказания услуг связи, относятся к персональным данным. Действия, производимые оператором с данными абонента, включенными в договор, (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение), понимаются как обработка персональных данных. Обработка данных возможна только с согласия субъекта

персональных данных. Впоследствии суд кассационной инстанции подтвердил верность данной позиции (см. постановление Шестнадцатого арбитражного апелляционного суда от 16.06.2011 по делу N А63-11458/2010, постановление ФАС Северо-Кавказского округа от 03.10.2011 по делу N А63-11458/2010).

Анализ представленной ситуации может свидетельствовать о том, что для персональных данных, их обработки требуется иной, более жесткий, правовой режим. Пример характерен в данной ситуации тем, что и персональные данные, и сведения об абоненте находятся на одном материальном носителе и как совокупность знаков, символов, во многом совпадают. Дальнейший анализ статьи 53 Федерального закона от 07.07.2003 N 126-ФЗ для сравнения правового режима баз данных об абонентах (возможного их хранения и использования, в том числе на магнитных носителях) с правовым режимом персональных данных, которые могут быть использованы в рекламных целях с применением средств электронных коммуникаций, позволяет допустить, что операторы и операторы связи используют практически одинаковые (идентичные) базы персональных данных. В этой связи представляется обоснованным констатировать, что должный уровень правопонимания и правоприменения норм, регулирующих отношения по поводу сведений об абонентах и персональных данных, заложенных в комментируемую статью, окончательно в России не сложился.

К аналогичным выводам приходит О.И. Трофимов, предметом исследования, которого были "...нормы информационного, гражданского, административного и других отраслей права, регулирующих общественные отношения, возникающие по поводу оборота баз данных операторов электросвязи"*(61). Он, в частности, полагает, что недооценка степени общественной опасности незаконного оборота баз данных приводит к негативным последствиям (рост правонарушений в информационной сфере, увеличение материального и морального ущерба операторам баз данных и субъектам персональных данных; рост числа попыток неправомерного использования баз данных операторов связи; несанкционированный анализ событий и фактов для установления личности другого пользователя; неправомерный доступ к информации абонента и другие)*(62). Автор предлагает дополнить законодательство обязанностью оператора связи приостановить оказание услуг связи при обнаружении определенных технических нарушений (совпадение идентификационного номера терминала с номером, включенным в базы данных утраченных, похищенных, несертифицированных номеров) и выдвигает ряд других предложений.

Режим персональных данных в процессе поиска и приобретения товаров, продуктов и услуг подвергается испытаниям не только правового характера. Оформляя разного рода отношения с различными субъектами (медицинские учреждения, магазины, мастерские, салоны, предприятия по оказанию развлекательных услуг и т.д.), потребители получают предложение оформить документы на дисконтную карту, карту постоянного посетителя, клубную карту и т.д. Получив такой документ, потребитель в первую очередь руководствуется своими интересами: потратить меньшую сумму денег, получить предварительное извещение о поставке товара, услуги, - при этом потребителю предлагается каким-то образом идентифицировать свою личность, оставить сведения о

телефоне, домашнем адресе и адресе электронной почты и т.д. Выполняя просьбу продавца и заполняя необходимую анкету, потребитель весьма редко выясняет порядок получения сообщений на оставленный у продавца контактный номер адрес и т.д. В этот момент потребитель поглощен процессом оформления льготы - иногда подобная ажиотажная ситуация формируется продавцом специально. Необходимо представлять, что в данной ситуации субъект, охваченный потребительским азартом, с большой долей вероятности не задумывается об условиях сделки. Игнорировать данное обстоятельство не следует. Примером, иллюстрирующим поведение людей в данной ситуации, являются марафоны распродаж, которые привлекают множество людей в различных странах. Оценить последствия акта распоряжения персональными данными в данной ситуации законодатель поручил оператору. Он возложил на оператора обязанность доказывания согласия субъекта на обработку персональных данных.

Статья 18 Федерального закона от 13.03.2006 N 38-ФЗ "О рекламе" закрепляет положения, аналогичные установленным в европейском и российском законодательстве. Так, например, распространение рекламы по сетям электросвязи, в том числе посредством использования телефонной, факсимильной, подвижной радиотелефонной связи, допускается только при условии предварительного согласия абонента или адресата на получение рекламы. При этом реклама признается распространенной без предварительного согласия абонента или адресата, если рекламораспространитель не докажет, что такое согласие было получено. Рекламораспространитель обязан немедленно прекратить распространение рекламы в адрес лица, обратившегося к нему с таким требованием. Федеральным законом от 13.03.2006 N 38-ФЗ также запрещено использование сетей электросвязи для распространения рекламы с применением средств выбора и набора абонентского номера без участия человека. На практике, заполнив анкету, предусматривающую согласие на получение в будущем рекламных материалов, потребитель, как правило, забывает о том, что ему придется принимать все направленные в его адрес сообщения, поскольку он дал на них согласие и сам дал адрес. Однако такие сообщения не будут являться спамом.

Особенностью, предусмотренной комментируемой статьей, является обязательное согласие субъекта на использование его персональных данных в рекламе. Изображение лица субъекта, которое в виде фотографии имеет место практически во всех значимых документах, удостоверяющих личность, также следует относить к персональным данным.

Наглядным примером тому является рассмотренное в одном из судов города Москвы дело об использовании клиникой фотографии одной популярной и узнаваемой певицы с припиской о том, что она является другом заведения*(63). Нет сомнения, что фотография использовалась в рекламных целях. В данном случае использования одной фотографии узнаваемого лица было достаточно, чтобы без каких-либо дополнительных сведений идентифицировать субъекта персональных данных. Узнаваемость лица и отсутствие письменного согласия на использование изображения в данном случае явились основаниями признать незаконным использование

фотографического изображения.

1.2. Нормы об особых условиях обработки персональных данных в целях политической агитации содержатся в избирательном законодательстве. В соответствии со ст. 16 и 17 Федерального закона от 12.06.2002 N 67-ФЗ "Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации" регистрация субъектов персональных данных (в редакции закона - избирателей, участников референдума) осуществляется на основе списков, которые в обобщенном виде представляют собой регистр избирателей, участников референдума - информационный ресурс ГАС "Выборы"*(64), содержащий совокупность персональных данных об избирателях, участниках референдума. Списки формируются под руководством главы соответствующей местной администрации муниципального района, округа. Список избирателей, участников референдума составляется в двух экземплярах. Сведения об избирателях, участниках референдума, включаемые в список избирателей, участников референдума, располагаются в алфавитном или ином порядке (по населенным пунктам, улицам, домам, квартирам). В списке указываются фамилия, имя, отчество, год рождения (в возрасте 18 лет - дополнительно день и месяц рождения), адрес места жительства избирателя, участника референдума. Аналогичные сведения формируются на основании других законов в сфере избирательных отношений. В соответствии со ст. 26 Федерального закона от 10.01.2003 N 19-ФЗ "О выборах Президента Российской Федерации" составлением списков избирателей занимается соответствующая избирательная комиссия. Список избирателей составляется в двух экземплярах. Сведения об избирателях, включаемых в список избирателей, располагаются в списке в алфавитном или ином порядке (по населенным пунктам, улицам, домам, квартирам). В списке указываются фамилия, имя, отчество, год рождения избирателя (в возрасте 18 лет - дополнительно день и месяц рождения), адрес его места жительства. В соответствии со ст. 15 Федерального закона от 18.05.2005 N 51-ФЗ "О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации" составлением списков избирателей занимается соответствующая территориальная избирательная комиссия. Список избирателей составляется в двух экземплярах. Первый экземпляр списка изготавливается на бумажном носителе в машинописном виде, второй экземпляр - в машиночитаемом виде. Сведения об избирателях, включаемых в список избирателей, располагаются в алфавитном или ином порядке (по населенным пунктам, улицам, домам, квартирам). В списке избирателей указываются фамилия, имя и отчество, год рождения избирателя (в возрасте 18 лет - дополнительно день и месяц рождения), адрес его места жительства. При составлении всех списков избирателей может использоваться ГАС "Выборы".

2. Часть 2 комментируемой статьи предусматривает немедленное устранение нарушения. Законодательство, рассмотренное применительно к комментируемой статье, также содержит требование о немедленном прекращении нарушения. Многолетней практикой в различных отраслях деятельности выработаны различные критерии терминов "немедленно", "срочно", "незамедлительно" и других. Как правило, такие резолюции формализованы и закреплены ведомственными нормативными актами,

регламентирующими делопроизводство. В иных случаях они передаются в качестве обычаев делового оборота либо иными способами. В каждом конкретном случае суду надлежит установить, насколько срочно требуется устранить нарушение, и дать соответствующее пояснение в самом решении либо в разъяснении. Требование прекратить обработку персональных данных будет корректным, если субъект, от которого оно исходит, укажет конкретный срок, например: "немедленно, в течение суток". В спорных случаях суд будет вынужден устанавливать наличие технической возможности "немедленного" устранения нарушения. Точное определение даты, точного времени, способа и процедуры устранения нарушения необходимо в каждом спорном случае. В любом случае оставлять данную фразу без толкования не следует, т.к. срок, не определенный формально, может быть истолкован каждым субъектом по-своему.

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

1. Комментируемая статья содержит понятие автоматизированной обработки, которое, по мнению законодателя, необходимо выделить в качестве отдельной, специальной категории и отдельного вида обработки персональных данных. Для того чтобы понять причины, побудившие выделить автоматизированную обработку в отдельную категорию, необходимо выяснить, как она возникла, что собой представляет и чем отличается от неавтоматизированной, ручной обработки для правовых целей (законодательных, правоприменительных и охранительных).

Понятие автоматизированной обработки тесно связано с теорией автоматов и относится к научным терминам, категориям математики и информатики. Вопросы автоматизации привлекали исследователей во все времена. В современной истории наиболее активные исследования начались в конце 20-х годов XX века. В период второй мировой войны основные усилия были направлены на расчеты и обработку разведывательных данных (расшифровку сообщений). По существу, эти исследования и привели к созданию первых электронно-вычислительных машин. Одновременно с практическими вопросами разрабатывалась и теория автоматов. Часть исследований после второй мировой войны была оформлена в виде Общей и логической теории автоматов (Д. Нейман - А. Тьюринг, 1960, в США) и в виде Абстрактной теории автоматов (В.М. Глушков, 1961, в СССР), а также в огромном количестве других работ на эту тему. Посещение в 1961 году СССР основателем кибернетики Н. Винером активизировало интерес к автоматизированной обработке данных в правовой сфере. В некоторых ВУЗах Москвы, Киева были открыты курсы правовой кибернетики. В период 60-70 годов XX века сформировались основные понятия, которые используются и в настоящее время.

Так, например, automatic data processing (ADP) - автоматическая обработка данных - включает несколько контекстов: "1) обработка данных, выполненная в основном автоматическими средствами; 2) в широком смысле дисциплина,

изучающая методы и технику обработки даны автоматическими средствами; 3) относится к оборудованию для обработки данных, такому, как электрические бухгалтерские машины и электронное оборудование для обработки данных"*(65). Более современные источники определяют автоматическую обработку данных как манипуляцию данными с помощью автоматизированных устройств*(66). В основном большинство источников содержат близкие по смыслу определения ключевого термина в данном словосочетании. Automatic - автоматический, - как правило определяется как процесс или устройство, способные (при заданных условиях) функционировать без вмешательства человека*(67). В этой связи имеются основания полагать, что именно отсутствие вмешательства человека и заданные условия обработки являются основными признаками автоматизации применительно к обработке персональных данных. Необходимо также учитывать, что правовое понятие, введенное Конвенцией Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных (ETS N 108), незначительно отличается от технического толкования термина, а именно "автоматическая обработка" включает следующие операции, если они полностью или частично осуществляются с применением автоматизированных средств: накопление данных, проведение логических и/или арифметических операций с такими данными, их изменение, стирание, восстановление или распространение.

Введенное задолго до эпохи Интернета понятие автоматизации обозначало действия по облегчению труда человека. Изначально автоматизация как явление не создавало угроз в части перехвата юридически значимых действий. Широкое использование термина, по сути, впитало дальнейшую компьютеризацию, интернетизацию и глобализацию. Семантический объем термина "автоматизация" вырос значительно. Это обстоятельство обусловило в современных условиях широкий спектр мнений по данному вопросу, включая следующее: "...на уровне определений достаточно трудно провести четкую линию раздела между автоматизированной и неавтоматизированной обработкой данных"*(68). Действительно, основываясь на имеющихся определениях, нельзя, к примеру, однозначно определить, следует ли рассматривать считывание штрих-кода с квитанции за оплату коммунальных услуг в качестве автоматизированной обработки данных. Другой пример, иллюстрирующий данное положение, можно найти в нормативном правовом акте: п. 2 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства РФ от 15.09.2008 N 687, гласит, что обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

Вместе с тем анализ текста упомянутого Положения позволяет выявить следующие обстоятельства:

классификация видов обработки данных осуществляется на основе применяемых при обработке предметов;

обработка персональных данных, осуществляемая без использования средств автоматизации, характеризуется использованием ручного труда, ручных

пометок и записей в соответствующих документах, бланках, карточках, реестрах, журналы журналах, книгах иных материальные (не электронных) носителях;

применительно к юридическим последствиям классификации не проводится.

Практически полностью цитирует положения п. 2 названного Положения одно из авторитетных экспертных изданий, которое приводит следующий комментарий: "К примеру, если пользователь внес данные в персональный компьютер только для того, чтобы их распечатать, и не сохранял данные на компьютере, то эту обработку можно считать неавтоматизированной"*(69).

Другой аспект этого вопроса - предмет специальной научной дисциплины - защита информации. Ввод информации в память компьютера и распечатка файла представляют собой действия, сопряженные с функционированием процессора - вычислителя, технические параметры которого характеризуются определенной тактовой частотой. Постоянные ввод и распечатка формируют устойчивый автоматизированный канал утечки информации, которая содержит и персональные данные. Радиоизлучение может быть зафиксировано, считано, сохранено и расшифровано, т.е. прочитано специальной техникой, если в компьютере нет специальной защиты. Естественно, такой вариант утечки данных невозможен при рукописном оформлении документа. В описанном варианте невозможно признать обработку персональных данных в форме ввода и распечатки с помощью компьютера, а также с помощью отдельных электронных печатных машин неавтоматизированной обработкой персональных данных. К аналогичному мнению склоняются практические специалисты и авторы публикаций в специализированных изданиях по защите информации. Современные научные исследования и достижения в этом направлении позволяют отслеживать активность пользователей по клавиатурному почерку, распознавать личность по фотографии, а также иные объекты по заданным признакам. Традиционными во многих странах стали камеры слежения за дорожным (автомобильным) трафиком и управление им без постоянного участия, но под контролем человека. Процесс управления в таком случае весьма часто включает фиксацию нарушений, наложение штрафных санкций, рассылку квитанций и т.д.

Вопрос отнесения обработки персональных данных к автоматизированной и неавтоматизированной имеет глубокое практическое значение и требует пристального изучения. Следствием признания обработки персональных данных автоматизированной является обязанность оператора изготовить и сертифицировать программные продукты для их защиты либо приобрести лицензированные продукты, а в случае автоматизированной обработки персональных данных по договору для других лиц - получить лицензию на деятельность по защите информации.

Автоматизированная обработка предполагает участие "автомата" на любой его стадии. В этом смысле невозможно утверждать, что, скажем, компьютер был использован только как устройство для набора текста, а все остальное было ручной обработкой. Подобного рода утверждения весьма часто имеют место в административной практике со стороны операторов и, в отдельных случаях, становятся объектом судебного спора.

До настоящего времени судебная практика не нашла единого подхода к точному и однозначному пониманию автоматизированного процесса обработки данных, общее представление в различных решениях концептуально не отличается. Только конкретные обстоятельства в каждом конкретном случае позволяют принять то или иное решение.

2. Часть 1 комментируемой статьи вводит ограничение на автоматизированную обработку персональных данных с последующим принятием юридически значимого решения. Дословно это ограничение сформулировано как запрет на обработку персональных данных и принятие решения исключительно на их основе. Однако в практической сфере, а именно в отношениях с использованием информационных сетей, принятие решения способом, который часто именуют как "один клик", происходит повсеместно.

Вопрос заключается в том, что многие авторы при рассмотрении фразы "...принятие решений на основании исключительно автоматизированной обработки..." переставляют акцент. В цитированной фразе внимание переключается с "исключительно автоматизированной" обработки на "исключительно автоматизированную" обработку. Юридическая конструкция, которая предполагает ограничение исключительности, но не запрет, ориентирует нас на обдуманное принятия решения, порождающего юридические последствия, на основе автоматизированной обработки, т.е. без участия человека. При смещении акцента в сторону автоматизированной обработки все дальнейшие вопросы рассматриваются в контексте, что есть автоматизированная и что есть ручная обработка.

Одно из решений вопроса опознания автомата предложено в форме теста CAPTCHA [К$^{\acute{а}}$апча, к$^{\acute{а}}$птча]*(70). Выполнение данного теста, повторение (путем ввода в специально предназначенное окно) написанных знаков, весьма затруднительно, практически невыполнимо для автомата. Уровень искажения знаков, вариативность графических и цветовых решений непреодолимо высок для автомата и легко преодолим для человека.

Другим решением является обязательная подпись субъекта персональных данных, которая подтверждает факт принятия волевого решения субъектом, а не автоматом. Поэтому запрет на использование автоматической обработки фактически следует рассматривать не как общее правило, а как исключение из правила, сформулированного в ч. 2 комментируемой статьи. В противном случае придется повсеместно отказываться от автоматизированной обработки данных и переходить на ручную обработку.

3. Часть 2 комментируемой статьи содержит общую норму об обязательном уведомлении субъекта об автоматизированной обработке его персональных данных и возможных последствиях такой обработки. Данное положение размещено в ч. 2 комментируемой статьи, но по смыслу это общее правило комментируемой статьи.

Исходный смысл данной юридической конструкции, по нашему убеждению, заключается в следующем: обработанные автоматизированным способом персональные данные должны быть понятны и, в идеальном варианте, представлены субъекту до принятия решения, которое влечет юридические последствия. Субъект в начале отработки должен быть уведомлен о том, что

обработка будет производиться в автоматическом режиме, что вмешательства человека в процесс не будет производиться. Соответственно, никто не сможет исправить его ошибки (если таковые допущены), и только сам субъект несет ответственность за последствия представления данных (если сведения ошибочные). Предварительное уведомление субъекта имеет цель предупредить о возможном наступлении юридических последствий.

4. Часть 3 комментируемой статьи содержит норму, которая носит процедурный характер, предусматривает обязанность оператора разъяснить субъекту порядок и условия обработки его персональных данных. Комментируемая норма прямо не закрепляет, каким именно документ должен быть. Из смысла статьи можно предполагать наличие определенного, закрепленного документом, порядка. Сложившаяся практика в отдельных отраслях деятельности (образовательной, здравоохранении и других) выработала закрепленные в подзаконных актах формы представления субъектам персональных данных информации о порядке обработки их персональных данных. Как правило, это:

приказ об условиях обработки персональных данных;

положение о порядке обработки персональных данных;

инструкции исполнителей;

другие необходимые документы, бланки, формы.

Весь комплекс документов именуют политикой предприятия (организации) в сфере обработки персональных данных. Оператор обязан информировать субъектов персональных данных об утвержденных документах, закрепляющих политику в сфере обработки персональных данных, гласно, например, разместить их на сайте. Оператор не может ограничиться упоминанием о том, что персональные данные будут обработаны в общем виде. Судебная практика по вопросу, должен ли быть ознакомлен под роспись субъект персональных данных с данным порядком, свидетельствует о том, что должны иметь место и подпись под данной фразой, и специальное место для подписи.

Пример: субъект персональных данных согласился на использование его данных в системе информационно-справочного обслуживания, заполнив и подписав стандартный бланк договора оказания услуг связи. Названная форма не содержит отдельное поле для получения согласия абонента на обработку его персональных данных, что является нарушением. Дальнейшие действия надзорного органа, предписавшего устранить нарушение, признаны законными (см. подробнее постановление Федерального арбитражного суда Северо-Кавказского округа от 03.10.2011 по делу N А63-11458/2010).

Одновременно ч. 3 комментируемой статьи предусматривает право субъекта персональных данных заявить возражение против исключительно автоматизированной обработки его персональных данных. По смыслу данной нормы оператор обязан предусмотреть в бланках, формах соответствующее место или объяснить, каким образом будут учтены и рассмотрены названные возражения субъекта.

5. Часть 4 комментируемой статьи содержит норму процедурного

характера, предусматривающую обязанность оператора предоставить субъекту персональных данных ответ на его возражения в течение тридцати дней. Вероятно, данная норма транслирует традиционные сроки ответов на обращения граждан. Установление данного срока необходимо в связи с тем, что ответственность за административные нарушения может быть реализована в ограниченный двухмесячный срок. Отсутствие широкой судебной практики по данному вопросу ограничивает возможности комментария. Тем не менее в эпоху информатизации установление тридцатидневного срока представляется ошибочным действием. В случаях автоматизированной обработки персональных данных, при наличии всех документов, оператор имеет возможность выдать ответ на возражение в течение рабочего дня. Соответственно, для формального соблюдения всех процедур и ответа достаточно установить срок пять дней. Представляется весьма вероятным, что сроки реагирования на заявление персональных данных будут изменены.

6. Автоматизированная обработка персональных данных проникает во все сферы, в том числе в торговлю и электронную торговлю. Данные вопросы регулирует современное европейское законодательство о защите персональных данных. Одним из таких актов является Резолюция Европейского парламента от 06.07.2011 о комплексном подходе к защите персональных данных в Европейском союзе (2011/2025 (INI)). Основные положения документа, которые имеют отношение к вопросу применения автоматизированной обработки персональных данных, подчеркивают необходимость защиты данных в связи с расширением деятельности, осуществляемой в Интернете; отмечают, что сбор, анализ, обмен и злоупотребления данными и риск профилирования, стимулируемый техническими разработками, достигли беспрецедентных размеров; карты лояльности (клубные карты, дисконтные карты, преимущество карты и т.д.) используются все чаще и чаще, как для онлайн клиентов, так и для граждан вне интернет-магазина. В документе обращено внимание на укрепление существующих принципов и элементов, таких как наличие предварительного и явного согласия; подчеркивается, что согласие должно считаться действительным только тогда, когда имеется однозначное сообщение, свободное, конкретное и четкое; когда имеется адекватный реализованный механизм для фиксации согласия или отзыва согласия пользователя. Европейский Парламент призывает Комиссию четко определить термины профиль и профилирование.

Рассмотренные положения комментируемой статьи и отдельные европейские документы свидетельствуют о сложности, неоднозначности и невозможности окончательного решения вопроса об автоматизированной обработке персональных данных. Необходимо постоянное совершенствование законодательства и знаний по данному вопросу.

Статья 17. Право на обжалование действий или бездействия оператора

1. Комментируемая статья содержит норму права, которая детализирует общее право на защиту, закрепленное ст. 46 Конституции РФ, применительно к отношениям в сфере защиты персональных данных. Часть 1 комментируемой статьи содержит норму, регулирующую право обжалования действий оператора

в уполномоченный орган. Право подачи жалобы в судебном порядке закрепляется как дополнительное (если не работает основное). Комментируемый закон не детализирует понятие жалобы, процедуру обжалования, действия по формированию и предоставлению ответа заявителю и прочие связанные с обжалованием действия, т.к. это предмет специального закона. Понятие жалобы - просьба гражданина о восстановлении или защите его нарушенных прав, свобод или законных интересов либо прав, свобод или законных интересов других лиц, - предусмотрено Федеральным законом от 02.05.2006 N 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации". Лицо, подавшее жалобу, указывает, какие права нарушены и каким субъектом, по возможности подробно описывает все обстоятельства, связанные с нарушением его прав. Подробные сведения необходимы для проведения всесторонней проверки и вынесения объективного решения по существу жалобы. Поскольку норма комментируемой статьи предусматривает обжалование незаконных действий и бездействий оператора, основным содержанием жалобы должно стать описание тех действий, которые заявитель рассматривает как действия (бездействие), нарушающие его права. Кроме того, в жалобе заявитель указывает обратный адрес или адрес для отправки ответа. Это необходимо для направления ответа заявителю (о допустимости анонимного обращения см. п. 4 комментария к настоящей статье).

2. Государственным органом, который уполномоченный осуществлять защиту прав субъектов персональных данных и рассматривать обращения и жалобы субъектов персональных данных, является назначенная Правительством Российской Федерации Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденным постановлением Правительства РФ от 16.03.2009 N 228, установлено, что Роскомнадзор осуществляет государственный контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

Министерством связи и массовых коммуникаций Российской Федерации, которому подведомствен Роскомнадзор, разработан документ, определяющий порядок осуществления функций контроля (надзора), а именно - Административный регламент 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, утвержденный приказом Министерства связи и массовых коммуникаций РФ от 14.11.2011 N 312. Названным документом регламентируются порядок приема и рассмотрения обращений, порядок очередных и внеочередных проверок, условия проведения проверок и другие сопутствующие обстоятельства. По результатам проверки в отношении нарушителя Роскомнадзор информирует о принятых мерах заявителя, а также сообщает о проведенных мероприятиях через официальной сайт. Например, по сообщению на сайте

Роскомнадзора*(71), после проверки и предписания прекратили деятельность два интернет-сайта, незаконно распространявших персональные данные граждан России.

Типичным примером нарушения прав субъектов персональных данных и законных интересов является передача жилищно-коммунальными хозяйствами персональных данных коллекторским агентствам.

Пример: Арбитражный суд Удмуртской Республики рассмотрел дело по жалобе жилищного управления на предписание Роскомнадзора об устранении нарушения установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) в части передачи персональных данных третьим лицам без получения согласия субъекта персональных данных и нарушения требований конфиденциальности при обработке персональных данных. Суд апелляционной инстанции установил, что оспариваемое предписание по результатам проверки заявителя вынесено уполномоченным органом. Требования предписания были основаны на том, что обработка персональных данных могла осуществляться оператором только с согласия субъектов персональных данных. Поскольку субъект согласия на передачу третьему лицу его персональных данных не давал, оператором было допущено нарушение, подлежащее устранению. Суд постановил, что предписание вынесено обосновано. Решением суда в удовлетворении жалобы было отказано в полном объеме (см. постановление Семнадцатого арбитражного апелляционного суда от 15.12.2011 N 17АП-12233/2011-АК по делу N А71-6733/2011).

Не все нарушители доводят ситуацию до судебного разбирательства. Большая часть дел, по данным отчетов Роскомнадзора, завершается устранением нарушения. Судебный порядок рассмотрения дел, предусмотренный ч. 1 комментируемой статьи как альтернативный административному, в ч. 2 комментируемой статьи предусмотрен как основной, единственный.

3. Часть 2 комментируемой статьи содержит норму, содержание которой закрепляет право субъекта персональных данных на защиту именно в судебном порядке как основных прав, так и законных интересов. Кроме того, в комментируемой части подчеркивается право субъекта персональных данных на возмещение убытков и материального вреда.

Для повседневной практики могут представлять определенный интерес разработки конструкции "законный интерес", полученные В.В. Субочевым в ходе подготовки докторской работы по теории права. "Законный интерес - это стремление субъекта пользоваться определенным социальным благом и в некоторых случаях обращаться за защитой к компетентным органам в целях удовлетворения не противоречащих нормам права интересов, которое в определенной степени гарантируется государством в виде юридической дозволенности, отраженной в объективном праве либо вытекающей из его общего смысла"*(72). Руководствуясь данным в рамках теоретического монографического исследования определением, предлагается применительно к

сфере оборота персональных данных рассматривать законные интересы как дозволенность не только представлять персональные данные, но и не представлять их в тех случаях, когда их представление противоречит интересам субъекта персональных данных. Применение категории "законный интерес" возможно также в тех случаях, когда права субъекта персональных данных формально не нарушены, либо когда нарушение не очевидно, либо его сложно доказать, особенно в случае бездействия оператора. Заявителю будет достаточно подтвердить относимость и законность интересов в связи с фактом бездействия.

Участие в судебных процессах в любом качестве не всеми субъектами персональных данных рассматривается как позитивное событие. Соответственно, одним из законных интересов, который тесно связан с правом на приватность частной жизни, является сокращение до нуля в медиасферах сообщений об участии субъектов в судебных процессах. С другой стороны, принцип гласности судебного производства требует раскрытия (обнародования) обстоятельств дела, к числу которых относятся и персональные данные. Как совместить эти встречные требования и устранить возможное противоречие, исследовала М.В. Слаутина. Законные интересы граждан, участвующих в судебных процессах в качестве свидетелей или иных лиц, могут быть нарушены в связи с размещением на сайте суда решений. Несмотря на то что операция с персональными данными - обезличивание - названа автором "деперсонификация", проблема обрисована достаточно точно. "Деперсонификация судебных актов осуществляется бессистемно и непоследовательно, основывается зачастую на субъективных предпочтениях сотрудников судов, отвечающих за эту работу, что приводит к коммуникативным неудачам. Тексты, построенные по нормам официально-делового стиля, и так достаточно трудны для восприятия неспециалиста; а, будучи перегруженными специальными знаками, сокращениями и т.п., становятся практически непонятны при первом прочтении"*(73).

Судебная практика возмещения морального вреда требует длительного периода формирования. В России суды, как правило, удовлетворяют требования о возмещении морального вреда в десятки, а то и сотни раз меньшем размере, чем истец указал в исковом заявлении. Практика возмещения морального вреда в связи с использованием изображения как персональных данных может быть проиллюстрирована решением, которое вынес Бабушкинский районный суд Москвы*(74). Представляется необходимым подчеркнуть, что комментируемая статья закладывает основы специальных прав субъектов персональных данных на возмещение морального вреда. Защита прав субъектов персональных данных на возмещение морального вреда будет осуществляться в рамках гражданского процесса, а норма, закрепляющая это право, содержится не в гражданском, а в специальном законодательстве о персональных данных.

4. Еще один аспект законных прав, который можно рассмотреть на основе практики Европейского суда по правам человека, - это вопрос о балансе между полным раскрытием персональных данных и анонимностью. Вопрос исследован М.В. Слаутиной в рамках лингвистики. Не представилось возможным найти судебных решений, споров по вопросу объема раскрытия персональных данных

заявителем в рамках судебного процесса в отечественной судебной практике. В этой связи предлагается обратиться к отдельным делам из практики Европейского суда по правам человека. В связи с тем, что Россия является участником целого ряда международных договоров в рамках Европейского союза, практика Европейского суда по правам человека в части определения критериев анонимности может представлять определенный интерес.

Пример: решением по одному из дел жалоба была признана анонимной, т.к. в деле не было ни одного документа, позволяющего идентифицировать личность заявителя. Когда ни в формуляре жалобы, ни в приложенных документах фамилия и имя заявителя не упомянуты, а фигурирует только псевдоним, и когда при этом доверенность на представителя подписана буквой "икс", считается, что личность заявителя не раскрыта*(75).

В других случаях Суд не считает, что жалоба была анонимной.

Примеры: жалоба была подана с указанием фиктивных имен - речь идет о случае, когда заявители использовали псевдонимы, объясняя это Суду необходимостью в контексте вооруженного конфликта не называть свои настоящие имена в целях защиты своих родственников и близких. Учитывая, что за тактикой неразглашения настоящих имен в силу причин, которые можно понять, скрываются конкретные реальные лица, личность которых может быть установлена по достаточному количеству других признаков, нежели имена и фамилии этих лиц, и в силу наличия достаточно тесной связи между заявителями и указанными событиями, Суд не посчитал, что жалоба была анонимной*(76). Не была отклонена за анонимностью жалоба, поданная церковным органом или религиозно-философской ассоциацией, не раскрывшими личности своих членов и участников*(77).

Комментируемая статья не содержит прямого указания на необходимость указания в заявлениях, жалобах определенных реквизитов в связи с защитой прав субъекта персональных данных. Право на защиту законных интересов допускает неполное раскрытие персональных данных (ограниченную анонимность). При дальнейшем развитии информационных технологий и расширении оборота персональных данных представляется прогнозируемым формирование судебной практики в сфере защиты персональных данных по делам с участием ограниченно анонимных субъектов.

Глава 4. Обязанности оператора

Статья 18. Обязанности оператора при сборе персональных данных

1. Европейское и российское законодательство признает персональные данные одним из объектов защиты, входящим в состав прав человека. Интерес к вопросу о соблюдении операторами прав субъектов персональных данных не ослабевает. В сентябре 2012 года в очередной раз к теме сохранности

персональных данных обратился Президент России на встрече с главой Минкомсвязи, которому было поручено "...довести эту работу до конца"*(78). Как было отмечено, "информация, особенно персональные данные населения, - это большая ответственность, в том числе финансовая"*(79). По данным Минкомсвязи России, озвученным на встрече, в стране операторами персональных данных является около 300 тысяч различных юридических лиц. Ведомство планирует максимально ужесточить контроль в этой сфере. Средства массовой информации в данном случае приводят приблизительную численность операторов. Более точные данные можно найти в публичных отчетах Роскомнадзора. Например, в декабре 2008 года, по данным Роскомнадзора было зарегистрировано 33 734 оператора*(80). В 2011 году было зарегистрировано всего 229 912 операторов. В 2011 году было проведено 1440 плановых проверок, в рамках внепланового контроля проведена 791 проверка*(81). На начало марта 2013 г. на учете состояло 269 959 операторов персональных данных*(82).

Специалист Роскомнадзора О.В. Борисенко утверждает, что нужно "контролировать 7 миллионов операторов, а лимит проверок всего 6 тысяч в год"*(83). Вопрос о количестве операторов и необходимом количестве проверок - предмет самостоятельного исследования. В данном случае важно другое - деятельность оператора по обработке персональных данных является важным направлением деятельности и правового регулирования, к которому все государства проявляют повышенный интерес.

В рамках исполнения поручения Президента России Правительство России подготовило документы, которые детализируют обязанности операторов персональных данных. Одним из таких документов является постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". Документом утверждены требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных. Обязанностью оператора является обеспечение безопасности персональных данных при их обработке в информационной системе при помощи системы защиты персональных данных (см. комментарий к ст. 19). В случае исполнения обязанностей оператора персональных данных уполномоченным лицом на основании заключаемого с этим лицом договора документом предусматривается обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

В обязанность оператора также входит выбор средств защиты информации для системы защиты персональных данных, анализ угроз, их классификация по 4-м типам и формирование системы защиты соответствующего класса.

Кроме технических мероприятий, оператор обязан выполнить целый ряд организационных мероприятий. В числе названных мероприятий: обучение персонала, который обеспечивает безопасность персональных данных при их обработке; разработка организационно-распорядительных документов, предусмотренных как положениями комментируемого закона, так и иными подзаконными актами; уведомление органов Роскомнадзора (см. комментарий к ст. 18.1).

В качестве примера иных подзаконных актов, которыми предусмотрены обязанности оператора персональных данных, можно привести административные регламенты. Так, например, в соответствии с п. 9 Административного регламента 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, утвержденного приказом Министерства связи и массовых коммуникаций РФ от 14.11.2011 N 312, руководитель или иной уполномоченный представитель оператора обязаны предоставить должностным лицам Роскомнадзора или ее территориального органа возможность ознакомиться с документами, связанными с целями, задачами и предметом выездной проверки, в случае если выездной проверке не предшествовало проведение документарной проверки, а также обеспечить доступ проводящих выездную проверку должностных лиц Роскомнадзора или ее территориального органа на территорию, в используемые оператором при осуществлении обработки персональных данных здания, строения, сооружения, помещения, к используемому оператором оборудованию.

Процитированный административный регламент утвержден приказом, который зарегистрирован в Минюсте РФ 13 декабря 2011 г. под N 22595. Это позволяет относить сам приказ и административный регламент к категории нормативно-правовых актов, т.е. документов, обязательных для исполнения не только подведомственными министерству субъектами, но и всеми субъектами, осуществляющими обработку персональных данных. Кроме того, весьма неожиданно для операторов в данном документе сформулированы обязанности оператора. Это сделано опосредовано, через предмет контроля и права проверяющего. Рассмотрим юридическую конструкцию предметной сферы государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных. В п. 5 названного административного регламента без прямого указания на обязанности оператора обозначены виды деятельности и материальные объекты, наличие которых для оператора персональных данных является обязательным, а именно: документы, характер информации в которых предполагает или допускает включение в них персональных данных; информационные системы персональных данных; деятельность по обработке персональных данных. Тот факт, что деятельность по обработке персональных данных является предметом государственного контроля (надзора), обязывает осуществлять этот вид деятельности. Документы, характер информации в которых предполагает или допускает включение в них персональных данных, обозначены и как предмет государственного контроля (надзора) (в п. 5 административного регламента), и как составная часть обязанностей оператора (в п. 9 административного регламента). Обязанность же по ведению информационной системы персональных данных (предусмотрена в п. 5 административного регламента) возникает только в том случае, если оператор осуществляет автоматизированную обработку персональных данных. В конструкции комментируемой нормы о предмете контроля (надзора) с

вытекающими отдельными обязанностями операторов нет очевидного противоречия. Однако операторам необходимо проявлять максимум внимания не только к положениям закона, в которых конкретно предусмотрены их обязанности, но и к тем положениям подзаконных актов, которыми предусматриваются права контролирующих (надзорных) органов. Такой подход позволит своевременно принять необходимые меры по организации соответствующей поднадзорной деятельности, выявить противоречия законодательства или подзаконных актов (что принципиально не исключается), а также избежать потенциальных конфликтов или нарушений законодательства во время проверок.

Для решения вопроса о своевременности контроля операторам рекомендуется использовать справочные сервисы консалтинговых компаний, которые информируют о предстоящих мероприятиях и о вступлении в силу отдельных положений законодательства и нормативных актов в формате календаря.

2. В ч. 1 комментируемой статьи предусмотрена обязанность оператора предоставить субъекту персональных данных по его просьбе следующую информацию:

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 комментируемым 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 комментируемым законом или другими федеральными законами.

Часть первая комментируемой статьи содержит основную, общую норму (общее правило), обязывающую ознакомить субъекта персональных данных с порядком и условиями обработки его персональных данных конкретным оператором. Как правило, операторы, которые стремятся минимизировать возможные риски, связанные с ненадлежащим исполнением наемным персоналом своих обязанностей, размещают подробную информацию на

официальных сайтах. Данное обстоятельство сокращает процесс ознакомления субъекта с целями и условиями обработки его персональных данных. Последующие части комментируемой статьи содержат отдельные исключения из общего правила. Отмеченное обстоятельство не исключает обязанности оператора ответить на запрос субъекта о предоставлении данных.

3. В ч. 2 комментируемой статьи предусмотрена обязанность оператора разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, если предоставление персональных данных является обязательным в соответствии с федеральным законом. Поскольку обязанностью оператора является декларирование целей и порядка обработки персональных данных, норма, содержащаяся в данной части комментируемой статьи, призвана урегулировать порядок дачи разъяснения субъекту персональных данных. В тех случаях, когда от факта отсутствия персональных данных зависит принятие решения о выполнении в отношении субъекта персональных данных каких либо юридически значимых действий, это лицо должно быть уведомлено надлежащим образом. Например, процедуры идентификации личности предусмотрены при прохождении на борт воздушного судна, в меньшей степени - в вагоны поездов дальнего следования, в отдельных регионах - в междугородные автобусы дальнего следования (межрегионального сообщения). Процедура идентификации предусмотрена при получения виз в большинство стран мира, где предусмотрен визовый режим, при пересечении границ государств, границ отдельных территорий и отдельных предприятий. Процедура идентификации предусмотрена также при посещении иных режимных территорий и объектов, порядок и процедура идентификации на которых предусмотрен законодательством.

В названных случаях оператор обязан уведомить субъекта о необходимости получения персональных данных и о последствиях отказа для субъекта предоставить свои персональные данные. Представляется, что во всех случаях данная процедура должна быть формализована, проводиться до момента наступления возможных последствий, временной промежуток между уведомлением субъекта и последствиями должен содержать время, необходимое для принятия субъектом решение, а возможно, и для дополнительной консультации со специалистом, которому субъект доверяет.

4. Часть 3 комментируемой статьи содержит норму, которая предусматривает возможность обработки персональных данных, полученных не от субъекта персональных данных. Следует учитывать, что в условиях формирования информационного общества совокупный объем данных, содержащихся в информационных системах, постоянно увеличивается по мере активности субъекта. Покупки билетов на транспорте, кредитные программы, поиск работы и связанные с этим поиском резюме и собеседования, - все это накапливается и в условиях нормального электронного документооборота в определенный момент может облегчить субъекту представление необходимых сведений. Планируемое введение с 2014 года локализации в одном документе (универсальной электронной карте) всех данных, необходимых в повседневной жизни, также способствует этой тенденции. Соответственно, субъекта персональных данных не должно удивлять и тем более шокировать, что

необходимые данные уже представлены по месту его обращения. Это должно свести к нулю количество необоснованных требований о наличии какой-либо справки. При всем удобстве использования данных информационных систем, оператор тем не менее обязан соблюдать определенные условия, а именно: сообщить субъекту персональных данных сведения об операторе, его представителе (фамилия, имя, отчество и адрес оператора/представителя). Нормой сложившейся практики следует принять наличие у обслуживающего офисного персонала оператора (крупных телекоммуникационных, транспортных, торговых компаний) специальных информационных знаков (так называемых бэйджей) с указанием логотипа компании, фамилии, имени лица, его должности, весьма часто - с его фотографией.

Кроме того, оператор обязан информировать субъекта о цели обработки персональных данных и правовом основании обработки персональных данных. Весьма часто это следует из обстановки (контакты с правоохранительными органами, проверка при посадке на транспортные средства). Однако этого бывает недостаточно, и вполне возможно, что операторы должны проводить специальные занятия, курсы подготовки, семинары с персоналом для выработки четкого навыка по информированию субъектов персональных данных о том, кто и какие сведения в конкретный момент от субъекта получает, каковы цель обработки, время хранения, дальнейшие действия. Предполагаемые пользователи персональных данных и права субъекта персональных данных, если это не следует из обстановки, должны быть представлены субъекту или, по возможности, размещены в доступных для субъекта персональных данных местах (кассовые залы, справочные, официальные сайты, обратная сторона печатной продукции, периодические объявления). Источник получения персональных данных - специфичная категория, сведения о которой должны предъявляться субъекту персональных данных по запросу.

5. Часть 4 комментируемой статьи предусматривает право оператора не выполнять обязанность по информированию субъекта персональных данных в нескольких специально оговоренных случаях.

Субъект персональных данных, будучи уведомленным о том, что осуществляется обработка его персональных данных, может вступить во взаимоотношения с иным оператором, который имеет право не уведомлять его об обработке персональных данных дополнительно. Аналогичной представляется ситуация, когда субъект обращается в филиал или другой офис оператора. Близким по содержанию правоотношений является случай получения персональных данных в связи с исполнением оператором федерального закона или договора, стороной в котором является субъект персональных данных. Единственным дополнением в данном случае будет указание на необходимость специального уведомления. В тексте договора (на бланке типовой формы) должна быть специально отведенная графа, поскольку общей подписи под текстом договора будет недостаточно (см. подробнее постановление Федерального арбитражного суда Северо-Кавказского округа от 03.10.2011 по делу N А63-11458/2010).

Пункт 3 ч. 4 комментируемой статьи предусматривает ситуацию, которая для многих пользователей информационными сетями является неочевидной.

Дело в том, что многие пользователи не контролируют информационные потоки, которые возникают в процессе их активности в разного рода информационных сетях (социальные сети, чаты, форумы, Интернет-телефония, Интернет-пэйджинг). Однако определено, что не требуется специального уведомления, если персональные данные субъекта получены из общедоступного источника.

Пункт 4 ч. 4 комментируемой статьи предусматривает право оператора не выполнять обязанность по информированию субъекта персональных данных в случае обработки 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.

Оператор не информирует субъекта персональных данных также в том случае, когда это информирование связано с нарушением прав и законных интересов третьих лиц, например, в соответствии с законодательством о средствах массовой информации.

Как отмечается в тексте ч. 3 комментируемой статьи, ч. 4 комментируемой статьи является исключением из общего правила об обязанности оператора предоставить субъекту персональных данных сведения об источниках получения сведений о субъекте персональных данных.

6. Органы государственной власти и местного самоуправления составляют значительную, если не преобладающую, часть от всех операторов, осуществляющих обработку персональных данных. Законодатель не выделяет эту категорию операторов специально и не предусматривает специальную норму в комментируемой статье закона. Вместе с тем законодательство в Российской Федерации состоит как из законов, так и из подзаконных нормативных актов (указов Президента России; постановлений Правительства России; приказов министерств, служб, агентств, зарегистрированных и опубликованных в установленном порядке). К числу соответствующих критерию относимости к данному вопросу документов следует причислить постановление Правительства РФ от 21.03.2012 N 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". Правительство устанавливает для государственных или муниципальных органов, которые являются операторами персональных данных, целый перечень специальных требований, например:

наличие назначенного ответственного за организацию обработки персональных данных;

наличие утвержденных документов (правила обработки персональных данных, сроки их обработки и хранения, порядок уничтожения, правила рассмотрения запросов субъектов персональных данных или их представителей, правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства, правила работы с

обезличенными данными, перечень информационных систем персональных данных, перечни персональных данных (отдельно по трудовым отношениям и по государственным, муниципальным контрактам), перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, должностные инструкции, типовые обязательства и форма согласия на обработку персональных данных, порядок доступа в помещения для обработки персональных данных и другие);

применение правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке;

проведение периодических проверок условий обработки персональных данных;

ознакомление служащих государственного или муниципального органа, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных и (или) организация обучения указанных служащих и др.

Установление Правительством России определенного набора правил для государственных и муниципальных органов может представлять собой положительный пример для организации работ с персональными данными в организациях, которые относятся к негосударственному сектору. Кроме экономии собственных средств на разработку положений и правил, это позволит унифицировать мероприятия и процедуры по защите персональных данных в различных секторах, облегчит обучение персонала, который переходит из госсектора в негосударственную экономику и обратно, и т.д.

7. Другим ресурсом накопления персональных данных в особом специальном контексте (история болезни) является сфера оказания медицинских услуг. Практически каждый субъект с момента рождения становится источником для формирования особой базы персональных данных. Специфичным в данном случае является как сам объект хранения - персональные данные в медицинской книжке (истории болезни), - так и оператор, его представители, потребители и иные субъекты. Представитель медицинского научного сообщества Р.С. Рыжов, отмечая необходимость урегулирования именно на уровне федерального закона медицинских услуг через телекоммуникации, отмечает целый ряд особенностей. Для размещения деперсонифицированной информации о трудных для диагностики и лечения случаях в целях получения рекомендаций от профильных специалистов он предлагает использовать веб-серверы клинических учреждений. К правовым аспектам телемедицинских технологий он относит решение вопросов ответственности медицинского и технического персонала. Ключевые моменты, отмеченные автором, - это организация и проведение телеконсультаций, включая:

оказание телемедицинской помощи, информированное согласие, ответственность консультанта;

предоставление сведений о состоянии больного и трактовка лечащим

врачом полученных рекомендаций;

аутентичность обсуждаемых документов;

конфиденциальность телеконсультации и последующая защита персональных данных пациентов.

Из внесенных в Государственную Думу альтернативных законопроектов: "Об электронной медицине" и "Об информационно-коммуникационных технологиях в медицине" автор более высоко оценивает последний. Критерием, по его мнению, является более высокий уровень проработанности отношений и наличие достаточно четких понятий таких категорий, как телемедицина, телемедицинские технологии и др.*(84) Вероятно, следует согласиться с необходимостью детальной регламентации на уровне специального закона вопросов защиты персональных данных в сфере оказания медицинских услуг, и в частности защиты персональных данных в телемедицине.

8. Исполнение оператором своих обязанностей по защите персональных данных не допускает их разглашения третьим лицам по законным основаниям, предусмотренным иными законами, но не предусмотренным комментируемым законом.

Пример: адвокат обратился в суд с заявлением об оспаривании действий оператора персональных данных за отказ предоставить адресные данные на гражданина, который являлся ответчиком по иску. Дело было истребовано и рассмотрено Верховным Судом Российской Федерации. Суд признал правомерность действий оператора, подтвердив, что адресная справка является персональными данными с ограниченным доступом. Суд также признал правомерность деятельности адвоката по защите интересов клиента и его права обращаться с различными запросами. Далее Суд пояснил, что право адвоката обращаться с запросом сведений не распространяется на персональные данные. Доступ к персональным данным без согласия субъекта имеет ограниченный перечень субъектов, к которым адвокат не относится. Отказ оператора был признан правомерным. Заявление адвоката не было удовлетворено (см. определение Верховного Суда Российской Федерации от 12.05.2010 по делу N 49-В10-5).

Таким образом, Суд подтвердил высокий уровень правового режима персональных данных как конфиденциальной информации. Суд также подтвердил, что конфиденциальность может быть нарушена только в специальных случаях, предусмотренных комментируемым законом. Права субъектов на запрос персональных данных могут быть реализованы только в том случае, если их право предусмотрено комментируемым законом. Обработка персональных данных без согласия субъекта возможна только в случаях, прямо предусмотренных комментируемым законом.

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

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

отсутствовала в первоначальной редакции комментируемого закона и была введена Федеральным законом от 25.07.2011 N 261-ФЗ, который также одновременно внес существенные изменения в ст. 19.

С позиции толкования данная статья является достаточно проблематичной ввиду наличия в ее положениях избыточного количества бланкетных и тавтологических оборотов.

В части первой комментируемой статьи сформулировано требование к оператору обработки персональных данных о принятии необходимых и достаточных мер по исполнению обязанностей, возложенных на него комментируемым законом и его подзаконной нормативной базой. При этом отмечается, что состав и перечень мер определяются оператором самостоятельно, за исключением прямого указания в федеральных законах и иных нормативных актах.

Далее приводится перечень мер, не являющийся исчерпывающим:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных. Порядок реализации данной меры определен положениями ст. 22.1 комментируемого закона;

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.

К таковым возможно отнести:

правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;

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;

перечень информационных систем персональных данных;

перечни персональных данных, обрабатываемых оператором в процессе осуществления своей деятельности, в том числе в связи с реализацией трудовых отношений;

перечень должностей работников оператора, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

должностная инструкция ответственного за организацию обработки

персональных данных в операторе;

типовое обязательство работника оператора, непосредственно осуществляющего обработку персональных данных, о недопущении неправомерных действий с персональными данными, включающее предупреждение об ответственности за нарушение требований законодательства в сфере обработки персональных данных.

типовое обязательство работника оператора, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением трудовых обязанностей;

типовая форма согласия на обработку персональных данных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

порядок доступа работников оператора в помещения, в которых ведется обработка персональных данных;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со ст. 19 комментируемого закона;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных комментируемому 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 комментируемого закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных комментируемым 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.

Результаты ознакомления работников оператора целесообразно оформить в письменной форме (лист ознакомления).

2. Часть вторая ст. 18.1 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 варианта обеспечения неограниченного доступа к указанным сведениям является соответствующий информационный стенд.

Кроме того, 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 информационно-телекоммуникационной сети.

3. Часть 3 рассматриваемой статьи определяет особенности мер, направленных на обеспечение выполнения обязанностей, предусмотренных комментируемым законом в отношении операторов, являющихся государственными или муниципальными органами. В частности, она указывает, что Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных комментируемым законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

В настоящее время указанный перечень утвержден постановлением Правительства РФ от 21.03.2012 N 211, в соответствии с положениями которого операторы, являющиеся государственными или муниципальными органами, принимают следующие меры, направленные на обеспечение выполнения обязанностей, предусмотренных комментируемым законом и принятыми в соответствии с ним нормативными правовыми актами:

а) назначают ответственного за организацию обработки персональных данных в государственном или муниципальном органе из числа служащих данного органа;

б) утверждают актом руководителя государственного или муниципального органа ряд необходимых документов, в частности:

правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;

правила рассмотрения запросов субъектов персональных данных или их представителей;

правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

правила работы с обезличенными данными;

перечень информационных систем персональных данных;

перечни персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией 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, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;

перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки

персональных данных либо осуществление доступа к персональным данным;

в) при эксплуатации информационных систем персональных данных, в случае если государственный или муниципальный орган является оператором таких информационных систем, принимают правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке, предусмотренные соответствующими нормативными правовыми актами, для выполнения установленных Правительством Российской Федерации требований к защите персональных данных при их обработке, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

г) при обработке персональных данных, осуществляемой без использования средств автоматизации, выполняют требования, установленные постановлением Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

д) в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организуют проведение периодических проверок условий обработки персональных данных в государственном или муниципальном органе. Проверки осуществляются ответственным за организацию обработки персональных данных в государственном или муниципальном органе либо комиссией, образуемой руководителем государственного или муниципального органа. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю государственного или муниципального органа докладывает ответственный за организацию обработки персональных данных в государственном или муниципальном органе либо председатель комиссии;

е) осуществляют ознакомление служащих государственного или муниципального органа, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных и (или) организуют обучение указанных служащих;

ж) уведомляют уполномоченный орган по защите прав субъектов персональных данных об обработке (намерении осуществлять обработку) персональных данных, за исключением случаев, установленных комментируемым законом;

з) согласно требованиям и методам, установленным уполномоченным органом по защите прав субъектов персональных данных, осуществляют обезличивание персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ.

4. Часть 4 ст. 18.1 обязывает оператора обработки по запросу уполномоченного органа по защите прав субъектов персональных данных представить документы и локальные акты, указанные в ч. 1 комментируемой статьи, и (или) иным образом подтвердить принятие определенных в ней мер.

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

1. Рассматривая ст. 19 комментируемого закона, следует отметить, что Федеральным законом от 25.07.2011 N 261-ФЗ была введена в действие ее новая редакция, содержание которой существенно отличается от предыдущей версии.

Основным подзаконным нормативным правовым актом, принятым в развитие положений предыдущей редакции ст. 19, являлось постановление Правительства РФ от 17.11.2007 N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных".

В соответствии с требованиями указанного нормативного правового акта были утверждены следующие нормативные правовые акты и методические документы:

приказ ФСТЭК РФ, ФСБ РФ, Мининформсвязи РФ от 13.02.2008 N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных";

приказ ФСТЭК РФ от 05.02.2010 N 58 "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных";

Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утв. ФСБ РФ 21.02.2008 N 149/54-144).

Однако в соответствии с положениями актуальной редакции ст. 19 было издано постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", в соответствии с которым постановление Правительства РФ от 17.11.2007 N 781 утратило силу. В связи с этим в настоящее время неопределенным представляется статус вышеуказанных подзаконных нормативных правовых актов и методических рекомендаций в сфере защиты персональных данных, принятых в соответствии с постановлением Правительства РФ от 17.11.2007 N 781, которые формально не утратили силу, однако не соответствуют актуальной редакции ст. 19, положениям постановления Правительства РФ от 01.11.2012 N 1119 и требуют значительных корректировок.

В новой редакции ст. 19 появились дефиниции, которые необходимо учитывать при ее толковании, а именно: угрозы безопасности персональных данных, уровень защищенности персональных данных.

2. Часть первая рассматриваемой статьи устанавливает обязанность оператора принимать необходимые 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, а именно:

- правовые;

- организационные;
- технические, -

или обеспечивать принятие таких мер.

В предыдущей редакции статьи речь шла только об организационных и технических мерах. Помимо этого, не предусматривался такой вариант действий оператора, как "обеспечение принятия мер", в данном контексте подразумевается возможность осуществления обработки персональных данных по поручению оператора другим лицом на основании договора. Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

3. Часть вторая ст. 19 определяет компоненты обеспечения безопасности персональных данных, перечень которых не является исчерпывающим:

1) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Дефиниция угрозы безопасности персональных данных приводится в ч. 11 комментируемой 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.

Кроме того, ч. 5-7 рассматриваемой статьи определяют необходимость формулирования в положениях нормативных правовых актов угроз безопасности персональных данных, актуальных 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.

Субъектами правотворчества в данном случае являются:

федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности (федеральные министерства);

органы государственной власти субъектов Российской Федерации;

Банк России;

органы государственных внебюджетных фондов;

иные государственные органы в пределах своих полномочий.

Например, Министерство транспорта Российской Федерации в своих приказах формулирует угрозы безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении перевозок пассажиров.

Помимо этого, 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.

Проекты вышеотмеченных 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;

2) применение 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.

Под уровнем защищенности персональных данных в соответствии с п. 11 рассматриваемой статьи понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

3) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

Отношения, возникающие при оценке соответствия, регулируются Федеральным законом от 27.12.2002 N 184-ФЗ "О техническом регулировании". Под оценкой соответствия подразумевается прямое или косвенное определение соблюдения требований, предъявляемых к объекту;

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

5) учет машинных носителей персональных данных;

6) обнаружение фактов несанкционированного доступа к персональным данным и принятие соответствующих мер по его обнаружению и пресечению;

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

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

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

Так, в соответствии с п. 17 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утв. постановлением Правительства РФ от 01.11.2012 N 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. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

Порядок лицензирования деятельности по технической защите конфиденциальной информации (не содержащей сведения, составляющие государственную тайну, но защищаемой в соответствии с законодательством Российской Федерации), осуществляемой юридическими лицами и индивидуальными предпринимателями, определен Положением о лицензировании деятельности по технической защите конфиденциальной информации, утв. постановлением Правительства РФ от 03.02.2012 N 79 "О лицензировании деятельности по технической защите конфиденциальной информации".

4. Часть третья комментируемой статьи определяет, что 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.

Указанные угрозы определены и систематизированы п. 6 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утв. постановлением Правительства РФ от 01.11.2012 N 1119:

угрозы 1-го типа актуальны для информационной системы, если для нее, в том числе, актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе;

угрозы 2-го типа актуальны для информационной системы, если для нее, в том числе, актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе;

угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе;

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

Пунктами 8-12 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утв. постановлением Правительства РФ от 01.11.2012 N 1119, определены 4 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:

а) 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;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 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:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) 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 100 000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 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:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) 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 100 000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) 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 100 000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100 000 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:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) 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 100 000 субъектов персональных данных, не являющихся сотрудниками оператора.

Пункты 12-13 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утв. постановлением Правительства РФ от 01.11.2012 N 1119, определяют требования, необходимые для обеспечения защищенности персональных данных при их обработке в информационных системах согласно соответствующим уровням;

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

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 N 512.

Пунктом 4 данного документа определено, что материальный носитель должен обеспечивать:

а) защиту от несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных;

б) возможность доступа к записанным на материальный носитель биометрическим персональным данным, осуществляемого оператором и лицами, уполномоченными в соответствии с законодательством Российской Федерации на работу с биометрическими персональными данными;

в) возможность идентификации информационной системы персональных данных, в которую была осуществлена запись биометрических персональных данных, а также оператора, осуществившего такую запись;

г) невозможность несанкционированного доступа к биометрическим

персональным данным, содержащимся на материальном носителе.

Кроме того, в случае если на материальном носителе содержится дополнительная информация, имеющая отношение к записанным биометрическим персональным данным, то такая информация должна быть подписана усиленной квалифицированной электронной подписью и (или) защищена иными информационными технологиями, позволяющими сохранить целостность и неизменность информации, записанной на материальный носитель.

5. Часть пятая статьи 19 подразумевает, что состав и содержание организационных и технических мер, необходимых для выполнения требований, установленных Правительством Российской Федерации в соответствии с рассмотренной выше ч. 3 комментируемой статьи, устанавливаются в пределах полномочий соответствующими приказами:

1) федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности;

2) федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

Часть восьмая 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 вышеуказанные органы в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных. Решением Правительства Российской Федерации контрольно-надзорные полномочия указанных органов могут быть с учетом значимости и содержания обрабатываемых персональных данных применены к не являющимся государственными информационным системам, эксплуатируемым при осуществлении определенных видов деятельности.

Согласно положениям Федерального закона от 03.04.1995 N 40-ФЗ, п. 1 Положения о Федеральной службе безопасности Российской Федерации, утв. Указом Президента РФ от 11.08.2003 N 960, федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, является Федеральная служба безопасности Российской Федерации (ФСБ России).

Пункт 1 Положения о Федеральной службе по техническому и экспортному контролю, утв. Указом Президента РФ от 16.08.2004 N 1085, определяет федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, Федеральную службу по техническому и экспортному контролю (ФСТЭК России).

Что касается вопроса разграничения компетенции применительно обеспечения безопасности персональных данных, то следует отметить, что к ведению ФСТЭК России относятся вопросы обеспечения защиты персональных данных некриптографическими методами (предотвращения их утечки по техническим каналам, несанкционированного доступа к ним, специальных воздействий на носители персональных данных в целях их добывания,

уничтожения, искажения и блокирования), ФСБ России осуществляет регулирование в области разработки, производства, реализации, эксплуатации шифровальных (криптографических) средств и защищенных с использованием шифровальных средств информационных систем персональных данных.

6. Часть десятая ст. 19 определяет общее положение о том, что 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.

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

1. Комментируемая статья корреспондирует ст. 14 комментируемого закона, определяющей право субъекта персональных данных на доступ к его персональным данным. Статья 14 определяет общие правила обращения к оператору либо подачи запроса, в том числе имеющего вид электронного документа, его содержание, а также перечень сведений, которые должны быть предоставлены субъекту персональных данных или его представителю при обращении или по запросу, (см. комментарий к ст. 14). Комментируемая статья, в свою очередь, определяет общие обязанности оператора, связанные с получением такого обращения либо запроса, принятием решения о предоставлении персональных данных и последующими действиями, сроки их исполнения.

Первая часть статьи посвящена обязанностям оператора, возникающим у него в момент обращения субъекта персональных данных или его представителя либо получения от них запроса. Она обеспечивает реализацию субъектом персональных данных права на получение сведений о его персональных данных, находящихся у оператора. В этих целях устанавливается, что оператор обязан:

сообщить информацию о наличии персональных данных в отношении субъекта персональных данных, обратившегося к оператору лично или через представителя;

предоставить 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.

Сроки выполнения названной обязанности оператора зависят от формы обращения субъекта персональных данных либо его представителя:

при обращении субъекта персональных данных или его представителя - непосредственно при обращении;

при направлении запроса - в течение тридцати дней с даты его получения.

Обратим внимание на то, что названный срок в тридцать дней был установлен Федеральным законом от 25.07.2011 N 261-ФЗ, ранее редакция комментируемой статьи говорила о десяти рабочих днях. Таким образом, срок предоставления информации о наличии персональных данных и возможности ознакомления с ними был значительно увеличен. Представляется, что в случае направления запроса в форме электронного документа логично было бы установить сокращенный срок, поскольку организационные затраты в случае рассмотрения такого запроса сведены к минимуму.

2. Часть 2 комментируемой статьи посвящена обязанностям оператора, возникающим у него при принятии решения об отказе в предоставлении информации о наличии персональных данных. Оператор может принять решение о таком отказе в случае ограничения права субъекта персональных данных на доступ к его персональным данным в соответствии с федеральными законами (ч. 8 ст. 14 комментируемого закона). В частности, такие ограничения действуют в случае, когда:

обработка персональных данных осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

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

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 комментируемая статья закрепляет за ним обязанность направить субъекту персональных данных (его представителю) мотивированный ответ. В нем должны содержаться основания для такого отказа в виде ссылки на соответствующие положения федерального закона. Срок для направления такого ответа составляет тридцать дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. В предыдущей редакции закона данный срок составлял семь рабочих дней.

Кроме того, субъекту персональных данных может быть отказано в получении доступа к ним в случае повторного обращения к оператору или направления повторного запроса с нарушением предусмотренных комментируемым законом требований (ч. 6 ст. 14 комментируемого закона), например, в течение тридцати дней после первоначального обращения или направления первоначального запроса. В данном случае комментируемый закон также предусматривает обязанность оператора мотивировать такой отказ и представить доказательства обоснованности отказа в выполнении повторного запроса. Предусматривающие это нормы содержатся непосредственно в ст. 14 комментируемого закона.

3. Часть 3 комментируемой статьи регулирует обязанности оператора, связанные с предоставлением субъекту персональных данных (его

представителю) возможности ознакомления с персональными данными и возможными последствиями реализации субъектом своего права требовать от оператора уточнения либо уничтожения своих персональных данных.

Возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных, предоставляется субъекту персональных данных или его представителю безвозмездно. Следовательно, незаконным будет требование о внесении оператору какой-либо платы за организацию доступа лица к его персональным данным.

Пример: суд, применяя норму, содержащуюся в комментируемой статье, указал, что выдачу населению справок о составе семьи и выписок из домовой книги (в том числе и при наличии у граждан задолженности по оплате жилищно-коммунальных услуг) за плату следует расценивать как ограничение права субъекта персональных данных на доступ к своим персональным данным, а следовательно как ограничение конституционного права граждан на информацию. Введение ограничения на доступ граждан к своим персональным данным посредством установления платы за их получение нарушает права неопределенного круга лиц на получение информации. Данная информация не является информацией, распространение которой в Российской Федерации ограничивается или запрещается. Следовательно, заинтересованные лица вправе свободно получать такую информацию (см. кассационное определение Нижегородского областного суда от 09.08.2011 по делу N 33-8160/2011).

Общее 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 предусмотрено ч. 1 ст. 14 комментируемого закона. Настоящая статья конкретизирует данное положение следующим образом:

в случае если персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения;

в случае если персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные.

Из этого можно сделать вывод о том, что субъект персональных данных не может требовать от оператора уничтожения его персональных данных, если они являются неактуальными, но при этом находятся у оператора на законном основании и необходимы для заявленной цели обработки.

Обязанность осуществить названные действия возникает у оператора в течение семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих данные факты.

Обратим внимание на то, что законодатель говорит о необходимости предоставления субъектом персональных данных (его представителем) сведений, подтверждающих действительность фактов, на которые он указывает. Данные сведения должны быть достоверными. Таким образом, обращение к оператору по указанным основаниям не будет являться безусловным

основанием к изменению или уничтожению персональных данных. В течение указанного семидневного срока оператором будет проводиться проверка обозначенных фактов и подтверждающих их сведений. В случае вынесения решения об отсутствии указанных фактов и (или) недостоверности (отсутствии) подтверждающих их сведений обратившемуся субъекту персональных данных (его представителю) может быть отказано в изменении либо уничтожении персональных данных. Также отказ может быть связан с тем, что субъект обращается к оператору по поводу персональных данных другого лица, представителем которого указанный субъект не является (за исключением уполномоченного органа по защите прав субъектов персональных данных).

С внесением в персональные данные необходимых изменений либо их уничтожением предусмотренные комментируемой статьей обязанности оператора не прекращаются. После совершения указанных действий оператор должен:

1) уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах;

2) принять разумные меры по уведомлению третьих лиц, которым персональные данные этого субъекта были переданы. Это связано с необходимостью обеспечить использование актуальных персональных данных о субъекте в целях, для которых осуществляется обработка таких персональных данных.

Подробнее об обязанностях оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных см. комментарий к ст. 21.

4. Часть 4 комментируемой статьи связана с реализацией субъектом персональных данных права на защиту своих персональных данных, которое может быть выражено в обращении в уполномоченный орган по защите прав субъектов персональных данных, а также реализацией указанным органом правомочия запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию.

Государственным органом, который уполномоченный осуществлять защиту прав субъектов персональных данных, является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). На Роскомнадзор возложены функции по обеспечению контроля и надзора за соответствием обработки персональных данных требованиям комментируемого закона.

В случае направления Роскомнадзором запроса о предоставлении данных оператор обязан сообщить необходимую информацию в течение тридцати дней с даты получения запроса (данный срок также был увеличен с семи рабочих дней с начала 2011 года).

Неисполнение обязанности по предоставлению органам Роскомнадзора требуемой информации в установленный срок является административным правонарушением и влечет соответствующую ответственность.

Пример: государственным инспектором РФ по надзору в сфере связи, информационных технологий и массовых коммуникаций Управления Роскомнадзора по РБ в отношении ООО "Стройэксплуатация" по результатам проведения мероприятий по контролю за выполнением операторами персональных данных требований законодательства в области обработки персональных данных было обнаружено нарушение ч. 4 ст. 20 комментируемого закона. Общество своевременно не предоставило уполномоченному органу по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления им деятельности. ООО "Стройэксплуатация" обязано было предоставить сведения об осуществляемых мерах по обеспечению безопасности персональных данных; сведения о предоставлении сторонним организациям (третьим лицам) персональных данных. Получение обществом направленного ему запроса подтверждалось с помощью уведомления о вручении, позволяющего определить срок для направления ответа. В тридцатидневный срок ответ на запрос не был представлен. Согласно ст. 19.7 КоАП РФ непредставление или несвоевременное представление в государственный орган (должностному лицу) сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, а равно представление в государственный орган (должностному лицу) таких сведений (информации) в неполном объеме или в искаженном виде влечет предупреждение или наложение административного штрафа. Постановлением мирового судьи общество было привлечено к административной ответственности за совершение административного правонарушения, предусмотренного ст. 19.7 КоАП РФ, подвергнуто административному наказанию в виде штрафа (см. решение Советского районного суда г. Уфы (Республика Башкортостан) от 03.05.2012).

В целях реализации своих полномочий Роскомнадзор может не только запрашивать и безвозмездно получать информацию, необходимую для реализации своих полномочий, но и требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных. Сроки выполнения оператором таких действий комментируемая статья не устанавливает, однако они определяются согласно ст. 21 комментируемого закона (см. комментарий к указанной статье).

В силу ч. 1 ст. 22 комментируемого закона оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных (случаи, когда оператор вправе осуществлять обработку персональных данных без направления в уполномоченный орган соответствующего уведомления, предусмотрены ч. 2 данной статьи). На практике возникали спорные ситуации относительно обязанности оператора сообщать необходимую информацию по запросу Роскомнадзора после направления уведомления об обработке персональных данных.

Пример: разрешая спор между ООО "Аст-Системс" и Управлением

Роскомнадзора по Астраханской области, арбитражный суд указал, что то обстоятельство, по которому согласно ч. 1 ст. 22 комментируемого закона соответствующее уведомление направляется в уполномоченный орган до начала обработки персональных данных, не исключает реализацию Управлением Роскомнадзора полномочий, прямо предусмотренных ч. 4 ст. 20 комментируемого закона, выраженных в запросе у оператора связи, после начала обработки персональных данных, необходимых сведений для осуществления деятельности соответствующего органа по защите прав субъектов персональных данных (см. постановление Двенадцатого арбитражного апелляционного суда N 12АП-4697/11 от 05.08.2011).

Также в комментарии к ч. 4 рассматриваемой статьи хотелось бы обратить внимание на предусмотренную законом обязанность оператора предоставлять запрашиваемую информацию только в органы Роскомнадзора. Ни в комментируемой части, ни в других положениях комментируемого закона не указывается на обязанность оператора предоставлять сведения о персональных данных субъектов по запросам иных органов власти.

Пример: признавая запрос прокурора не соответствующим закону в части требований о предоставлении личных дел сотрудников ГУВД, материалов, необходимость в предоставлении которых возможно возникнет в ходе проверки, а также требований о предоставлении копий документов, без указания в запросах конкретных документов, суд, руководствуясь п. 1 ст. 3, ст. 6, 7 комментируемого закона, п. 5 ст. 14 Федерального закона от 27.05.2003 N 58-ФЗ, ч. 2 ст. 9 Федерального закона от 26.07.2006 N 149-ФЗ, пришел к выводу о том, что предоставление информации о персональных данных субъекта по запросу прокурора федеральным законодательством не предусмотрено (см. определение Верховного Суда РФ от 08.02.2011 N 19-Впр11-3).

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

1. Статья 21 комментируемого закона посвящена обязанностям оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, - в отличие от предыдущей статьи в данном случае не важен источник, от которого оператор получил информацию о наличии указанных фактов (субъект персональных данных, его представитель, уполномоченный орган, собственные наблюдения). В любом случае на оператора возлагаются обязанности по устранению нарушений законодательства, допущенных при обработке персональных данных, блокированию на время рассмотрения вопроса о достоверности поступивших сведений, уточнению, и уничтожению персональных данных. Согласно комментируемой статье основаниями для исполнения какой-либо из этих обязанностей или их комплекса могут быть:

выявление неправомерной обработки персональных данных (ч. 1 и 3

статьи);

выявление неточных персональных данных (ч. 1 и 2 статьи);

достижение цели обработки персональных данных (ч. 4 статьи);

отзыв субъектом персональных данных согласия на обработку его персональных данных (ч. 5 статьи).

2. Часть 1 комментируемой статьи посвящена исполнению оператором персональных данных обязанности по их блокированию. Блокирование информации обеспечивает временную невозможность ее использования, в то же время сама информация остается сохранной (подробнее о блокировании см. ч. 6 комментария к ст. 3).

Такая обязанность оператора может наступить в случае, если:

в обращении субъекта персональных данных или его представителя;

в запросе субъекта персональных данных или его представителя;

в запросе уполномоченного органа по защите прав субъектов персональных данных, -

будет содержаться указание на следующие факты:

неправомерная обработка персональных данных;

неточность персональных данных.

В результате выявления указанных данных оператор обязан осуществить блокирование персональных данных или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора). Данная блокировка должна быть осуществлена непосредственно в момент обращения указанных лиц или получения от них запроса и действовать в течение периода проверки. Сроки проверки поступившей информации определяются с учетом ст. 20 комментируемого закона (см. комментарий к указанной статье), а также ч. 2 и 3 комментируемой статьи.

Блокирование производится исключительно в отношении персональных данных, относящихся к тому субъекту персональных данных, в отношении которого направлены обращение либо запрос. В случае получения информации о том, что обработка персональных данных осуществляется неправомерно, блокирование допускается исключительно в отношении неправомерно обрабатываемых персональных данных данного лица. Из этого следует сделать вывод, что в случае если лицо предоставило согласие на обработку определенных персональных данных (фамилии, имени отчества), но не предоставило согласие в отношении других (номер телефона, изображение), - блокироваться будут не все персональные данные указанного лица, а лишь те, которые обрабатываются без соответствующих оснований.

Кроме того, осуществляемое блокирование не должно нарушать права и законные интересы субъекта персональных данных или третьих лиц, - в ином случае оно не будет производиться.

3. Часть 2 комментируемой статьи продолжает логически ч. 1 и определяет дальнейшие действия оператора в случае получения информации о неточности персональных данных. Если сведения, подтверждающие указанный факт, признаны достоверными или он подтвержден иным образом, оператор 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;

снять блокирование персональных данных, - для данного действия законодатель не предусмотрел конкретный срок, однако представляется, что снятие блокирования должно быть произведено одномоментно с учетом технической возможности.

Уточнение персональных данных производится на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, которые, как представляется, могут быть запрошены оператором у указанных лиц.

Положение, предусмотренное комментируемой частью, согласуется с ч. 3 ст. 20 комментируемого закона, согласно которой оператор обязан внести в персональные данные лица необходимые изменения в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что такие данные являются неполными, неточными или неактуальными.

4. Часть 3 комментируемой статьи также логически продолжает ч. 1 и определяет дальнейшие действия оператора в случае получения информации о неправомерной обработке персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора. Так, как предусмотрено данной частью статьи, оператор в указанном случае обязан осуществить следующие действия:

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;

уничтожить такие персональные данные или обеспечить их уничтожение, если обеспечить правомерность обработки персональных данных невозможно, - в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных;

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, - конкретный срок не установлен, однако представляется, что уведомление должно направляться непосредственно в день совершения указанных действий.

Толкование данной части статьи представляется довольно сложным ввиду ее неполного логического согласования с другими положениями комментируемого закона. В первую очередь, если в предыдущей части комментируемой статьи прямо указывается на то, что основанием для исполнения перечисленных в ней обязанностей оператора является "подтверждение факта неточности персональных данных", то есть

положительный результат проводимой проверки, в комментируемой части указание на это не содержится. При этом согласно ч. 1 комментируемой статьи блокировка данных осуществляется в обоих случаях на время проводимой проверки. Возможно сделать вывод, что и в данном случае следует понимать используемую формулировку законодателя "выявление неправомерной обработки персональных данных" как указание на положительность результата проводимой проверки действительной неправомерности такой обработки. Можно говорить о том, что в данном словосочетании неправомерность указанных данных уже подразумевается, о ней говорится как о действительном факте, и нет необходимости указывать на его подтверждение в ходе проверки. Однако в таком случае вопрос вызывает использование аналогичных формулировок в отношении выявления неточности персональных данных: "выявление неточных персональных данных" в ч. 1 комментируемой статьи и "подтверждение факта неточности персональных данных" в ч. 2. Согласно предложенному толкованию обязанности, которые наступают для оператора согласно комментируемой части статьи, появляются в момент подтверждения факта о неправомерности обрабатываемых сведений, о котором ему стало известно от субъекта персональных данных (его представителя) либо от Роскомнадзора. Если же данный факт не подтверждается (лицо, подавшее запрос, ошибочно считает обработку его персональных данных оператором неправомерной), указанные обязанности не возникают. Отметим также, что согласно ст. 9 комментируемого закона субъект персональных данных может отозвать согласие на обработку персональных данных, но при этом в ряде случаев оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных (см. комментарий к ст. 9).

В ином случае складывается ситуация, в которой оператор обязан прекратить обработку персональных данных и даже уничтожить их в том случае, когда в обращении или запросе субъекта персональных данных (его представителя), запросе Роскомнадзора указывается на неправомерность обработки данных, несмотря на то, что данные факты не подтверждаются. При этом оператор будет иметь право обжаловать поступившее к нему требование о прекращении неправомерной обработки данных. Данный порядок будет действовать в случае указания на неправомерность обработки персональных данных Роскомнадзором, однако не в случае направления оператору запроса, а в случае выдачи обязательного для исполнения предписания.

Пример: управлением Роскомнадзора в связи с жалобой гражданина Н. проведена внеплановая проверка соблюдения предприятием требований законодательства в сфере обработки персональных данных. В ходе данной проверки были выявлены нарушения требований ч. 1 ст. 6 и ч. 3 ст. 21 комментируемого закона в части обработки персональных данных без согласия субъекта персональных данных и в части неисполнения обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уничтожению персональных данных.

Проверкой было установлено, что МУП "Теплоэнергетика" в нарушение указанных норм обрабатывает персональные данные абонентов, в частности, гражданина Назарова С.А., с целью предоставления коммунальных услуг

населению (теплоснабжения), начисления платежей и расчетов с населением за оказанные услуги. Предприятию были выданы предписания, указавшие на необходимость в течение трех рабочих дней с даты получения предписания устранить нарушения ч. 3 ст. 21 комментируемого закона. Требования предписания предприятием были выполнены, о чем сообщено административному органу. Вместе с тем заявитель, посчитав, что требования об уничтожении персональных данных применительно к МУП "Теплоэнергетика", не основаны на законе, обратился в суд с заявлением (см. решение Арбитражного суда Калининградской области от 26.10.2010 по делу N А21-6046/2010).

Неоднозначность используемых в комментируемой части формулировок, позволяющая двоякое толкование, может повлечь неоднозначность складывающейся практики и увеличение количества связанных с этим судебных споров.

Момент начала течения сроков, предусмотренных комментируемой статьей, также определяется выражением "выявление неправомерной обработки персональных данных" (в ч. 2, для сравнения, используется выражение "со дня представления таких сведений"). Часть 3 ст. 20 также закрепляет, что оператор обязан уничтожить персональные данные лица 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. Комплексный анализ указанных положений, устанавливающих равный срок для уничтожения неправомерно обрабатываемых персональных данных, приводит нас к выводу, что под "выявлением неправомерной обработки персональных данных" понимается день представления субъектом персональных данных или его представителем, органом Роскомнадзора сведений, подтверждающих такую неправомерность, что влечет указанные нами ранее последствия в виде обязательности для оператора прекратить обработку или уничтожить данные, о неправомерности обработки которых ему было сообщено, независимо от того, действительно ли она неправомерна. Представляется, что операторам, применяющим комментируемый закон на практике, было бы удобнее использование законодателем более прозрачных и логически взаимосвязанных формулировок.

Также комментируемая часть предусматривает, что неправомерность обработки персональных данных влечет уничтожение таких данных (в течение 7 рабочих дней) только в случае, если невозможно обеспечить правомерность такой обработки (в течение 3 рабочих дней). Можно сделать соответствующий вывод: в первую очередь оператор должен направить все силы для обеспечения правомерности обработки данных (получения согласия на обработку у субъектов персональных данных), и лишь после определения невозможности такого обеспечения - уничтожить персональные данные.

Оператор сам будет исполнять данные обязанности по обеспечению правомерности обработки и уничтожению персональных данных, если данная обработка производится им непосредственно. В случае если обработка осуществляется лицом, действующим по поручению оператора, на оператора возлагаются обязанности по обеспечению указанных действий.

5. Часть 4 комментируемой статьи определяет обязанности оператора при достижении цели обработки персональных данных. Согласно ч. 2 ст. 5 комментируемого закона обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей (см. комментарий к ст. 5).

В случае достижения цели обработки персональных данных оператор обязан:

прекратить обработку персональных данных или обеспечить ее прекращение, - конкретный срок законодателем не установлен, однако представляется, что такая обязанность возникает у оператора непосредственно при достижении названной цели;

уничтожить персональные данные или обеспечить их уничтожение, - в тридцатидневный срок с даты достижения цели обработки персональных данных.

Уничтожение персональных данных не всегда является необходимым последствием достижения цели их обработки. Если оператор обладает правом осуществлять обработку персональных данных лица без его согласия, он может не уничтожать такие данные. Отметим, что хранение персональных данных относится к обработке персональных данных. Кроме того, иной порядок может быть также предусмотрен соглашением между оператором и субъектом персональных данных (договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением).

Также стоит отметить, что в данном случае комментируемый закон не предусматривает частичного уничтожения персональных данных оператором, в том числе в зависимости от вида носителя, на котором хранится такая информация (см. решение Арбитражного суда Республики Бурятия от 09.07.2012 по делу N А10-125/2012), поэтому в данном случае следует уничтожать как персональные данные, хранящиеся в электронном виде в информационной системе, так и данные, зафиксированные на материальном носителе.

Неисполнение указанной обязанности оператора может быть выявлено в ходе проверки, проводимой Роскомнадзором, уполномоченным осуществлять контроль и надзор соответствием обработки персональных данных требованиям комментируемого закона, и повлечь вынесение в его адрес предписания с требованием устранить нарушения.

Пример: в ходе проверки деятельности ЗАО "КОМСТАР-Регионы", проводимой Роскомнадзором, было установлено, что договор, заключенный с абонентом М., был расторгнут 1 июня 2011 г., задолженность ее погашена, следовательно, цель обработки достигнута 1 июня 2011 г. Однако, несмотря на указанные обстоятельства, оператор по истечении трех рабочих дней продолжал обрабатывать персональные данные М. с использованием автоматизированной системы расчетов "Телеком", что подтверждается распечатками полей АСР "Телеком" от 08.06.2011. Обществу было выдано соответствующее предписание. Данное предписание было обжаловано в суде, однако суд подтвердил, что оно не противоречат законодательству Российской Федерации (см. постановление

ФАС Поволжского округа от 28.04.2012 N Ф06-2316/2012).

6. Часть 5 комментируемой статьи определяет обязанности оператора, наступающие при отзыве субъектом персональных данных согласия на обработку его персональных данных. Согласно ч. 2 ст. 9 комментируемого закона согласие на обработку персональных данных может быть отозвано субъектом персональных данных. Однако в ряде случаев оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных (см. комментарий к ст. 9). В случае такого отзыва оператор обязан:

прекратить обработку персональных данных или обеспечить ее прекращение, - представляется, что такая обязанность возникает у оператора непосредственно при достижении названной цели;

уничтожить персональные данные или обеспечить их уничтожение, - в тридцатидневный срок с даты с даты поступления указанного отзыва.

Уничтожение персональных данных не всегда является необходимым последствием отзыва субъектом персональных данных согласия на обработку его персональных данных. Как мы уже говорили, оператор может обладать правом осуществлять обработку персональных данных лица без его согласия, соответственно обращение обладателя персональных данных с отзывом согласия на их обработку не повлечет для него обязательных последствий. Также уничтожение персональных данных производится лишь в тех случаях, когда их сохранение более не требуется для целей обработки персональных данных. Иной порядок может быть также предусмотрен соглашением между оператором и субъектом персональных данных. В качестве такого соглашения, например, может выступать кредитный договор, заключаемый между банком и заемщиком.

Пример: между ОАО "Азиатско-Тихоокеанский банк" в г. Улан-Удэ и гражданином М. (выступающим как заемщик) был заключен кредитный договор. Пунктом 5.7 договора предусмотрено, что данный договор одновременно является выражением согласия заемщика на обработку, распространение в случаях, предусмотренных комментируемым законом, использование, трансграничную передачу, обезличивание с использование средств автоматизации или без использования таких средств его персональных данных, содержащихся в настоящем договоре, в целях надлежащего исполнения условий настоящего договора. Согласно п. 5.7.2 согласие может быть отозвано заемщиком путем направления банку заявления в письменной форме. В этом случае банк прекращает обработку персональных сведений и уничтожает их после исполнения сторонами условий обязательств, вытекающих из настоящего договора (см. решение Арбитражного суда Республики Бурятия от 09.07.2012 по делу N А10-125/2012).

Хотелось бы отметить, что ч. 4 и 5 комментируемой статьи сформулированы законодателем довольно сложно, что затрудняет их применение на практике. Использование таких сложных грамматических конструкций не обеспечивает однозначности толкования указанных положений правоприменителями.

Неисполнение указанной обязанности оператора может быть выявлено в

ходе проверки, проводимой Роскомнадзором, уполномоченным осуществлять контроль и надзор за соответствием обработки персональных данных требованиям комментируемого закона, проводимой в связи с обращением в его адрес заинтересованного субъекта персональных данных, и повлечь вынесение предписания с требованием устранить нарушения.

Пример: в результате заключения и исполнения кредитного договора между ОАО "Азиатско-Тихоокеанский банк" в г. Улан-Удэ и гражданином М. возникла спорная ситуация, связанная с обработкой банком персональных данных М. В связи с полным погашением кредита в банке М. подал заявление об удалении, уничтожении всех личных данных, включая номер паспорта, номера телефонов, адреса и прочие сведения, находящиеся в распоряжении (базе данных) банка. Банком было отказано в уничтожении персональных данных М. Роскомнадзором на основании обращения М. была проведена внеплановая выездная проверка в отношении ОАО "АТБ", которая подтвердила, что персональные данные М. хранятся как в информационной системе ОАО "АТБ", так и на бумажных носителях, в том числе копия паспорта М. Право субъекта персональных данных на удаление своих персональных данных реализовано не было. Банку было вынесено предписание, обжалованное им в дальнейшем в суд.

Суд апелляционной инстанции, рассматривая указанное дело, указал на то, что исполнение заключенного между сторонами кредитного договора породило для каждой из сторон не только гражданско-правовые права и обязанности, но и публично-правовые обязанности, которые каждая из сторон кредитного договора обязана исполнить вне зависимости от желания другой стороны гражданско-правового соглашения. Суд посчитал, что наличие у кредитной организации персональных данных контрагента по договору обуславливается необходимостью обработки персональных данных для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно-значимых целей. Уничтожение указанных персональных данных не позволит банку надлежащим образом соблюсти требования законодательства Российской Федерации о бухгалтерском учете, о противодействии легализации доходов, полученных преступным путем, и др., чем нарушатся его законные интересы в соблюдении требований данного законодательства. В связи с этим требования о признании предписания незаконным суд не признал (см. подробнее решение Арбитражного суда Республики Бурятия от 09.07.2012 по делу N А10-125/2012).

7. Часть 6 комментируемой статьи определяет порядок действий оператора в том случае, когда отсутствует возможность уничтожения персональных данных в течение предусмотренного предыдущими частями статьи срока. Указанные данные должны быть уничтожены в любом случае при возникновении соответствующей обязанности оператора в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами. До этого времени указанные персональные данные должны находиться в заблокированном состоянии.

Статья 22. Уведомление об обработке персональных данных

1. Статья 22 комментируемой статьи посвящена обязанностям операторов персональных данных, связанным с направлением уведомления об обработке персональных данных. Указанное уведомление подается оператором персональных данных до начала работы с персональным данными и предваряет такую работу. В нем выражается намерение оператора осуществлять обработку персональных данных. Порядок предоставления уведомлений также регулируется 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", утв. приказом Минкомсвязи России от 21.12.2011 N 346.

Случаи направления указанного уведомления определены по остаточному принципу: оно подается во всех случаях, кроме прямо обозначенных в ч. 2 комментируемой статьи. К наиболее распространенным случаям из перечисленных, в которых не требуется предоставление уведомления об обработке персональных данных, относятся:

1) обработка 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, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. Таким образом, при осуществлении работодателем обработки персональных данных своих сотрудников за пределами, установленными ст. 86 ТК РФ, на него будет распространяться обязанность по направлению уведомления об обработке персональных данных;

2) получение персональных данных оператором в связи с заключением договора, стороной которого является субъект персональных данных. В указанном случае персональные данные должны:

не распространяться, а также не предоставляться 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 средствах массовой информации, в информационно-телекоммуникационных сетях или предоставление доступа к данным иным возможным способом;

использоваться оператором исключительно для исполнения указанного договора и заключения новых договоров с субъектом персональных данных.

Только выполнение всех перечисленных условий в совокупности дает право оператору не уведомлять управление Роскомнадзора о том, что он занимается обработкой персональных данных (см. решение Арбитражного суда Ставропольского края от 20.09.2010 по делу N А63-6610/2010). Невыполнение

хотя бы одного из названных условий влечет необходимость подачи такого уведомления;

3) обработка персональных данных, относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией. Для того чтобы осуществлять такую обработку без уведомления уполномоченного органа, необходимо соблюдать следующие условия:

обработка осуществляется для законных целей, предусмотренных их учредительными документами;

персональные данные не распространяются или раскрываются третьим лицам без согласия в письменной форме субъектов персональных данных;

3) обработка персональных данных, 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. Обработка персональных данных без использования средств автоматизации осуществляется в соответствии с Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утв. постановлением Правительства РФ от 15.09.2008 N 687 (о критериях разграничения автоматизированной и неавтоматизированной обработки см. п. 1 комментария к ст. 1, п. 4 комментария к ст. 3).

Кроме того, уведомление не следует подавать, если обработка производится в отношении общедоступных персональных данных, а также персональных данных:

включающих в себя только фамилии, имена и отчества субъектов персональных данных;

необходимых в целях однократного пропуска их субъекта на территорию оператора;

включенных в государственные автоматизированные информационные системы и государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

обрабатываемых в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса.

2. Требования к уведомлению об обработке персональных данных как к документу предусмотрены комментируемой статьей, а также Рекомендациями по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных, утв. приказом Роскомнадзора от 19.08.2011 N 706.

Часть 3 комментируемой статьи содержит перечень сведений, которые в обязательном порядке включаются в уведомление:

- наименование (фамилия, имя, отчество), адрес оператора.

Если оператором является юридическое лицо, указываются его полное наименование с указанием организационно-правовой формы и сокращенное наименование, адрес (юридический и почтовый, а также контактные данные), ИНН. Если такая организация имеет филиалы или представительства,

указываются их наименования и адреса. При этом указываются адреса (как юридического лица, так и его филиалов и представительств), где осуществляется непосредственная обработка персональных данных, и уточняется, осуществляется ли обработка персональных данных только юридическим лицом (формирование центральной информационной системы), только филиалами (представительствами), либо и юридическим лицом и филиалами (представительствами).

Если оператором является физическое лицо, указываются его фамилия, имя, отчество, адрес (место нахождения, почтовый адрес, контактные данные), данные документа, удостоверяющего личность; ИНН.

Если же оператором является государственный или муниципальный орган, указываются его полное и сокращенное наименование, наименование территориальных органов, адрес (место нахождения, почтовый адрес, контактные данные), ИНН;

- цель обработки персональных данных. Данная цель должна соответствовать компетенции оператора. Поэтому под ней понимаются как цели, указанные в учредительных документах оператора, так и цели фактически осуществляемой оператором деятельности по обработке персональных данных;

- категории персональных данных (персональные данные, биометрические персональные данные, специальные категории персональных данных (расовая принадлежность, национальная принадлежность, состояние здоровья и др.));

- категории субъектов, персональные данные которых обрабатываются, - также указываются виды отношений с указанными субъектами (например, физические лица - абоненты, состоящие в договорных и иных гражданско-правовых отношениях с юридическим лицом);

- правовое основание обработки персональных данных. Обработка персональных данных может осуществляться на основании федерального закона, постановления Правительства РФ, иного нормативно-правового акта, закрепляющего основание и порядок обработки персональных данных. В данном случае должны быть указаны конкретные статьи таких документов. При наличии лицензии на осуществление деятельности указываются номер, дата выдачи и наименование лицензии на осуществляемый вид деятельности, а также лицензионные условия, закрепляющие запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

- 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 (это должна быть конкретная дата начала любого действия (операции) или совокупности действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными);

- срок или условие прекращения обработки персональных данных (он может быть определен как конкретная дата или основание (условие), наступление которого повлечет 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 Российской Федерации.

Уведомление может быть направлено в виде документа на бумажном носителе или в форме электронного документа на бланке оператора и подписывается уполномоченным лицом. Образец формы уведомления об обработке (о намерении осуществлять обработку) персональных данных также утвержден приказом Роскомнадзора от 19.08.2011 N 706. Ранее комментируемая статья содержала требование о том, что уведомление, направленное в электронной форме, должно быть подписано электронной цифровой подписью. Актуальная редакция такого требования не содержит. Такое уведомление может быть направлено через Портал персональных данных Уполномоченного органа по защите прав субъектов персональных данных путем заполнения специальной формы*(85). 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.

3. Уполномоченный орган по защите прав субъектов персональных данных ведет реестр операторов персональных данных, порядок ведения такого реестра установлен Административным регламентом, утв. приказом Минкомсвязи России от 21.12.2011 N 346. Данный реестр является общедоступным и доступ к нему возможен через официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. По состоянию на 28.03.2013 в реестре содержатся данные о 271 657 операторах персональных данных*(86). Срок размещения общедоступных сведений, содержащихся в реестре, на официальном сайте Роскомнадзора составляет три дня с даты подписания приказа о внесении сведений об операторе в реестр. Исключение составляют сведения о средствах обеспечения безопасности персональных данных при их обработке, которые не являются общедоступными.

Согласно ч. 4 комментируемой статьи уполномоченный орган в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения, содержащиеся в уведомлении, а также сведения о дате направления указанного уведомления в реестр операторов. Пункт 16 Административного регламента, утв. приказом Минкомсвязи России от 21.12.2011 N 346, определяет общий срок внесения сведений об операторе в реестр как 15 дней с момента регистрации уведомления.

Рассмотрение уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также внесение сведений в реестр операторов осуществляются для оператора бесплатно (ч. 5 комментируемой статьи). Пункт 30 Административного регламента также предусматривает, что плата за предоставление данной государственной услуги не взимается.

В целях соответственного ведения уполномоченный орган по защите прав субъектов персональных данных в лице сотрудника территориального органа Роскомнадзора вправе требовать от оператора уточнения предоставленных сведений в случае предоставления неполных или недостоверных сведений до их внесения в реестр операторов (это право закреплено в ч. 6 комментируемой статьи). В этих целях сотрудник территориального органа Роскомнадзора направляет оператору письмо с уведомлением о его вручении, содержащее запрос с указанием перечня недостающих сведений для внесения в реестр. После подписания письма и присвоения ему регистрационного номера файл со сканированным письмом вносится в информационную систему Роскомнадзора в срок не позднее дня, следующего за днем его регистрации. Оператор обязан сообщить в территориальный орган Роскомнадзора по его запросу уточненные сведения, необходимые для осуществления деятельности указанного органа, в течение 30 дней с даты получения такого запроса. После получения от оператора уточненных сведений сотрудник Роскомнадзора (территориального органа Роскомнадзора), ответственный за работу в области персональных данных, вносит уточненные сведения в информационную систему Роскомнадзора в целях последующего внесения сведений об операторе в реестр. Если в течение 30 дней с даты получения запроса оператор не представил уточненные сведения, то по истечении указанного срока уведомление с неполными или недостоверными сведениями возвращается оператору без внесения сведений о нем в Реестр.

Порядок изменения сведений об операторе в реестре операторов персональных данных, а также исключения из него сведений об операторе также регламентируется упомянутым нами Административным регламентом. Часть 7 комментируемой статьи закрепляет обязанность оператора персональных данных в целях обеспечения указанной деятельности направлять уведомление в Роскомнадзор при изменении сведений, содержащихся в уведомлении об обработке персональных данных, - для изменения сведений, содержащихся в реестре, а также о прекращении обработки персональных данных, - для исключения сведений об операторе из реестра. Данная обязанность должна быть реализована им в течение десяти рабочих дней. Сведения об изменении сведений об операторе в реестре направляются им в Роскомнадзор в форме

информационного письма. Электронная форма информационного письма о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных, содержится на Портале персональных услуг*(87). Исключение сведений осуществляется на основании заявления об исключении сведений об операторе из реестра.

4. Очень часто нарушение требований комментируемой статьи является основанием выдачи операторам персональных данных предписаний об устранении нарушений требований комментируемого закона территориальными органами Роскомнадзора, выявленных в ходе проводимых проверок.

Пример: ЗАО "СевКавТИСИЗ", являясь оператором по обработке персональных данных, осуществило обработку персональных данных лица, не состоящего на момент обработки данных в трудовых отношениях с обществом, без указания на обработку специальной категории персональных данных - состояние здоровья - в уведомлении, представленном уполномоченному органу. Предписанием Управления Роскомнадзора по Краснодарскому краю ЗАО "СевКавТИСИЗ" было обязано устранить данное нарушение ч. 2 ст. 22 комментируемого закона. Несогласие заявителя с указанным предписанием послужило основанием для обращения в арбитражный суд, требования заявителя удовлетворены не были (см. решение Арбитражного суда Краснодарского края от 10.12.2010 по делу N А32-12882/2010).

Непредставление в уполномоченный орган уведомления об обработке персональных данных либо его несвоевременное представление (предоставление после начала обработки персональных данных) либо представление уведомления, содержащего неполные или недостоверные сведения, влечет административную ответственность по ст. 19.7 КоАП РФ. Ответственность по данной статье может наступить в виде предупреждения или наложения административного штрафа.

Пример: постановлением мирового судьи ТСЖ "Надежность" было привлечено к административной ответственности, предусмотренной ст. 19.7 КоАП РФ, ему было назначено наказание в виде административного штрафа 3000 руб., поскольку ТСЖ в установленный срок не представило в Управление Роскомнадзора по Хабаровскому краю уведомление об обработке персональных данных, нарушив ч. 4 ст. 20, ч. 1 ст. 22 комментируемого закона (см. решение Центрального районного суда г. Комсомольска-на-Амуре Хабаровского края от 05.10.2010).

Статья 22.1. Лица, ответственные за организацию обработки персональных данных в организациях

1. Статьей 22.1 "Лица, ответственные за организацию обработки персональных данных в организациях" комментируемый закон был дополнен Федеральным законом от 25.07.2011 N 261-ФЗ.

Часть первая данной статьи устанавливает для юридических лиц, являющихся операторами обработки персональных данных, обязательное

требование о назначении лица, ответственного за организацию обработки персональных данных.

Лицом, ответственным за организацию обработки персональных данных, может выступать физическое или юридическое лицо. В свою очередь, к физическим лицам относятся специально назначенные сотрудники организации, являющейся оператором обработки персональных данных, а также индивидуальный предприниматель, с которыми организацией - оператором заключен соответствующий договор. С юридическим лицом, назначенным оператором ответственным за организацию обработки персональных данных также необходимо заключение договора.

Независимо от того, является ли указанное лицо работником оператора, индивидуальным предпринимателем либо юридическим лицом, с которыми оператором заключен соответствующий договор, согласно ч. 2 комментируемой статьи оно получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему.

2. Часть третья рассматриваемой статьи возлагает на оператора обработки обязанность предоставлять лицу, ответственному за организацию обработки персональных данных, следующие сведения:

1) официальное наименование юридического лица являющегося оператором обработки полное и (в случае, если имеется) сокращенное, адрес (место нахождения) оператора;

2) цель обработки персональных данных;

3) категории персональных данных (например, специальные категории персональных данных);

4) категории субъектов, персональные данные которых обрабатываются. Данная категория может быть определена исходя из правовой природы отношений между оператором обработки и субъектами персональных данных, например:

трудовые отношения: работодатель (оператор обработки) - работник (субъект персональных данных);

оказание услуг: оператор связи (оператор обработки) - абонент (субъект персональных данных);

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными (сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение), общее описание используемых оператором способов обработки персональных данных;

7) описание мер, предусмотренных ст. 18.1 и 19 комментируемого закона, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

8) дату 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;

11) сведения об обеспечении безопасности персональных данных в

соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

3. Часть четвертая комментируемой статьи определяет обязанности лица, ответственного за организацию обработки персональных данных, в частности:

1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных. Требования к защите персональных данных при их обработке в информационных системах персональных данных утверждены постановлением Правительства РФ от 01.11.2012 N 1119;

2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов (акты принятые оператором) 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. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя определены ст. 20 комментируемого закона (см. комментарий к ней).

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. Часть 1 комментируемой статьи определяет, что уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям комментируемого закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи. В период с 2007 по 2011 годы орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи, подвергался неоднократной реорганизации. В настоящее время данные функции выполняет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), которая находится в ведении Министерства связи и массовых коммуникаций Российской Федерации. Роскомнадзор осуществляет свою деятельность непосредственно и через свои территориальные органы во взаимодействии с другими федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, общественными объединениями и иными организациями. Территориальные органы дислоцированы по субъектам Российской Федерации. Положение о

федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций утверждено постановлением Правительства РФ от 16.03.2009 N 228.

Следует отметить, что отношения в области организации и осуществления государственного контроля (надзора) регулируются Федеральным законом от 26.12.2008 N 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля".

Указанным федеральным законом устанавливаются:

1) порядок организации и проведения проверок юридических лиц, индивидуальных предпринимателей органами, уполномоченными на осуществление государственного контроля (надзора), муниципального контроля;

2) порядок взаимодействия органов, уполномоченных на осуществление государственного контроля (надзора), муниципального контроля, при организации и проведении проверок;

3) права и обязанности органов, уполномоченных на осуществление государственного контроля (надзора), муниципального контроля, их должностных лиц при проведении проверок;

4) права и обязанности юридических лиц, индивидуальных предпринимателей при осуществлении государственного контроля (надзора), муниципального контроля, меры по защите их прав и законных интересов.

2. Часть 2 комментируемой статьи указывает, что 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.

Порядок рассмотрения обращений определен Федеральным законом от 02.05.2006 N 59-ФЗ. В соответствии со ст. 12 указанного закона письменное обращение, поступившее в государственный орган, орган местного самоуправления или должностному лицу в соответствии с их компетенцией, рассматривается в течение 30 дней со дня регистрации письменного обращения. В исключительных случаях указанный срок рассмотрения может быть продлен, но не более чем на 30 дней, о чем должен быть уведомлен гражданин, направивший обращение.

3. Частью 3 комментируемой статьи закреплены права уполномоченного органа по защите прав субъектов персональных данных, а именно:

1) запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию (п. 1).

В соответствии с ч. 4 ст. 20 оператор обработки 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.

Статья 19.7 КоАП РФ "Непредставление сведений (информации)" предусматривает ответственность за непредставление или несвоевременное представление в государственный орган сведений информации, представление

которой предусмотрено законом, а также за представление такой информации в неполном объеме или в искаженном виде;

2) осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий (п. 2).

Административные процедуры проведения проверок определены 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, утв. приказом Министерства связи и массовых коммуникаций РФ от 14.11.2011 N 312;

3) указанные далее права, определенные в пп. 3-5, в процессе их реализации взаимосвязаны, это права:

3.1) требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных (п. 3). Указанное требование направляется оператору обработки в письменной форме;

3.2) принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований комментируемого закона (п. 4).

В качестве основной административной меры приостановления следует особо отметить выдачу предписания. Часть 1 ст. 19.5 КоАП РФ "Невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль)", устанавливающая ответственность за неисполнение требований указанных представлений и предписаний, предусматривает в качестве административного наказания дисквалификацию на срок до трех лет;

3.3) 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 (п. 5). Данное право реализуется в порядке, определенном подразделом II "Исковое производство" раздела II ГПК РФ;

4) 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:

а) направленных на обеспечение выполнения оператором обязанностей, предусмотренных комментируемым законом (ст. 18.1);

б) по обеспечению безопасности персональных данных при их обработке (ст. 19 комментируемого закона), в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств.

Пункт 5.1 ч. 3, предусматривающий данные правомочия уполномоченного органа, был введен в комментируемую статью Федеральным законом от 25.07.2011 N 261-ФЗ.

Как мы уже отмечали ранее (см. комментарий к ст. 19), федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, является Федеральная служба безопасности Российской Федерации (ФСБ России), а органом, уполномоченным в области противодействия техническим разведкам и технической защиты информации, - Федеральная служба по техническому и экспортному контролю (ФСТЭК России).

В соответствии с п. 2 Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), утв. постановлением Правительства РФ от 16.04.2012 N 313, к шифровальным (криптографическим) средствам (средствам криптографической защиты информации), включая документацию на эти средства, относятся:

средства шифрования;

средства имитозащиты;

средства электронной подписи;

средства кодирования;

средства изготовления ключевых документов;

ключевые документы;

аппаратные шифровальные (криптографические) средства;

программные шифровальные (криптографические) средства;

программно-аппаратные шифровальные (криптографические) средства;

5) 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 (п. 6).

Порядок приостановления, возобновления, прекращения действия лицензии и аннулирования лицензии определен Федеральным законом от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности", в соответствии со ст. 20 которого действие лицензии может быть приостановлено лицензирующим органом в следующих случаях:

а) привлечение лицензиата к административной ответственности за неисполнение в установленный срок предписания об устранении грубого нарушения лицензионных требований, выданного лицензирующим органом в

порядке, установленном законодательством Российской Федерации;

б) назначение лицензиату административного наказания в виде административного приостановления деятельности за грубое нарушение лицензионных требований в порядке, установленном законодательством Российской Федерации.

Вместе с тем следует помнить, что положения Федерального закона от 04.05.2011 N 99-ФЗ не распространяются на отношения, связанные с лицензированием ряда отдельных видов деятельности (ч. 2 ст. 1). В данном случае следует руководствоваться отдельными нормативными актами, определяющими, в том числе, порядок приостановления, возобновления, прекращения действия лицензии и аннулирования лицензии. В отношении видов деятельности, перечисленных в ч. 3 ст. 1 Федерального закона от 04.05.2011 N 99-ФЗ, в частности оказания услуг связи, особенности лицензирования, в том числе в части, касающейся порядка принятия решения о предоставлении лицензии, срока действия лицензии и порядка продления срока ее действия, приостановления и возобновления действия лицензии, могут устанавливаться федеральными законами, регулирующими осуществление таких видов деятельности;

6) 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 (п. 7). Подследственность уголовных дел определяется ст. 151 УПК РФ;

7) вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных (п. 8).

В соответствии со ст. 23 Федерального конституционного закона от 17.12.1997 N 2-ФКЗ "О Правительстве Российской Федерации" Правительство Российской Федерации на основании и во исполнение комментируемого закона издает имеющие нормативный характер акты в форме постановлений, обеспечивает их исполнение. В соответствии со ст. 36 Федерального конституционного закона от 17.12.1997 N 2-ФКЗ Правительству Российской Федерации принадлежит право законодательной инициативы в Федеральном Собрании, которое реализуется посредством внесения законопроектов в Государственную Думу;

8) привлекать к административной ответственности лиц, виновных в нарушении комментируемого закона (п. 9).

Основным составом, предусматривающим административную ответственность за нарушение положений комментируемого закона, является ст. 13.11 КоАП РФ "Нарушение установленного законом порядка сбора, хранения, или распространения информации о гражданах (персональных данных)" (иные составы, опосредовано устанавливающие административную ответственность, рассмотрены в комментарии к ст. 24). При этом следует отметить, что в соответствии со ст. 28.4 КоАП РФ процессуальное полномочие по возбуждению дела об административном правонарушении по указанному составу отнесено к исключительной компетенции прокурора. Рассмотрение

указанных дел в соответствии с положениями ст. 23.1 КоАП РФ осуществляется мировыми судьями. Материалы, содержащие данные, указывающие на наличие нарушений положений комментируемого закона, переданные уполномоченным органом по защите прав субъектов персональных данных (Роскомнадзором и его территориальными органами) прокурору, согласно п. 1 ч. 1 ст. 28.1 КоАП РФ будут служить поводом для возбуждения дела об административном правонарушении.

Согласно данным Отчета о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2011 год*(88) основными, типичными нарушениями требований комментируемого закона, выявленными в ходе плановых и внеплановых проверок, являются:

а) нарушение требований конфиденциальности при обработке персональных данных (ст. 7 комментируемого закона).

Пример: в ходе проведения проверки в отношении общества с ограниченной ответственностью "А" должностными лицами Уполномоченного органа были установлены факты доставки платежных документов в незаконвертованном виде. По данному факту органами прокуратуры на основании материалов Уполномоченного органа было возбуждено дело об административном правонарушении по ст. 13.11 КоАП РФ. По результатам рассмотрения материалов дела судом принято решение о привлечении общества к административной ответственности и наложении штрафа в размере пяти тысяч рублей;

б) неуведомление гражданина о начале обработки его персональных данных (ч. 3 ст. 18 комментируемого закона).

Пример: в N-ской области муниципальное унитарное предприятие "Расчетный центр" г. N-ска, получив от сторонней организации персональные данные нанимателей и собственников жилых помещений, а также членов их семей, не уведомило указанных лиц о начале обработки их персональных данных. Управление Уполномоченного органа по N-ской области по данному факту выдало предписание об устранении выявленных нарушений, соответствующие материалы были направлены в органы прокуратуры. Органами прокуратуры было возбуждено дело об административном правонарушении по ст. 13.11 КоАП РФ, по результатам рассмотрения которого на указанное предприятие был наложен штраф в размере пяти тысяч рублей.

4. Часть 5 комментируемой статьи определяет обязанности уполномоченного органа по защите прав субъектов персональных данных, а именно:

1) организовывать в соответствии с требованиями комментируемого 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.

Сроки и последовательность административных процедур и административных действий Роскомнадзора и его территориальных органов с операторами, осуществляющими обработку персональных данных, при предоставлении государственной услуги "Ведение реестра операторов, осуществляющих обработку персональных данных" определены соответствующим административным регламентом. Административный регламент Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги "Ведение реестра операторов, осуществляющих обработку персональных данных" утвержден приказом Минкомсвязи России от 21.12.2011 N 346.

Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными;

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. Часть 5.1., введенная Федеральным законом от 25.07.2011 N 261-ФЗ, указывает, что 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, а также утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных.

В качестве примеров органов иностранных государств, уполномоченных по защите прав субъектов персональных данных, можно отметить Федеральную комиссию по защите данных и свободе информации (Германия); Комиссию по защите персональных данных (Чехия); Национальное агентство по защите данных и свободе информации (Венгрия).

Одной из форм международного обмена информацией о защите прав субъектов персональных данных выступают специализированные международные конференции и семинары, организуемые по инициативе Роскомнадзора.

6. Часть 6 комментируемой статьи определяет, что решения уполномоченного органа по защите прав субъектов персональных данных могут

быть обжалованы в судебном порядке. Следует отметить, что порядок судопроизводства по делам об оспаривании указанных выше решений, а также действий (бездействий) уполномоченного органа по защите прав субъектов персональных данных определен главой 25 ГПК РФ.

7. Часть 7 обязывает уполномоченный орган по защите прав субъектов персональных данных ежегодно направлять отчет о своей деятельности Президенту Российской Федерации, в Правительство Российской Федерации и Федеральное Собрание Российской Федерации. Указанный отчет подлежит опубликованию в средствах массовой информации. В частности, ознакомиться с отчетами деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2009-2011 годы можно на официальном сайте Роскомнадзора*(89).

8. Часть 8 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 текущий год утвержден Федеральным законом от 03.12.2012 N 216-ФЗ "О федеральном бюджете на 2013 год и на плановый период 2014 и 2015 годов".

9. Часть 9 указывает, что при уполномоченном органе по защите прав субъектов персональных данных на общественных началах создается консультативный совет, порядок формирования и порядок деятельности которого определяются уполномоченным органом по защите прав субъектов персональных данных.

В настоящее время Положение о Консультативном совете при уполномоченном органе по защите прав субъектов персональных данных утверждено приказом Роскомнадзора от 20.06.2012 N 621. Согласно данному документу консультативный совет формируется из представителей Роскомнадзора и федеральных органов государственной власти, членов Общественной палаты Российской Федерации, объединений операторов, осуществляющих обработку персональных данных и осуществляющих сотрудничество с Роскомнадзором, экспертов в области персональных данных и информационной безопасности, руководителей предприятий и организаций, входящих в сферу деятельности Роскомнадзора, общественных организаций, рекомендованных Общественной палатой Российской Федерации.

Состав Консультативного совета утверждается приказом Роскомнадзора и состоит из председателя, заместителя председателя, ответственного секретаря и членов Консультативного совета. На сегодняшний день состав Консультативного совета утвержден приказом Роскомнадзора от 06.07.2012 N 679 "Об утверждении состава Консультативного совета при уполномоченном органе по защите прав субъектов персональных данных".

Основными задачами Консультативного совета являются подготовка предложений и рекомендаций по вопросам:

гармонизации законодательства Российской Федерации в области защиты персональных данных с учетом общественного мнения и опыта правоприменительной практики;

обеспечения соблюдения законодательства Российской Федерации в

области защиты персональных данных;

методического обеспечения правоприменительной деятельности в области защиты персональных данных;

содействия распространению положительного опыта по организации защиты прав субъектов персональных данных;

содействия формированию позитивного общественного мнения, способствующего созданию и развитию эффективной системы защиты прав субъектов персональных данных;

создания условий для повышения правового уровня и активной гражданской позиции общества.

Консультативный совет осуществляет следующие функции:

участие в формировании программ и планов деятельности Роскомнадзора на среднесрочную и долгосрочную перспективу в области защиты персональных данных;

рассмотрение приоритетных категорий операторов, осуществляющих обработку персональных данных, для включения 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 Российской Федерации в области персональных данных; рассмотрение перечня проектов нормативных правовых актов и иных документов в области защиты персональных данных; обсуждение проектов законодательных и иных нормативных правовых актов в области персональных данных;

содействие реализации мер, направленных на защиту прав субъектов персональных данных, а также на расширение международного сотрудничества по вопросам защиты прав субъектов персональных данных.

Деятельность Консультативного совета является открытой для общественности. Информация о проводимых заседаниях Консультативного совета, принимаемых решениях, деятельности постоянных и временных рабочих группах размещается на официальном сайте Роскомнадзора (http://www.rsoc.ru/personal-data/advisory-board) и Портале персональных данных (http://pd.rsoc.ru/advisory-council/).

Статья 24. Ответственность за нарушение требований комментируемого закона

1. Комментируемая статья посвящена вопросам ответственности за нарушение требований комментируемого закона.

Первоначальный вариант ст. 24 предусматривал только положение о том, что лица, виновные в нарушении требований комментируемого закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

В последующем Федеральным законом от 25.07.2011 N 261-ФЗ ст. 24 была редактирована и дополнена частью второй.

Часть первая в новой редакции является бланкетной, ее содержание от предыдущей редакции отличается еще меньшей конкретикой, в ней указывается, что виновные в нарушении требований комментируемого закона лица несут ответственность предусмотренную законодательством Российской Федерации, без указания ее видов и отсылочных норм.

Законодательство Российской Федерации за нарушения комментируемого закона в настоящее время предусматривает уголовную, административную, гражданскую и дисциплинарную ответственность.

1.1. Уголовная ответственность.

В УК РФ впервые специальная норма, предусматривающая ответственность за нарушение законодательства в области обработки персональных данных и употребляющая понятие "персональные данные", появилась в связи с введением Федеральным законом от 07.12.2011 N 419-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации" ст. 173.2 "Незаконное использование документов для образования (создания, реорганизации) юридического лица", ч. 2 которой предусматривает ответственность за использование персональных данных, полученных незаконным путем для образования (создания, реорганизации) юридического лица в целях совершения одного или нескольких преступлений, связанных с финансовыми операциями либо сделками с денежными средствами или иным имуществом.

Статья 272 УК РФ "Неправомерный доступ к компьютерной информации" в отношении автоматизированной обработки персональных данных в настоящее время является наиболее действенной и применяемой нормой, устанавливающей ответственность за незаконный доступ к обрабатываемым в автоматизированных информационных системах персональным данным.

Обязательным признаком объективной стороны преступления, предусмотренного ст. 272 УК РФ, являются последствия в виде уничтожения, блокирования, модификации, копирования персональных данных в электронной форме. Данное преступление материальное, оно окончено в случае наступления указанных последствий. Ознакомление с персональными данными, хранящимися в памяти компьютера, не позволяет привлечь лицо к уголовной ответственности по ст. 272 УК, если не наступили вышеуказанные последствия. В настоящее время криминальная практика выработала различные способы организации неправомерного доступа, в том числе путем задействования вредоносных программ. В таких случаях деяние будет квалифицироваться по совокупности статей 272 УК РФ "Неправомерный доступ к охраняемой законом информации", 273 УК РФ "Создание, использование и распространение вредоносных компьютерных программ".

Кроме того, необходимо выделить ряд составов, опосредовано устанавливающих ответственность за нарушение комментируемого закона.

К таковым следует отнести:

1) ст. 137 УК РФ "Нарушение неприкосновенности частной жизни".

Применительно к автоматизированной обработке персональных данных объективная сторона данного деяния состоит в незаконном собирании или распространении в электронной форме персональных данных, составляющих сведения о частной жизни лица, его личную или семейную тайну, без его согласия либо распространении этой информации публично, в том числе посредством возможностей Интернета.

Необходимо оговорить, что до настоящего времени в законодательстве отсутствует четкое определение объема персональных данных, составляющего сведения о частной жизни лица. Попытка установить его делается в ст. 10 комментируемого закона, в которой вводится понятие специальных категорий персональных данных. К ним закон относит персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

2) ст. 140 УК РФ "Отказ в предоставлении гражданину информации" имеет лишь потенциальную возможность опосредованного применения.

Так, государственные, муниципальные органы в соответствии со ст. 13 комментируемого закона создают в пределах своих полномочий государственные или муниципальные информационные системы персональных данных, т.е. являются операторами обработки персональных данных. В ст. 24 Конституции РФ указывается, что органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить любому гражданину возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Комментируемый закон предусматривает в ст. 14 случаи ограничения доступа субъекта к своим персональным данным. В случае отсутствия подобных ограничений должностные лица государственных и муниципальных органов обязаны предоставить гражданину информацию о действиях с его персональными данными. Соответственно применение ст. 140 УК РФ к представителям иных групп операторов обработки персональных данных (юридические, физические лица) невозможно. Неправомерный отказ должностного лица в предоставлении гражданину информации о действиях с его персональными данными, перечень которой установлен комментируемым законом, либо предоставление гражданину неполной или заведомо ложной информации образуют состав преступления. Мотивы и цели могут быть самыми разнообразными (неприязнь, месть, ревность, ненависть). При этом в диспозиции статьи указано, что данные действия должны обязательно причинить вред правам и законным интересам граждан;

3) ст. 155 УК РФ "Разглашение тайны усыновления (удочерения)".

Развитие информационных технологий, в частности создание автоматизированных информационных систем в органах записи актов гражданского состояния и создание электронных баз данных об усыновлении, обусловили актуализацию ст. 155 УК РФ "Разглашение тайны усыновления" как элемента системы правовой защиты персональных данных специальных категорий, относящихся к семейной тайне. Объективная сторона указанного деяния применительно к автоматизированной обработке данных об усыновлении

состоит в несанкционированном распространении информации из автоматизированной информационной системы, в том числе путем размещения подобной базы данных в режиме свободного доступа в открытых телекоммуникационных сетях (Интернет). Неправомерность оснований получения доступа к базам персональных данных позволяет квалифицировать деяние по совокупности преступлений ст. 155, 272 УК РФ;

4) ст. 171 УК РФ "Незаконное предпринимательство".

Объективная сторона данного деяния применительно автоматизированной обработки персональных данных состоит в осуществлении без соответствующих лицензий предпринимательской деятельности, связанной с технической защитой персональных данных; созданием информационных систем персональных данных, защищенных с использованием шифровальных (криптографических) средств, их обслуживанием - в случаях, если это деяние причинило крупный ущерб гражданам, организациям или государству либо сопряжено с извлечением дохода в сумме, превышающей один миллион пятьсот тысяч рублей средств.

Примером подобной деятельности может выступать контроль выполнения Требований к защите персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 01.11.2012 N 1119).

При этом следует отметить, что деятельность по защите персональных данных для собственных нужд юридическое лицо или индивидуальный предприниматель вправе осуществлять без соответствующих лицензий.

1.2. Административная ответственность.

КоАП РФ содержит составы, предусматривающие ответственность за нарушение требований комментируемого закона.

В соответствии с положениями ст. 14 комментируемого закона субъект имеет право на получение информации, касающейся обработки его персональных данных. За неправомерный отказ в предоставлении субъекту персональных данных указанной информации, ее несвоевременное предоставление либо предоставление заведомо ложной информации виновное лицо может быть привлечено к административной ответственности в соответствии со ст. 5.39 КоАП РФ "Отказ в предоставлении информации".

Статья 13.11 КоАП РФ предусматривает ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Содержание диспозиции ст. 13.11 КоАП РФ является достаточно широким и делает норму практически универсальной применительно к вопросу ответственности за нарушение права на защиту персональных данных. Анализ комментируемого закона и формирующейся в настоящее время правоприменительной практики свидетельствует о многообразии возможных вариантов использования ст. 13.11 КоАП РФ для привлечения к ответственности операторов обработки за нарушение законодательства в области обработки персональных данных. К таковым можно отнести:

- нарушение конфиденциальности персональных данных;

- нарушение порядка представления сведений для целей ведения реестра операторов персональных данных;

- обработку персональных данных в отсутствие согласия субъекта персональных данных;

- нарушение права субъекта персональных данных на доступ к своим персональным данным;

- незаконную обработку специальных категорий персональных данных;

- нарушение требований обеспечения безопасности персональных данных.

Кроме того, ч. 1 ст. 13.13 "Незаконная деятельность в области защиты информации" КоАП РФ применительно к автоматизированной обработке персональных данных устанавливает ответственность за осуществление без соответствующих лицензий предпринимательской деятельности, связанной с технической защитой персональных данных; созданием информационных систем персональных данных, защищенных с использованием шифровальных (криптографических) средств, их обслуживания.

Данный состав корреспондирует ст. 171 УК РФ.

1.3. Гражданская ответственность.

В соответствии со ст. 17 комментируемого закона заинтересованное лицо вправе в порядке, установленном законодательством о гражданском судопроизводстве, обратиться в суд за защитой нарушенных либо оспариваемых прав, свобод или законных интересов.

Заинтересованное лицо вправе в порядке, установленном законодательством о гражданском судопроизводстве, обратиться в суд за защитой нарушенных либо оспариваемых прав, свобод или законных интересов.

В соответствии со ст. 3 ГПК РФ заинтересованное лицо вправе в порядке, установленном законодательством о гражданском судопроизводстве, обратиться в суд за защитой нарушенных либо оспариваемых прав, свобод или законных интересов. Так, в порядке гражданского судопроизводства судами общей юрисдикции могут рассматриваться иски о нарушении права граждан на неприкосновенность частной жизни при автоматизированной обработке их персональных данных.

В порядке, предусмотренном главой 25 ГПК РФ, судами общей юрисдикции рассматриваются заявления об оспаривании решений, действий (бездействий) органов государственной власти, органов местного самоуправления, должностных лиц, государственных или муниципальных служащих по вопросам обработки персональных данных, в том числе с использованием средств автоматизации, которыми нарушено право на неприкосновенность частной жизни, включая его структурные элементы - право на защиту персональных данных, конфиденциальность персональных данных, а также созданы препятствия к их осуществлению.

Пример: Верховный Суд РФ рассмотрел заявление П.С.П. о признании недействующим образца списка членов регионального отделения политической партии - приложения к приказу Федеральной регистрационной службы от 25.04.2007 N 60 "Об утверждении образцов документов, необходимых для государственной регистрации политической партии и ее регионального отделения". В обоснование требований заявителем указывалось на нарушение его права на конфиденциальность персональных данных, вызванного

противоречием образца списка комментируемому закону. Спорным моментом являлось указание в данном образце данных о каждом члене регионального отделения политической партии, а именно: фамилии, имени, отчества, даты рождения, гражданства, адреса проживания, контактного телефона. Заявитель полагал, что сложившаяся ситуация нарушает его право на конфиденциальность персональных данных и неприкосновенность частной жизни, личную и семейную тайну. Вместе с тем Верховный Суд РФ нашел довод заявителя о противоречии образца списка комментируемому закону необоснованным, указав, что представление для государственной регистрации регионального отделения политической партии списка его членов ни распространением, ни разглашением персональных данных не является и, следовательно, согласия субъектов персональных данных в этом случае не требуется (см. решение Верховного Суда РФ от 17.01.2008 N ГКПИ07-1198).

1.4. Дисциплинарная ответственность.

Статья 192 ТК РФ предусматривает следующие виды дисциплинарных взысканий за совершение дисциплинарного проступка:

1) замечание;

2) выговор;

3) увольнение по соответствующим основаниям.

При этом к дисциплинарным взысканиям, относится увольнение работника по основанию, предусмотренному подп. "в" п. 6 ч. 1 ст. 81, а именно: 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.

2. Часть вторая комментируемой статьи, введенная Федеральным законом от 25.07.2011 N 261-ФЗ, определяет, что моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных комментируемым законом, а также требований к защите персональных данных, установленных в соответствии с комментируемым законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Статья 151 ГК РФ понимает под моральным вредом физические или нравственные страдания. Пункт 2 постановления Пленума Верховного суда РФ от 20.12.1994 N 10 "Некоторые вопросы применения законодательства о компенсации морального вреда" указывает примеры морального вреда, оставляя их перечень открытым. В частности, отмечается, что моральный вред может заключаться в нравственных переживаниях в связи с утратой родственников, невозможностью продолжать активную общественную жизнь, потерей работы, раскрытием семейной врачебной тайны, распространением не соответствующих действительности сведений, порочащих честь, достоинство или деловую репутацию гражданина, временным ограничением или лишением каких-либо прав, физической болью, связанной с причиненным увечьем, иным

повреждением здоровья либо в связи с заболеванием, перенесенным в результате нравственных страданий.

Способ и размер компенсации морального вреда определяется в соответствии со ст. 1101 ГК РФ, в положениях которой определено, что:

компенсация морального вреда осуществляется в денежной форме;

размер компенсации морального вреда определяется судом в зависимости от характера причиненных потерпевшему физических и нравственных страданий, а также степени вины причинителя вреда в случаях, когда вина является основанием возмещения вреда. При определении размера компенсации вреда должны учитываться требования разумности и справедливости;

характер физических и нравственных страданий оценивается судом с учетом фактических обстоятельств, при которых был причинен моральный вред, и индивидуальных особенностей потерпевшего.

Из общего смысла комментируемого закона, в частности ст. 17, следует необходимость установления вины причинителя вреда субъекту персональных данных.

Глава 6. Заключительные положения

Статья 25. Заключительные положения

1. Часть первая рассматриваемой статьи устанавливает срок вступления в силу комментируемого закона. Он вступает в силу по истечении ста восьмидесяти дней после дня его официального опубликования.

В соответствии с ч. 3 ст. 15 Конституции РФ законы подлежат официальному опубликованию. Неопубликованные законы не применяются. Порядок вступления в силу федеральных законов устанавливается Федеральным законом от 14.06.1994 N 5-ФЗ "О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания". Согласно положениям указанного закона федеральные законы применяются на территории Российской Федерации только после их официального опубликования. Официальным опубликованием считается первая публикация полного текста документа в "Парламентской газете", "Российской газете", "Собрании законодательства Российской Федерации" или первое размещение (опубликование) на "Официальном интернет-портале правовой информации" (www.pravo.gov.ru) (ст. 4 Федерального закона от 14.06.1994 N 5-ФЗ).

Комментируемый закон опубликован в "Российской газете" от 29.07.2006 N 165, в "Парламентской газете" от 03.08.2006 N 126-127, в Собрании законодательства Российской Федерации от 31.07.2006 N 31 (часть I), ст. 3451.

Согласно постановлению Конституционного суда РФ от 24.10.1996 N 17-П "По делу о проверке конституционности части первой статьи 2 Федерального закона от 07.03.1996 года "О внесении изменений в Закон Российской Федерации "Об акцизах" (п. 6), день, которым датируется выпуск "Собрания законодательства Российской Федерации" с текстом федерального закона, не может считаться днем его обнародования, поскольку указанная дата, как

свидетельствуют выходные данные, совпадает с датой подписания издания в печать и, следовательно, с этого момента еще реально не обеспечивается получение информации о содержании закона его адресатами. Днем официального опубликования федерального закона согласно позиции Конституционного суда РФ должен быть признан день опубликования его полного текста в "Российской газете". Таким образом, днем официального опубликования комментируемого закона следует считать 29 июля 2006 г., т.е. день опубликования закона в "Российской газете".

Как предусмотрено в ст. 6 Федерального закона от 14.06.1994 N 5-ФЗ, федеральные законы вступают в силу одновременно на всей территории России по истечении 10 дней после дня их официального опубликования, если самими законами не установлен другой порядок вступления их в силу. Комментируемой статьей установлен такой иной порядок вступления в силу комментируемого закона - закон вступает в силу по истечении ста восьмидесяти дней после дня его официального опубликования.

В соответствии со ст. 191 ГК РФ течение срока, определенного периодом времени, 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., началом течения срока будет являться 30 июля 2006 г., а днем вступления комментируемого закона в силу - 26 января 2007 г.

Следует отметить, что обязательность повторного опубликования в официальных изданиях полного текста федерального закона, в который внесены изменения, Федеральный закон от 14.06.1994 N 5-ФЗ не предусматривает. Часть 4 ст. 9 указанного закона предусматривает лишь возможность повторного официального опубликования в полном объеме федерального закона, в который были внесены изменения или дополнения. Достаточно лишь официального опубликования федерального закона, которым внесены изменения в ранее изданный федеральный закон.

2. Часть 2 комментируемой статьи устанавливает, что после дня вступления в силу комментируемого закона (т.е. с 26 января 2007 г.), обработка персональных данных, включенных в информационные системы персональных данных до дня его вступления в силу (т.е. до 26 января 2007 г.), осуществляется в соответствии с комментируемым законом.

По общему правилу, нормативный правовой акт не распространяется на отношения, возникающие до его вступления в силу (ст. 54 Конституции РФ). Принцип права "закон обратной силы не имеет" является одним из основополагающих принципов правовой системы Российской Федерации.

Комментируемый закон частично ретроактивен, т.е. он не распространяет свое действие на те правоотношения по обработке персональных данных, которые возникли до вступления указанного закона в силу, но те персональные данные, которые были переданы на обработку до вступления закону в силу и не были обработаны, подлежат обработке уже в соответствии с комментируемым законом.

3. Части 2.1 и 4 комментируемой статьи устанавливают для операторов определенные обязанности по направлению сведений и уведомлений в

уполномоченный орган по защите прав субъектов персональных данных (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)).

Так, операторы, которые осуществляли обработку персональных данных до 01 июля 2011 г., обязаны представить в Роскомнадзор сведения, указанные в пп. 5, 7.1, 10 и 11 ч. 3 ст. 22 комментируемого закона, не позднее 01 января 2013 г.

Операторы, которые осуществляли обработку персональных данных до дня вступления в силу комментируемого закона и продолжают осуществлять такую обработку после дня его вступления в силу, обязаны направить в Роскомнадзор, за исключением случаев, предусмотренных ч. 2 ст. 22 комментируемого закона, уведомление, предусмотренное ч. 3 ст. 22, не позднее 01 января 2008 г. (см. подробнее об этом комментарий к ст. 22).

4. Часть 5 комментируемой статьи была введена в действие Федеральным законом от 05.04.2013 N 43-ФЗ "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" (ст. 33). Она определяет закон, который должен применяться к отношениям, связанным с обработкой персональных данных, осуществляемой при предоставлении государственных и муниципальных услуг, исполнении государственных и муниципальных функций в субъекте Российской Федерации - городе федерального значения Москве. В общем случае применяется комментируемый закон, однако, если Федеральный закон от 05.04.2013 N 43-ФЗ содержит отличные от него положения, применению будет подлежать последний из названных законов. В сущности, в комментируемой норме содержится правило разрешения коллизий между указанными законами, и приоритет отдается специальному и более позднему акту.

Амелин Р.В.,

Богатырева Н.В.,

Волков Ю.В.,

Марченко Ю.А.,

Федосин А.С.

---

*(1) См.: Вифлеемский А. Информационные системы персональных данных // Бюджетные организации: бухгалтерский учет и налогообложение. 2009. N 12. С. 52-69.

*(2) См.: Теория государства и права. Курс лекций / Под ред. Матузова Н.И., Малько А.В. М.: Юристъ, 1997. С. 95-98.

*(3) См.: Шахов Н.И. Теоретико-правовые основы функции обеспечения

государством права на неприкосновенность информации о частной жизни: автореф. дис. ... канд. юрид. наук. Краснодар, 2008.

*(4) См.: Цадыкова Э.А. Конституционное право на неприкосновенность частной жизни (сравнительно-правовое исследование): дис. ... канд. юрид. наук. М., 2007.

*(5) См.: Балашкина И.В. Право на неприкосновенность частной жизни в Российской Федерации: конституционно-правовое исследование: автореф. дис. ... канд. юрид. наук. М. 2007.

*(6) См.: Вельдер И.А. Система правовой защиты персональных данных в Европейском Союзе: дисс. ... канд. юрид. наук. Казань, 2006.

*(7) См.: Просветова О.Б. Защита персональных данных: Дисс. ... канд. юрид. наук. Воронеж, 2005.

*(8) Волкова О. Персональные данные работника и их защита // Кадровик. Трудовое право для кадровика, 2008. N 10. С. 29-36.

*(9) См.: Ходус Н.Н. Человек конструирует персональную идентичность // Вестник Алтайского государственного аграрного университета. 2005. Т. 17. N 1. С. 189-192.

*(10) См.: Борисенко О.В. Анализ Федерального закона N 152-ФЗ "О персональных данных" // Электронное приложение к "Российскому юридическому журналу". 2012 N 2. С. 26-30.

*(11) См.: Соколова О.С. Персональные данные как информация ограниченного доступа: проблемы правового регулирования // Современное право, 2004. N 2. С. 18-21.

*(12) Гришаев С.П. Право гражданина на изображение // Гражданин и право. 2012. N 9. С. 48-53.

*(13) См., например, апелляционное определение Верховного суда Удмуртской Республики от 23.04.2012 по делу N 33-1198, указавшего, что в удовлетворении исковых требований о компенсации морального вреда, причиненного незаконным получением сведений персонального характера, было отказано правомерно, поскольку работодатель, запрашивая информацию о месте нахождения работника в рабочее время, осуществлял свои полномочия по контролю за трудовой дисциплиной, и по своему характеру и объему информация, которая была запрошена, не является персональными данными по смыслу комментируемого закона.

*(14) См., например, апелляционное определение Московского городского суда от 30.03.2012 по делу N 11-2145, указавшего, что в удовлетворении исковых требований о защите персональных данных, взыскании компенсации морального вреда было отказано правомерно, поскольку персональные данные, использованные ответчиком, являются общедоступными и размещены истцом в сети Интернет.

*(15) См. Амелин Р.В. О правовых принципах разработки государственных АИС, обрабатывающих персональные данные // Информационное право. 2009. N 2. С. 32-35.

*(16) Информационное право: актуальные проблемы теории и практики: колл. монография / Под общ. ред. И.Л. Бачило. М.: Издательство Юрайт, 2009. С. 63.

*(17) Вифлеемский А. Информационные системы персональных данных // Бюджетные организации: бухгалтерский учет и налогообложение. 2009. N 12. С. 52-69.

*(18) Комментарий к Уголовному кодексу Российской Федерации (постатейный) (5-е издание, исправленное и дополненное) // Отв. ред. В.М. Лебедев. М.: Юрайт-Издат, 2005.

*(19) Ищенко Е.П., Топорков А.А. Криминалистика: Учебник (2-е издание, исправленное и дополненное). М.: Контракт, Инфра-М, 2006.

*(20) Комментарий к Уголовному кодексу Российской Федерации (постатейный) (3-е издание, исправленное, дополненное и переработанное) // Под ред. А.И. Чучаева. М.: Контракт, 2011.

*(21) Сизов А.В. Квалификация нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети // Информационное право, 2007, N 4.

*(22) См.: Personal data protection in the European Union. European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI)) // Official Journal C 033 E, 05/02/2013. P. 0101-0110.

*(23) ICO urges more care with personal data as Nursing and Midwifery Council receives ?150,000 penalty // ICO site News release: 15 February 2013. URL: http://www.ico.gov.uk/news/latest_news/2013/nursing-and-midwifery-council -receives-150000-penalty-15022013.aspx (дата обращения: 10.03.2013).

*(24) Становление человечества // Алексеев В.П. Избранное. Т. 1. Антропогенез. М.: Наука, 2007. С. 255.

*(25) См.: Чалая Л.Э. Модель идентификации пользователей по клавиатурному почерку // Штучний інтелект, 2004. N 4. С. 811-817.

*(26) См.: Гончаров С.М., Суховей А.А. Этапы генерации уникальных ключевых последовательностей на основе папиллярного узора отпечатков пальцев // Доклады ТУСУРа, 2010. N 1 (21). ч. 1, июнь. С. 97-99.

*(27) Куликова О.В. Биометрические криптографические системы и их применение // Безопасность информационных технологий. 2009. N 3. С. 53-57.

*(28) Сесин Е.М., Белов В.М. Системы идентификации личности, основанные на интеграции нескольких биометрических характеристик человека // Доклады ТУСУРа, 2012. N 1 (25). ч. 2. Июнь. С.175-179; Сесин Е.М., Белов В.М. Построение моделей идентификации личности, основанных на сравнении множества физических или поведенческих характеристик человека // Вестник СибГУТИ. 2011. N 4. С. 41-50.

*(29) Biometrics Design Standarts for UID Applications / Unique Identification Authority of India New Delhi.- 2009. V 1.0. P. 30.

*(30) См.: Conformance Test Architecture for Biometric Data Interchange Formats - Version Beta 2.0 / Fernando L. Podio, Dylan Yaga, Mark Jerde. U.S. Department of Commerce. National Institute of Standards and Technology: 2011. 37 p.

*(31) Biometric Data Safeguarding Technologies Analysis and Best Practices Study Report: Report DRDC CSS CR 2011-29 / Pierre Meunier. International Biometric Group. DRDC Centre for Security Science Defence R&D. Canada. 2011. P. 10.

*(32) Руководство по реадмисии: для экспертов и специалистов-практиков. Главный редактор Марина МАНКЕ. М.: Бюро по международной миграции в

Москве, 2009. В 2-х томах. Том. 1. С. 13.

*(33) Соглашение между Правительством Российской Федерации и Федеральным Советом Швейцарской Конфедерации 21.09.2009 года "О реадмиссии" // Национальное деловое партнерство Альянс Медиа: Сайт Предпринимательское право. URL: http://www.businesspravo.ru/Docum/DocumShow_DocumID_161069.html (дата обращения: 10.02.2013).

*(34) Полный перечень лиц составляют:

1) лица, замещающие: а) государственные должности Российской Федерации, в отношении которых федеральными конституционными законами или федеральными законами не установлен иной порядок осуществления контроля за расходами; б) должности членов Совета директоров Центрального банка Российской Федерации; в) государственные должности субъектов Российской Федерации; г) муниципальные должности на постоянной основе; д) должности федеральной государственной службы, включенные в перечни, установленные нормативными правовыми актами Президента Российской Федерации; е) должности государственной гражданской службы субъектов Российской Федерации, включенные в перечни, установленные законами и иными нормативными правовыми актами субъектов Российской Федерации; ж) должности муниципальной службы, включенные в перечни, установленные законами, иными нормативными правовыми актами субъектов Российской Федерации и муниципальными нормативными правовыми актами; з) должности в Банке России, перечень которых утвержден Советом директоров Банка России; и) должности в государственных корпорациях, включенные в перечни, установленные нормативными правовыми актами Российской Федерации; к) должности в Пенсионном фонде Российской Федерации, Фонде социального страхования Российской Федерации, Федеральном фонде обязательного медицинского страхования, включенные в перечни, установленные нормативными правовыми актами Российской Федерации; л) должности в иных организациях, созданных Российской Федерацией на основании федеральных законов, включенные в перечни, установленные нормативными правовыми актами Российской Федерации; м) отдельные должности на основании трудового договора в организациях, создаваемых для выполнения задач, поставленных перед федеральными государственными органами, включенные в перечни, установленные нормативными правовыми актами федеральных государственных органов;

2) Президент Российской Федерации, члены Правительства Российской Федерации, члены Совета Федерации Федерального Собрания Российской Федерации, депутаты Государственной Думы Федерального Собрания Российской Федерации, судьи, депутаты законодательных (представительных) органов государственной власти субъектов Российской Федерации.

*(35) См.: Personal data protection in the European. Union European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI)) // Official Journal C 033 E, 05/02/2013. P. 0101-0110.

*(36) Directive 2002/58/EC of the European Parliament and of the Council of 12

July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) // Official Journal L 201 of 31.07.2002.

*(37) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data // Official Journal L 8 of 12.01.2001.

*(38) См., например: Дрючина Е.В. Вопросы применимого права при трансграничной передача данных. Европейский опыт // Актуальные проблемы права, 2012. N 2. С. 285-292.

*(39) См.: Directive of the European Parliament and of the Council 2012/0010 (COD) on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Brussels, 25.01.2012 (проект).

*(40) См., например: Resolution of the 85th Conference of the Data Protection Commissioners of the Federal Government and the Landerin Bremerhaven on 13-14 March 2013 "Europe must strengthen data protection".

*(41) См. Наумов В.Б. Право и Интернет: Очерки теории и практики. М., 2002. С. 113-150.

*(42) Ожегов С.И. Словарь русского языка / Под ред. Н.Ю. Шведовой. 22-е изд. стер. М. 1990. С. 26.

*(43) Постановление Правительства Российской Федерации от 16.03.2009 N 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций".

*(44) Официальный сайт Роскомнадзора. URL: http://роскомнадзор.рф/news (дата обращения: 28.03.2013).

*(45) См.: Международное законодательство // Портал персональных данных Уполномоченного органа по защите прав субъектов персональных данных. URL: http://www.pd.rsoc.ru/law/ (дата обращения: 28.03.2013).

*(46) См., например: Раздел "Трансграничная передача персональных данных" на сайте "Информационная безопасность" предлагает наиболее подробное описание процедуры трансграничной передачи персональных данных:

1) общие положения (организационная структура компании; страна (страны), в которую передаются персональных данных; цель передачи и обработки персональных данных за границей);

2) правовое обоснование трансграничной передачи персональных данных (перечень нормативно-правовых документов, на основании которых осуществляется передача и обработка персональных данных);

3) описание объекта защиты;

4) характеристики передаваемых персональных данных (категории персональных данных, передаваемых за границу; категории субъектов персональных данных; способы обработки персональных данных (автоматизированная, неавтоматизированная, смешанная обработка));

5) регламент обеспечения безопасного информационного обмена

персональными данными с зарубежными филиалами (представительствами) (описание информационной системы персональных данных, из которой передаются персональные данные; описание информационной системы персональных данных, куда передаются персональные данные; каналы передачи данных; стандарты и протоколы передачи данных и т.д.); описание мероприятий и средств обеспечения защиты передаваемых персональных данных (организационные мероприятия; технические средства защиты информации, в том числе средства криптографической защиты информации);

6) состав законодательства иностранного государства, отражающего вопросы защиты персональных данных;

7) заключительные положения (зарубежный филиал обязуется соблюдать законодательство по обработке персональных данных страны, в которой он находится; обязуется обеспечить соответствующую защиту полученных и обрабатываемых персональных данных; подписи ответственных лиц головной организации и зарубежного филиала под вышеперечисленными положениями) (URL: http://www.itsec.ru/articles2/Inf_security/transgranichnaya-peredacha-pd (дата обращения: 28.03.2013)).

*(47) См.: Постановление Правительства РФ от 27.11.2006 N 719 "Об утверждении Положения о воинском учете".

*(48) См.: Постановление Правительства Москвы от 05.08.2008 N 709-ПП "О Городской целевой программе "Электронная Москва (2009-2011 гг.)".

*(49) См.: Постановление Правительства Москвы от 22.07.2008 N 591-ПП "О мерах по оптимизации привлечения иностранных работников на предприятия города Москвы".

*(50) См.: Жихарев П.А. Автоматизированные информационные системы и ресурсы г. Москвы: науч. издание. М.: ЮНИТИ-ДАНА; Закон и право, 2006. С. 22-114.

*(51) См.: Распоряжение правительства Москвы от 04.08.2008 N 1771-РП "О вводе в промышленную эксплуатацию автоматизированной информационной системы учета граждан, имеющих право на социальную поддержку при оплате жилых помещений и коммунальных услуг".

*(52) См., напр.: Приказ Федеральной службы по надзору в сфере образования и науки от 01.02.2005 N 130 "Об утверждении форм бланков ответов участника единого государственного экзамена, проводимого с использованием автоматизированной информационной системы "Экзамен", в 2005 году".

*(53) См.: Письмо Министерства образования и науки РФ от 26.05.2006 N 01-295/08-01 "Об участии вузов и ссузов в опытной эксплуатации АИС ЕСП в 2006 год".

*(54) См.: Приказ ФС по надзору в сфере защиты прав потребителей и благополучия человека от 30.12.2005 N 810 "О Перечне показателей и данных для формирования Федерального информационного фонда социально-гигиенического мониторинга".

*(55) Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. М.: Статут, 2011.

*(56) См.: Положение о порядке государственной регистрации субъектов

предпринимательской деятельности, утвержденное Указом Президента РФ от 08.07.1994 N 1482 "Об упорядочении государственной регистрации предприятий и предпринимателей на территории Российской Федерации".

*(57) Горелишвили Д. Человек и власть: однооконный интерфейс // Компьютерра. 2005. N 3.

*(58) См.: Дворецкий А.В. О принципах защиты персональных данных // Вестник ТГПУ. Серия: Гуманитарные науки, 2005. Выпуск 5 (49). С. 113-115.

*(59) См.: Терещенко Л.К. О соблюдении баланса интересов при установлении мер защиты персональных данных // Журнал российского права, 2011. N 5. С. 5-12.

*(60) См.: Малеина М.Н. Право на тайну и неприкосновенность персональных данных // Журнал Российского права. 2010. N 11 (167). С. 18-27.

*(61) См.: Трофимов О.И. Правовая охрана баз данных операторов электросвязи: Автореф. дисс. ... канд. юрид. наук. Москва, 2008. С. 6.

*(62) См.: Трофимов О.И. Указ. соч. С. 9-11.

*(63) Первый в истории процесс из-за фото с подписью "друг" // Право. Новости Шоу-бизнес. 2012. 19 окт. URL: http://pravo.ru/news/view/78874/ (дата обращения: 10.03.2013).

*(64) Федеральный закон от 10.01.2003 N 20-ФЗ "О Государственной автоматизированной системе Российской Федерации "Выборы".

*(65) Вычислительная техника и обработка данных. Терминологический толковый словарь фирмы IBM. Перевод с англ. Т. Тер-Микаэляна. М., Статистика. 1978. С. 20.

*(66) См.: Англо-русский энциклопедический словарь по современной электронной технике и программированию: компьютеры, Интернет, телекоммуникации, аудио-, видео-, теле- и радиотехника и пр. / И.Л. Мостицкий. М. Изд. Триумф, 2004. С. 73.

*(67) Там же.

*(68) Петров М.И. Комментарий к Федеральному закону "О персональных данных" (постатейный). М.: ЗАО Юстицинформ, 2007. С. 109.

*(69) Jet info - информационный бюллетень. 2009. N 5 (192). С. 11.

*(70) CAPTCHA, Completely Automatic Public Turing Test to Tell Computers and Humans Apart - полностью автоматизированный публичный тест Тьюринга для различия компьютеров и людей. Пользователю предлагается ввести в специальное поле формы автоматически созданное выражение на картинке из цифр и/или букв разного регистра, разного цвета, прочтение которого требует логического (человеческого) восприятия, недоступного автомату.

*(71) Новости от 17.10.2012 // Официальный сайт Роскомнадзора. URL: http://роскомнадзор.рф/news/rsoc/news16907.htm (дата обращения: 10.03.2013).

*(72) Субочев В.В. Теория законных интересов. Автореф. дисс. ... докт. юрид. наук.: 12.00.01. Тамбов. 2009. С. 12.

*(73) Слаутина М.В. Приемы деперсонификации юридического текста на сайте суда // Уральский филологический вестник, 2012. N 2. С. 80-4.

*(74) Первый в истории процесс из-за фото с подписью "друг" // Право. Новости Шоу-бизнес. 2012. 19 окт. URL: http://pravo.ru/news/view/78874/ (дата обращения: 10.03.2013).

*(75) См.: п. 100. "Blondje" против Нидерландов. Практическое руководство по критериям приемлемости. Совет Европы / Европейский суд по правам человека, 2011. С. 29.

*(76) См.: п. 103. Chamaiev и другие против Грузии и России. Практическое руководство по критериям приемлемости. Совет Европы / Европейский суд по правам человека, 2011. С. 30.

*(77) См.: п. 104. Omkarananda ile Divine Light Zentrum против Швейцарии. Практическое руководство по критериям приемлемости. Совет Европы / Европейский суд по правам человека, 2011. С. 30.

*(78) Латухина К. Закон на контроле. Президент Владимир Путин поговорил с Николаем Никифоровым // Российская газета - Федеральный выпуск. 2012. N 5876 (203).

*(79) Там же.

*(80) См.: Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2008 год // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: http://роскомнадзор.рф (дата обращения: 26.01.2013).

*(81) См.: Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2011 год // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: http://роскомнадзор.рф (дата обращения: 26.01.2013).

*(82) См.: Портал персональных данных. URL: http://pd.rsoc.ru/ (дата обращения: 10.03.2013).

*(83) Борисенко О.В. Анализ Федерального закона N 152-ФЗ "О персональных данных" // Электронное приложение к "Российскому юридическому журналу". 2012. N 2. С. 26-30.

*(84) Рыжов Р.С. Актуальные проблемы правового обеспечения накопления конфиденциальной информации о гражданах в телемедицине // Теория и практика общественного развития, 2011. N 7. С. 247-249.

*(85) URL: http://www.pd.rsoc.ru/operators-registry/notification/form/ (дата обращения: 10.03.2013).

*(86) Реестр операторов, осуществляющих обработку персональных данных // Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: http://www.rsoc.ru/personal-data/register/ (дата обращения: 10.03.2013).

*(87) URL: http://www.rsoc.ru/personal-data/forms/p333/ (дата обращения: 10.03.2013).

*(88) Отчеты о деятельности Уполномоченного органа по защите прав субъектов персональных данных // Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). URL: http://www.rsoc.ru/personal-data/reports/ (дата обращения: 10.03.2013).

*(89) Отчеты о деятельности Уполномоченного органа по защите прав субъектов персональных данных // Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). URL: http://www.rsoc.ru/personal-data/reports/ (дата обращения:

10.03.2013).