

Комментарий к Федеральному закону от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (коллектив авторов). - Специально для системы ГАРАНТ, 2021 г.

Пешкова (Белогорцева) Х.В., Ротко С.В., Рыдченко К.Д.,
Солдаткина О.Л., Струков К.В., Прокопенко А.Н., Тимошенко Д.А.

Глава 1. Общие положения

Статья 1. Сфера действия настоящего Федерального закона

1. Комментируемая статья очерчивает пределы правового регулирования настоящего федерального закона, определяет объект воздействия (персональные данные), субъектов правоприменения (**ч. 1 ст. 1**), предметную сферу действия, а также перечень изъятий из сферы его действия. Такой подход является классическим для кодифицированного законодательства, что подтверждает и содержание **гл. 1** Регламента ЕС о защите персональных данных, с разницей в том, что нормы несколько иначе скомпонованы в статье.

Поскольку объект воздействия и субъекты подробнее будут рассмотрены нами далее, остановимся подробнее на сфере воздействия.

Юридическое содержание сферы действия комментируемого закона составляют отношения, связанные с обработкой персональных данных любыми методами: с участием информационно-коммуникационных технологий и (или) без использования таковых, при условии, что это соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

При этом сфера действия комментируемого закона во времени конкретизируется в его заключительных положениях (**ст. 25**).

Сфера действия комментируемого **закона** в пространстве никак не определяется, что оставляет открытым вопрос об иностранных гражданах, на которых распространяются требования закона. Действительно, в связи с тем, что сеть Интернет обеспечивает возможность приобретения товаров и услуг у иностранных лиц, возникает вопрос, при каких условиях требования комментируемого закона распространяются на иностранные организации, не имеющие физического присутствия на территории Российской Федерации. Разъяснения даются, в частности, Министерством цифрового развития, связи и массовых коммуникаций РФ (Минцифры).

Минцифры отмечает, что при осуществлении деятельности в сети Интернет, которая в силу своего трансграничного, децентрализованного и виртуального характера не позволяет четко обозначить географические границы осуществления такой деятельности, необходимо установление специальных критериев, при которых она может быть отнесена к осуществляемой на территории Российской Федерации. Одной лишь доступности интернет-сайта на территории Российской Федерации недостаточно для вывода о том, что на него распространяется законодательство Российской Федерации, в том числе о персональных данных, поскольку в таком случае сфера его применения носила бы по существу всемирный характер и делала бы практически невозможным контроль за его исполнением. Поэтому здесь применяется критерий направленности деятельности лица на территорию Российской Федерации как условия применения законодательства РФ к отношениям с иностранным субъектом^{*(1)}.

2. В **ч. 1 ст. 1** определяются предметная сфера действия законодательства РФ о персональных данных и субъектный состав возникающих отношений. Выделяются два основных признака правоотношений:

наличие связи таких отношений с процессами обработки персональных данных;

использование средств автоматизации или иных средств, которые по своему характеру схожи с ними и позволяют осуществлять поиск персональных данных в соответствии с заданным алгоритмом.

Первый признак (квалификация выступающей объектом правоотношения информации в качестве персональных данных) законодатель раскрывает далее (в **ст. 3** комментируемого закона), давая определение понятия обработки персональных данных, охватывающее любые действия, совершаемые с ними.

Второй признак, имеющий место во всех случаях автоматизированной обработки, вызывает споры у участников правоотношений.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники. Однако стоит отметить, что не любая обработка персональных данных с помощью компьютерной техники будет автоматической. Например, составление трудового договора в MS WORD вручную не может считаться автоматизированным, хотя и

делается на компьютере.

Для разграничения автоматизированной и неавтоматизированной обработки персональных данных на нормативном уровне используется критерий участия человека в данном процессе. Подробные разъяснения по этому вопросу можно найти в [Положении](#) об особенностях обработки персональных данных, утв. [постановлением](#) Правительства от 15 сентября 2008 г. N 687.

Кроме того, второй признак имеет место при осуществлении неавтоматизированной обработки персональных данных - то есть в том случае, когда человек непосредственно осуществляет значимые действия по обработке персональных данных. Чтобы неавтоматизированная обработка персональных данных являлась предметом регулирования комментируемого закона, она должна удовлетворять в совокупности следующим условиям:

а) поиск и (или) доступ к таким данным осуществляется в соответствии с определенным алгоритмом, что предполагает наличие систематизации соответствующих документов по конкретным критериям;

б) использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных осуществляются при непосредственном участии человека независимо от того, хранятся такие сведения в информационной системе персональных данных или нет ^{*(2)}.

В подзаконных нормативных актах выделяется также смешанная обработка персональных данных. Например, в [Методических рекомендациях](#) по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения, утв. [приказом](#) Роскомнадзора от 30 мая 2017 г. N 94, упоминаются следующие способы обработки персональных данных:

неавтоматизированная обработка;

исключительно автоматизированная обработка с передачей полученной информации по сети или без таковой;

смешанная обработка.

Если деятельность по обработке персональных данных не сопряжена с использованием автоматизированных или неавтоматизированных средств обработки, удовлетворяющих условиям, то она в соответствии с [ч. 1](#) комментируемой статьи не подпадает под действие настоящего федерального закона.

Также в судебной практике сформировалась позиция, согласно которой действие комментируемого закона не распространяется на отношения по собиранию, проверке, хранению сведений в процессе возбуждения, расследования и рассмотрения уголовных дел и сам по себе закон не может ограничивать права участников уголовного процесса и заявителей о преступлениях на ознакомление с материалами уголовных дел и проверок сообщений о преступлениях (см. [определение](#) Конституционного Суда РФ от 29 сентября 2011 г. N 1251-О-О; [апелляционное определение](#) Санкт-Петербургского городского суда от 1 октября 2014 г. N 33-14325/2014 г. по делу N 2-1111/2014).

[Регламент](#) ЕС о защите персональных данных устанавливает в целом похожую фактическую сферу применения. Регламент применяется в отношении обработки персональных данных полностью либо частично при помощи автоматизированных средств, а также в отношении обработки персональных данных иными способами, которые являются частью файловой системы или которые имеют целью стать частью файловой системы.

Однако, как мы видим, [Регламент](#) о защите персональных данных напрямую закрепляет в числе прочего смешанную обработку персональных данных, а также дает, на наш взгляд, более четкое определение неавтоматизированной обработки персональных данных через понятие "файловая система", определяемое далее как любой структурированный набор персональных данных, доступных в соответствии с определенными критериями, вне зависимости от того используется ли при этом централизованный, децентрализованный, функциональный или географический принцип.

Что касается субъектного состава, то круг субъектов очерчен в комментируемой части следующим образом:

государственные органы;

муниципальные органы;

юридические лица;

физические лица.

У каждого из указанных субъектов есть свои особенности, рассмотрим их далее.

Орган государственной власти (государственный орган) - это часть государственного аппарата, наделенная государственно-властными полномочиями и осуществляющая свою компетенцию в установленном государством порядке. В соответствии со [ст. 10](#) Конституции органы государственной власти делятся на органы законодательной, исполнительной и судебной власти.

К федеральным органам государственной власти относятся:

Федеральное Собрание РФ (Совет Федерации и Государственная Дума) - федеральный орган законодательной власти;

Правительство во главе с Председателем - федеральный орган исполнительной власти. Также федеральными органами исполнительной власти считаются министерства, федеральные службы и федеральные агентства, управляемые Президентом или подведомственные и управляемые Правительством;

Верховный Суд РФ, Конституционный суд РФ, кассационные суды общей юрисдикции, апелляционные суды общей юрисдикции, верховные суды республик, краевые, областные суды, суды городов федерального значения, суды автономной области и автономных округов, районные суды, военные и специализированные суды, составляющие систему федеральных судов общей юрисдикции, а также арбитражные суды округов, арбитражные апелляционные суды, арбитражные суды субъектов РФ и специализированные арбитражные суды, составляющие систему федеральных арбитражных судов, - федеральные органы судебной власти.

Согласно **Федеральному закону** от 6 октября 1999 г. N 184-ФЗ "Об общих принципах организации законодательных (представительных) и исполнительных органов государственной власти субъектов Российской Федерации" систему органов государственной власти субъекта РФ составляют:

законодательный (представительный) орган государственной власти субъекта РФ;

высший исполнительный орган государственной власти субъекта РФ;

иные органы государственной власти субъекта РФ, образуемые в соответствии с конституцией (уставом) субъекта РФ.

К муниципальным органам как субъектам правоотношений в сфере персональных данных комментируемая часть 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). 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 (**ст. 132** Конституции).

Согласно **ст. 48** ГК юридическое лицо - это организация, которая имеет обособленное имущество и отвечает им по своим обязательствам, может от своего имени приобретать и осуществлять гражданские права и нести гражданские обязанности, быть истцом и ответчиком в суде. Юридические лица обладают правоспособностью.

Участниками правоотношений в сфере персональных данных выступают также физические лица. Такая формулировка означает, что участие в рассматриваемых правоотношениях могут принимать не только граждане Российской Федерации, но и иностранные граждане, и лица без гражданства. 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).

3. **Часть 2** комментируемой статьи устанавливает исчерпывающий перечень отношений, на которые требования настоящего федерального закона не распространяются.

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

Представляется, что установленное исключение об обработке персональных данных для личных нужд с условием о ненарушении прав субъектов персональных данных согласуется с международной юридической практикой.

В российской юридической науке понятие "личные нужды" традиционно понимается как потребности, которые существуют у самого гражданина или лиц, связанных с ним личными (например, семейными) связями, и их удовлетворение никак не связано с удовлетворением потребностей неопределенного круга третьих лиц*(3).

Например, физическое лицо может вести домашнюю адресно-телефонную книгу, где указываются фамилии, имена, отчества, даты рождения, адреса, телефоны и иные сведения о его друзьях, родных и близких, причем сейчас такие записи делаются в основном на компьютерных устройствах. В связи с этим можно предположить, что под обработку персональных данных для личных и семейных нужд будут подпадать организация и использование списка контактов в телефонах или коммуникационных сервисах, хранение писем, содержащих персональные данные, на компьютерных устройствах, и т. п. Поэтому отдельно встает вопрос о том, действует ли исключение в отношении распространения физическим лицом персональных данных третьих лиц в сети Интернет.

В европейской судебной практике исключение на такую информацию не распространяется, хотя Регламент ЕС о защите персональных данных содержит иной подход. Регламент не применяется в отношении обработки персональных данных физическими лицами в ходе осуществления исключительно личной или бытовой деятельности. Личная или бытовая деятельность может включать в себя переписку и сохранение адресов, взаимодействие через социальные сети и сетевую активность, осуществляемые в контексте такой деятельности ([п. 18 Преамбулы](#)).

В целом, решение о применении исключения об обработке персональных данных для личных нужд должно приниматься с учетом всех обстоятельств конкретного случая.

2) Отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда РФ и других архивных документов в соответствии с законодательством об архивном деле.

Данное положение является прямым следствием из [ч. 3 ст. 4](#) ФЗ "Об информации, информационных технологиях и о защите информации", согласно которой порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

Отношения в сфере организации хранения, комплектования, учета и использования документов Архивного фонда РФ 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 октября 2004 г. N 125-ФЗ "Об архивном деле в Российской Федерации", а также принимаемыми в соответствии с ним иными нормативными правовыми актами Российской Федерации и субъектов РФ.

Согласно [ФЗ](#) "Об архивном деле в РФ" архивный документ - материальный носитель с зафиксированной на нем информацией, который имеет реквизиты, позволяющие его идентифицировать, и подлежит хранению в силу значимости указанных носителя и информации для граждан, общества и государства. Таким образом, отличие данного вида правоотношений от правоотношений по обработке персональных данных заключается в том, что обработке подвергается не информация, а только отдельные виды документов как носители информации. Кроме того, обработка документов ограничена, допустимы не любые действия, а только действия по организации хранения, комплектования, учета и использования.

Однако рассматриваемое исключение не означает, что право граждан на частную жизнь никак не учитывается. В данном случае применяется специальная норма [ч. 3 ст. 25](#) ФЗ "Об архивном деле в РФ", согласно которой существует ограничение на доступ к архивным документам, содержащим сведения о личной и семейной тайне гражданина, его частной жизни, а также сведения, создающие угрозу для его безопасности.

3) Отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

Согласно [ст. 29](#) Конституции перечень сведений, составляющих государственную тайну, определяется федеральным законом. Все отношения по обработке сведений, составляющих государственную тайну (в том числе, если они могут быть отнесены к персональным данным), регулируются [Законом](#) РФ от 21 июля 1993 г. N 5485-1 "О государственной тайне".

Согласно [ст. 2](#) названного закона к государственной тайне относятся 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, указан в [ст. 3](#) Закона РФ "О государственной тайне". Следовательно, если персональные данные субъекта являются информацией, относящейся к перечню сведений, составляющих государственную тайну, их обработка осуществляется в соответствии со специальными нормами Закона о государственной тайне.

В целом [ч. 2 ст. 1](#) комментируемого закона имеет существенные отличия от аналогичных норм-исключений, установленных [Регламентом](#) ЕС о защите персональных данных. Так, Регламент не применяется в отношении обработки персональных данных:

в процессе деятельности, которая не подпадает под действие законодательства Союза; государствами - членами ЕС при осуществлении деятельности, которая подпадает под действие [Главы 2 Раздела V](#) Договора о Европейском Союзе; физическим лицом в процессе осуществления исключительно личной или бытовой деятельности;

компетентными органами в целях предупреждения, расследования, выявления уголовных преступлений, или привлечения к ответственности, или приведения в исполнение уголовных наказаний, включая защиту и предотвращение угроз общественной безопасности.

Пересечение здесь мы видим только в одном пункте, касающемся личной или бытовой деятельности, - комментарий по этому вопросу был дан нами ранее. При этом обращает на себя внимание вынесенное в отдельный пункт исключение, касающееся предупреждения, расследования, выявления уголовных преступлений. В отечественном законодательстве о персональных данных аналогичное исключение также присутствует, но выражено в несколько другой форме. Так, согласно [п. 3 ч. 1 ст. 6](#) комментируемого закона обработка персональных данных допускается, если она осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах.

4. Предоставление, распространение, передача и получение информации о деятельности судов в Российской Федерации, содержащей персональные данные, ведение и использование информационных систем и информационно-телекоммуникационных сетей в целях создания условий для доступа к указанной информации осуществляются в соответствии с [Федеральным законом](#) от 22 декабря 2008 года N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации".

[Часть 3](#) рассматриваемой статьи введена в комментируемый закон [Федеральным законом](#) от 29 июля 2017 г. N 223-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации", принятым с целью обеспечить наличие судебной информации в сети Интернет, включая тексты судебных актов. Также этим законом признан утратившим силу [п. 5 ч. 2](#) комментируемой статьи, согласно которому на отношения, связанные с предоставлением уполномоченными органами информации о деятельности судов в Российской Федерации, не распространялось действие настоящего федерального закона.

Вместе с данными изменениями [Федеральный закон](#) от 29 июля 2017 г. N 223-ФЗ перенес часть норм, связанных с персональными данными, в Федеральный закон от 22 декабря 2008 г. N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации". В частности, согласно [ч. 4 ст. 15](#) указанного федерального закона персональными данными применительно к судебным актам являются:

1) фамилии, имена и отчества участников судебного процесса, дата и место рождения, место жительства или пребывания, номера телефонов, реквизиты паспорта или иного документа, удостоверяющего личность, ИНН - физического лица, основной государственный регистрационный номер индивидуального предпринимателя, страховой номер индивидуального лицевого счета;

2) сведения о месте нахождения земельного участка, здания, сооружения, жилого дома, квартиры, транспортного средства, иные сведения об имуществе и о находящихся в банках или иных кредитных организациях денежных средствах участников судебного процесса, если эти сведения относятся к существу дела.

При размещении в сети Интернет эти персональные данные исключаются из текстов судебных актов, принятых судами общей юрисдикции, Верховным Судом РФ.

[Статья 2](#). Цель настоящего Федерального закона

Комментируемая [статья](#) определяет целевые ориентиры настоящего федерального закона - обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Данная формулировка похожа на закрепленную в ныне отмененной [Директиве](#) Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных.

Однако Регламент ЕС о защите персональных данных, определяя цели законодательства о персональных данных, идет уже по другому пути. Целью данного Регламента является содействие формированию пространства свободы, безопасности и правосудия и экономического союза, содействие экономическому и социальному прогрессу, укреплению и сближению экономик в рамках внутреннего рынка, а также содействие благосостоянию физических лиц. Практически то же самое закреплено и в его [ст. 1](#): Регламент защищает основные права и свободы физических лиц и, в частности, право на защиту персональных данных. Таким образом, Регламент более не связывает персональные данные с защитой прав на неприкосновенность частной жизни, личную и семейную тайну.

Однако, поскольку в отечественном законодательстве смены позиции по этому вопросу не произошло, персональные данные необходимо рассматривать во взаимосвязи с категориями "частная жизнь", "личная и семейная тайны". Право на неприкосновенность частной жизни, личную и семейную тайну закреплено в [ст. 23](#) Конституции. Комментируемый закон является логическим продолжением Конституции в части детальной регламентации нормы о правах субъекта персональных данных. Кроме того, с учетом трансграничности потоков информации, в том числе персональных данных, законодатель обеспечил имплементацию в российское законодательство требований общеевропейского права.

Само понятие "частная жизнь" ("privacy") трактуется в контексте европейского права весьма

широко. Так, в [постановлении](#) Европейского Суда по делу "Перри против Соединенного Королевства" от 17 июля 2003 г. дается следующее заключение: "Частная жизнь - понятие, не предоставляющее возможности для исчерпывающего определения. Такие аспекты, как половая принадлежность, имя, сексуальная ориентация и сексуальная жизнь, являются важнейшими элементами частной сферы...". Однако в постановлении Европейского Суда по [делу](#) "Нимитц против Германии" от 16 декабря 1992 г. говорится, что "не следует ограничивать ее [частную жизнь] интимным кругом, в котором каждый может жить своей собственной личной жизнью... и тем самым полностью исключать внешний мир из этого круга"*[\(4\)](#).

Поскольку Российская Федерация ратифицировала Конвенцию о защите прав человека и основных свобод ETS N 005 от 4 ноября 1950 г., надо учитывать и ее нормы ([ст. 8](#), гарантирующую право на уважение частной и семейной жизни), а также позицию ЕСПЧ в этом вопросе. Последняя имеет ряд особенностей:

1) ЕСПЧ рассматривает положения [ст. 8](#) Конвенции о защите прав человека и основных свобод применительно и к современным технологиям (электронной почте, GPS-технологиям, видеонаблюдению и пр.).

Например, в [деле](#) S. and Marper v. United Kingdom ЕСПЧ констатировал нарушение [ст. 8](#) Конвенции в случае бессрочного хранения в электронной базе данных отпечатков пальцев и образцов ДНК заявителей, а в [постановлении](#) по делу Copland v. United Kingdom по делу, касающемуся мониторинга работодателями электронной почты сотрудников и использования ими Интернета на рабочем месте, ЕСПЧ усмотрел нарушение ст. 8 Конвенции *[\(5\)](#).

2) Позиция ЕСПЧ по поводу дефиниции понятия "частная жизнь" в целом похожа на существующую в отечественной доктрине: категория "частная жизнь" не имеет юридического содержания, а правовое регулирование лишь устанавливает пределы ее неприкосновенности ("приватности"). ЕСПЧ не дает точного определения понятию, а устанавливает расширительное его толкование, включая туда сексуальную жизнь индивидов; физическую и психологическую неприкосновенность индивида при оказании ему медицинской помощи или психиатрическом обследовании; право индивида знать свое происхождение; личную физическую и психологическую неприкосновенность и др.

3) ЕСПЧ подчеркивает, что право на частную жизнь не ограничивается обязанностью государства воздерживаться от такового вмешательства, но распространяется и на отношение лиц между собой (см., например, [постановление](#) ЕСПЧ от 24 июня 2004 г. по делу Фон Ганновер (Принцесса Ганноверская) (Von Hannover) против Германии, жалоба N 59320/00, связанному с публикацией фотографий повседневной жизни). Как следствие, горизонтальные отношения между частными лицами (операторами и субъектами персональных данных по поводу личной информации) вполне являются объектом обязанности государства по обеспечению права на частную жизнь в понимании ЕСПЧ.

Таким образом, категория "частная жизнь" в решениях ЕСПЧ представляется достаточно объемной и предусматривает широкий спектр прав и свобод, подпадающих под сферу защиты указанного права.

В законодательстве Российской Федерации понятие частной жизни достаточно полно отражает позицию ЕСПЧ, особенно в части расширительного толкования данной дефиниции, и представляет собой сведения:

- о сексуальной ориентации или сексуальной жизни;
- о психосоциальном типе личности;
- профессионального или делового характера;
- медицинского характера;
- о смене пола;

о личной или профессиональной жизни лица, и иные сведения, круг которых определяется национальными и международными нормами права*[\(6\)](#).

Например, в [п. 2.2](#) определения Конституционного суда от 16 февраля 2006 г. N 63-О "Об отказе в принятии к рассмотрению жалобы гражданина Кузнецова А.Н. на нарушение его конституционных прав отдельными положениями статей 89, 121, 123, 125 и 131 Уголовно-исполнительного кодекса РФ" дается следующее определение: "Частная жизнь - сфера жизни, которая относится к отдельному лицу, касается только этого лица и, если его действия носят непротивоправный характер, не подлежит контролю со стороны общества и государства"*[\(7\)](#).

Несмотря на то, что согласно комментируемой статье персональные данные необходимо рассматривать во взаимосвязи с категорией "частная жизнь", следует помнить о том, что эти понятия не тождественные: законодательство о персональных данных не в полной мере охватывает ситуации, которые подпадают под действие права на неприкосновенность частной жизни. Например, согласно [ст.](#)

1 комментируемого закона он не регулирует отношения, связанные с обработкой данных, которые в том числе могут составлять личную или семейную тайну, если такая обработка не осуществляется с использованием средств автоматизации или приравненных к ним, но при этом лицо не лишено возможности защищать свои права в порядке, установленном [гл. 8 ГК](#).

В то же время некоторые ситуации, связанные с обработкой персональных данных, выходят за рамки права на неприкосновенность частной жизни. Так, законодательство о персональных данных в круг регулируемых информационных отношений включает отношения по поводу публичной и общедоступной информации, которая по своей природе не может являться личной или семейной тайной. Если изобразить их на диаграммах Эйлера, то это будут два пересекающихся, но не совпадающих круга, каждый из которых не поглощает другой.

Даже сама формулировка комментируемой статьи не ограничивает цели настоящего федерального закона защитой прав на неприкосновенность частной жизни. К иным правам и свободам человека, связанным с обработкой персональных данных, можно отнести упоминаемое в [ч. 2 ст. 23](#) Конституции право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений и закрепленное [ч. 2 ст. 24](#) Конституции право лица требовать от органов государственной власти и органов местного самоуправления, их должностных лиц обеспечения возможности ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Кроме того, закрепление в комментируемой статье его целей является одним из приемов юридической техники, согласно которому в целях обозначаются ориентиры правового регулирования общественных отношений (в рассматриваемом случае это обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных) и конечные результаты, на достижение которых направлено правовое регулирование (то есть достижение личной безопасности граждан или отсутствие потенциально и реально существующих угроз этой безопасности). Соответственно, на решение этой задачи должно быть направлено не только законодательное регулирование, но и деятельность всех государственных институтов. Обеспечивая защиту персональных данных, Российская Федерация тем самым создает благоприятную обстановку для всестороннего развития граждан и общества в целом.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

Комментируемая [статья](#) устанавливает перечень основных понятий, которые составляют основу системы законодательства в области защиты персональных данных. Подобного рода статьи, имеющиеся во многих нормативных правовых актах, преследуют обычно цель по устранению неправильного толкования законодательных положений в процессе правоприменения. Однако в рассматриваемом случае присутствует и стремление к правовому единообразию, способствующему осмыслению лежащих в основе защиты персональных данных технологий и построению на крепком терминологическом фундаменте механизмов правового регулирования. Конечно, попытки сформировать терминологическую базу, в целом, можно оценить положительно, хотя некоторые из определений сами по себе вызывают много вопросов.

В европейском законодательстве так же присутствуют аналогичные нормативные конструкции. В Регламенте ЕС о защите персональных данных она представлена в [ст. 4](#), в Директиве ЕС о защите физических лиц при обработке персональных данных компетентными органами - в [ст. 3](#). Сами же дефиниции по составу и содержанию в двух названных документах очень похожи^{*(8)}, а вот от российского законодательства сильно отличаются.

1) Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Безусловно, это данное понятие является ключевым для данного нормативного акта. Так же ему принадлежит и решающее значение в системе представленных терминов, поскольку именно с ним связываются в дальнейшем вопросы о правах и обязанностях субъектов регулируемых отношений, а также вопросы ответственности.

Данная в комментируемой статье дефиниция имеет ряд особенностей. Понятие персональных данных традиционно привязывается к физическим лицам, не распространяясь на юридических лиц. Определяя персональные данные как любые сведения, независимо от формы их представления, законодатель тем самым предоставляет открытый перечень таковых сведений.

Закон также не содержит полномочий по уточнению этого термина подзаконными актами. С одной стороны, это предоставляет субъектам рассматриваемых отношений возможность расширения перечня по мере изменения социального статуса их обладателя, с другой - вызывает множество вопросов относительно того, какая информация относится к персональным данным, а какая нет.

Обычно к персональным данным относят:

- фамилию, имя, отчество субъекта (физического лица);

- дату рождения;
- место постоянного (временного) проживания;
- любые данные о семейном, финансовом положении;
- любые данные, связанные с родом деятельности, заработком, образованием;
- данные паспорта и других документов;
- финансовую информацию и т. п.

Однако, согласно разъяснениям Роскомнадзора, здесь существуют нюансы. Например, само по себе имя или даже имя, фамилия, отчество не будут являться персональными данными в том смысле, который вкладывается в это понятие в рамках законодательства, - только если по данным возможно прямо или косвенно определить конкретную личность, они будут являться персональными данными^{*(9)}.

Необходимо помнить о том, что состав персональных данных неоднороден, при этом ответственность за действия с разными категориями персональных данных различна, равно как и ответственность тех, кто их обрабатывает. Персональные данные разделяются по разным критериям, в частности по степени информативности. Например, существуют наборы информации, позволяющие только идентифицировать субъекта (фамилия, имя и дата рождения или адрес и сведения о заработках). Есть специальные категории персональных данных, включающие в себя информацию о национальной и расовой принадлежности субъекта, о религиозных либо философских убеждениях, информацию о здоровье и интимной жизни субъекта, судимости и пр.^{*(10)}

Также существуют общедоступные и обезличенные персональные данные. На них стоит обратить особое внимание. Общедоступные персональные данные, в соответствии с законодательством, не подлежат сокрытию или защите. В качестве таковых традиционно приводят сведения о доходах представителей органов государственной и муниципальной власти либо персональные данные, доступ к которым предоставлен с разрешения самого субъекта. К последним относятся и пользователи социальных сетей - субъект размещает в открытом доступе на своей странице ту информацию о себе, которую считает необходимой. И даже если такая страница является закрытой, это не меняет статуса предоставляемых на ней сведений о субъекте, и возникают казусы, так как, по сути, на закрытых аккаунтах информация не предоставляется в свободный доступ.

Сеть Интернет вообще ставит много вопросов в плане регулирования персональных данных, в том числе и с точки зрения того, какие сведения входят в состав персональных данных. Так, вопросы вызывают такие данные, как IP-адрес, электронный ящик, номер телефона, фотографии и видео субъекта, и прочие сведения.

По сути комментируемого [закона](#), номер телефона можно причислить к персональным данным, так как с его помощью достаточно легко идентифицировать абонента, хотя и используя дополнительные средства. По аналогии к персональным данным можно отнести и адрес электронного ящика (хотя, если в адресе не фигурирует Ф. И. О. субъекта, такая информация считается обезличенной). Логины и пароли не входят в категорию персональных данных^{*(11)}.

Что же касается IP-адреса, то единой позиции тут нет. С одной стороны, IP-адрес характеризует только точку доступа к сети. С другой стороны, по нему можно определить не только место нахождения точки доступа, но и лицо, которое выходило в сеть Интернет. Учитывая сказанное, целесообразно признавать IP-адрес персональными данными^{*(12)}.

Фотографии (видео) являются персональными данными, только если с их помощью можно установить личность субъекта. Однако это все еще остается спорной позицией Роскомнадзора. Тем не менее в одном из дел было установлено, что для использования фотографии для оформления пропуска в бассейн необходимо получить согласие гражданина на получение его персональных данных^{*(13)}.

Обезличенными персональными данными является информация, по которой невозможно определить ее принадлежность к конкретному физическому лицу. Такие данные могут быть зашифрованы, содержать код или идентификатор, наиболее часто такой метод используется в медицинских системах, в статистической отчетности и пр.^{*(14)}

Таким образом, данный в комментируемом законе подход к определению персональных данных вызывает большое количество вопросов по их составу. В пояснениях к комментируемой дефиниции, данных на официальном портале Минцифры, говорится о том, что понятие, содержащееся в [п. 1](#) комментируемой статьи, соответствует международному праву и точно определить состав персональных данных, в том числе привести их перечень, представляется нереализуемым^{*(15)}.

Однако в свете данной в [Регламенте](#) ЕС о защите персональных данных дефиниции это не совсем так. Определение звучит следующим образом: "под термином "персональные данные" понимается любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу ("субъект данных"); идентифицируемое лицо - это лицо, которое может быть идентифицировано, прямо или косвенно, в частности, посредством таких идентификаторов как имя, идентификационный номер, сведения о местоположении, идентификатор в режиме онлайн или через

один или несколько признаков, характерных для физической, психологической, генетической, умственной, экономической, культурной или социальной идентичности указанного физического лица".

То есть это определение содержит не только похожие положения (первая часть его идентична российской норме), но и приводит перечень категорий сведений, которые можно отнести к персональным данным, снижая тем самым вероятность различных толкований.

1.1) Персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим федеральным законом.

Субъект персональных данных или его законный представитель вправе дать согласие на обработку персональных данных в любой позволяющей подтвердить факт его получения форме, если иное не установлено законом (см. [комментарий](#) к ст. 9).

По общему правилу согласие может быть дано в любой верифицируемой форме, например, согласие в устной форме валидно лишь при условии его аудиальной или видеоаудиальной фиксации. Однако применительно к специальным категориям персональных данных (см. [комментарий](#) к п. 1 ч. 2 ст. 10), биометрических данных (см. [комментарий](#) к ч. 1 ст. 11), а также при трансграничной передаче персональных данных (см. [комментарий](#) к п. 1 ч. 4 ст. 12) согласие субъекта персональных данных должно быть дано исключительно в письменной форме:

на бумажном носителе с собственноручной подписью субъекта;

или в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Письменное согласие субъекта персональных данных на бумажном носителе должно включать в себя следующие реквизиты:

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

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

- наименование или 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;

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

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

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

- подпись субъекта персональных данных.

Об особенностях обработки персональных данных, разрешенных субъектом персональных данных для распространения, см. [комментарий](#) к ст. 10.1.

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

Согласно комментируемому закону субъектами в отношениях, связанных с персональными данными, являются:

- владельцы персональных данных;

- операторы персональных данных;

- орган по защите прав субъектов персональных данных.

Стоит отметить, что категория "оператор персональных данных" не создает нового субъекта общественных отношений по обработке персональных данных. Понятие "оператор" представляет своего рода обезличенной категорией, позволяющей сосредоточиться не на организационно-правовой форме организаций, которые по роду деятельности связаны со сбором, накоплением, хранением, обработкой и передачей персональных данных, а лишь на выполняемых ими функциях. Придерживаясь

избранного направления, законодатель считает оператором любое лицо, работающее с информационной системой персональных данных, независимо от оснований получения доступа к работе с последней.

Положения федерального законодательства распространяются на всех вышеуказанных субъектов. Принятый федеральный закон не распространяет **ч. 5 ст. 18** комментируемого закона только на операторов, для которых обработка персональных данных является основным видом деятельности, либо на операторов, обрабатывающих персональные данные только с использованием информационно-телекоммуникационных сетей. Кроме того, принимая во внимание, что **ст. 3** настоящего федерального закона не содержит исключений в части осуществления лицом отдельных операций по обработке персональных данных, а равно иных определений, отличных от оператора, лицо, определяющее цель обработки персональных данных либо осуществляющее отдельные действия по обработке персональных данных, в контексте положений настоящего федерального закона является оператором, осуществляющим обработку персональных данных (пояснения к комментируемой дефиниции, данные на официальном портале Минцифры*(16)).

Таким образом, операторами персональных данных могут считаться:

- нотариусы и нотариальные конторы;
 - любые организации, которые нанимают работников по трудовым договорам, договорам гражданско-правового характера;
 - государственные и муниципальные учреждения, ведомства и службы;
 - органы судебной власти;
 - страховые компании;
 - операторы сотовой связи;
 - образовательные организации;
 - медицинские организации;
 - интернет-магазины;
 - банки и финансовые организации и т. п.
- Оператор имеет право определять:
- цели обработки персональных данных;
 - состав персональных данных, подлежащих обработке;
 - действия (операции), совершаемые с персональными данными.

Однако это не означает произвольности сбора персональных данных. Оператору нельзя требовать от субъектов персональных данных сведений сверх того, чем это нужно для какой-то конкретной цели. При этом храниться персональные данные могут не дольше, чем этого требуют цели, для которых они накапливались. Кроме того, операторы персональных данных обязаны гарантировать конфиденциальность информации и предоставить гражданину право самостоятельно решать, какую информацию и в каком объеме он готов раскрывать.

Европейский законодатель (см. **Регламент** ЕС о защите персональных данных) идет при определении субъектов отношений по поводу персональных данных по другому пути, не вводя единого унифицированного субъекта. Более того, разные субъекты, обрабатывающие персональные данные, выделяются по разным основаниям:

- по выполняемым функциям:

"(7) под термином "контролер" понимается физическое или юридическое лицо, органы государственной власти, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и способы обработки персональных данных; <...>

(8) под термином "обрабатывающее данные лицо" понимается физическое или юридическое лицо, органы государственной власти, агентство или иной орган, который обрабатывает персональные данные от имени контролера;

(9) под термином "получатель" понимается физическое или юридическое лицо, органы государственной власти, агентство или иной орган, которому раскрываются персональные данные, вне зависимости от того, является ли он третьим лицом или нет <...>;

(10) под термином "третья сторона" понимается физическое или юридическое лицо, органы государственной власти, агентство или орган, отличный от субъекта данных, контролера, обрабатывающего данные лица или лиц, которые уполномочены проводить обработку персональных данных под непосредственным руководством контролера или обрабатывающего данные лица";

- по организационно-правовой форме:

"(16) под термином "основное учреждение" понимается:

(а) в отношении контролера с учреждениями в нескольких государствах-членах ЕС, месторасположение его центральной администрации в Союзе, кроме случаев, когда решения о целях и способах обработки персональных данных принимаются в другом учреждении контролера в Союзе, и последнее учреждение обладает правом на имплементацию указанных решений, в этом случае

учреждение, принимающее такие решения, должно рассматриваться в качестве основного учреждения;

(b) в отношении лица, обрабатывающего данные, с учреждениями в нескольких государствах-членах ЕС, месторасположение его центральной администрации в Союзе, или, если лицо, обрабатывающее данные, не имеет центральной администрации в Союзе, учреждение указанного лица в Союзе, где производится основная обработка в контексте деятельности учреждения лица, обрабатывающего данные, в той степени, в какой указанное лицо ограничено специальными обязательствами в соответствии с настоящим [Регламентом](#);

(17) под термином "представитель" понимается физическое или юридическое лицо, учрежденное в Союзе, которое в письменной форме назначается контролером или лицом, обрабатывающим данные, в соответствии со [Статьей 27](#) и представляет контролера или лицо, обрабатывающее данные, с учетом их соответствующих обязательств согласно настоящему Регламенту;

(18) под термином "компания" понимается физическое или юридическое лицо, участвующее в экономической деятельности, вне зависимости от организационно-правовой формы, в том числе товарищества или объединения, регулярно участвующие в экономической деятельности;

(19) под термином "группа предприятий" понимается контролирующее предприятие и подконтрольные ему предприятия".

Анализ приведенных определений позволяет констатировать, что в целом понятие оператора персональных данных распадается в [Регламенте](#) ЕС о защите персональных данных на два отдельных субъекта:

- Data controller - контролер данных - физическое или юридическое лицо, государственный орган, учреждение или другой орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных, - то есть фактически это субъект, который решает, "что" и "как" можно делать с персональными данными в целях обработки, независимо от его организационной структуры (например, социальная сеть или служба такси);

- Data processor - процессор данных, "обрабатывающее данные лицо" - это физическое или юридическое лицо, государственный орган, учреждение или другой орган, который обрабатывает персональные данные от имени по поручению контролера. Понятие включает в себя широкий круг субъектов, в том числе физических или юридических лиц, государственных органов, агентств или других организаций (например, поставщик облачных услуг). Существование процессора зависит от решения, принятого контроллером, который может решить выполнить определенные операции обработки самостоятельно или делегировать всю или часть обработки процессору.

Согласно пояснениям "EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) [2018/1725](#)"*(17) такое разделение вводится для распределения ответственности там, где есть фактическое и формальное влияние или использование персональных данных.

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

Содержание термина "обработка персональных данных" законодатель предусматривает достаточно объемным. В частности, в него включаются прямо перечисленные в определении действия:

- сбор;
- запись;
- систематизация;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передача (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

Однако представляется, что используемая законодателем конструкция "любое действие (операция) или совокупность действий (операций)" означает, что этот перечень составляющих ее действий (операций) не является исчерпывающим.

Часть из данных в законе действий в дальнейшем раскрывается в отдельных определениях, часть

остается без пояснений. Анализ тех дефиниций, которые присутствуют в комментируемом законе, можно объяснить тем, что процесс обработки персональных данных можно условно разделить на две стадии: формирование информационной системы персональных данных и последующие операции с ними с использованием средств автоматизации или без их применения. В отношении каждой из представленных стадий действуют свои правовые механизмы, регулирующие поэтапную процедуру ее реализации.

Отдельные термины впоследствии поясняются регулятором, например, что понимается под сбором персональных данных в контексте требований закона. В целях толкования под сбором персональных данных можно понимать "документально оформленную процедуру получения оператором от субъекта его персональных данных, для их последующей обработки в соответствии с заявленными целями сбора. Схожее определение содержится в [ст. 2](#) Модельного закона о персональных данных, принятого на XIV пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ постановлением от 16 октября 1999 года N 14-19 (Сбор персональных данных - документально оформленная процедура получения держателем персональных данных от субъектов этих данных)"*(18).

Также стоит отметить, что, в зависимости от отрасли права, при обработке персональных данных могут возникать характерные для отрасли проблемы, которые урегулируются нормами отраслевых кодексов или разъяснениями регулятора.

Так, [ст. 86](#) ТК устанавливаются общие требования при обработке персональных данных работника и гарантии их защиты, например, необходимость руководствоваться [Конституцией](#), ТК и иными федеральными законами при определении объема и содержания обрабатываемых персональных данных работника и др.

В деятельности учебных учреждений так же возникали проблемы, связанные с порядком обработки образовательными организациями персональных данных обучающихся при предоставлении государственной услуги по ведению электронных дневников и журналов в случае отказа законных представителей несовершеннолетних предоставить согласие на обработку персональных данных. Роскомнадзор в своем отчете за 2014 год дал разъяснение, что в случае оказания услуги по ведению электронных дневников и журналов посредством Единого портала государственных и муниципальных услуг согласия субъекта персональных данных на обработку данных не требуется*(19).

Хочется также отметить, что в рамках теоретических работ организация защиты персональных данных только с точки зрения их обработки называется основной проблемой федерального законодательства о персональных данных, поскольку такой подход сужает область защиты, исключая из нее, например, наложение и снятие конфиденциальности, хранение сведений для аутентификации и идентификации пользователей цифровых порталов и др.*(20)

[Регламент](#) ЕС о защите персональных данных содержит по данному вопросу полностью аналогичную конструкцию.

Под термином "обработка" понимается любая операция или набор операций, осуществляемых с персональными данными, с применением автоматизированных средств или без таковых, например сбор, запись, организация, структурирование, хранение, модификация и изменение, извлечение, консультирование, использование, раскрытие посредством передачи, распространение или предоставление иным способом, упорядочение или комбинирование, ограничение, стирание или разрушение.

Несмотря на то, что набор операций с персональными данными отличается, в разъяснениях говорится, что данный параграф содержит только примеры действий с персональными данными, а не полный список операций. При этом доступ к персональным данным также относится к обработке, как и предоставление такого доступа*(21).

В приведенном определении отсутствует упоминание цели, но по сути под обработкой понимаются действия (операции), объединенные одной целью.

4) Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Вопрос автоматизированной обработки персональных данных поднимался и подробно рассматривался нами в [комментарии](#) к [ст. 2](#), где был сделан вывод о том, что для разграничения автоматизированной и неавтоматизированной обработки персональных данных на нормативном уровне используется критерий участия человека в данном процессе (подробные разъяснения по этому вопросу можно найти в [Положении](#) об особенностях обработки персональных данных, утв. [постановлением](#) Правительства от 15 сентября 2008 г. N 687).

Стоит отметить, что подобного термина в [ст. 4](#) Регламента ЕС о защите персональных данных нет, равно как и терминов, закрепленных [пп. 5-10](#) комментируемой статьи. Последнее связано с тем фактом, что в Регламенте ЕС не используются уточняющие определения по отдельным способам обработки персональных данных.

5) Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Исходя из [п. 9 ст. 2](#) ФЗ "Об информации, информационных технологиях и о защите информации" распространение информации представляет собой действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

На сегодняшний день в качестве основных форм распространения персональных данных можно выделить, пожалуй, две:

- обнародование в средствах массовой информации;
- размещение в информационно-телекоммуникационных сетях.

В первом случае возникает большое количество спорных ситуаций. Для начала уточним, что в соответствии со [ст. 2](#) Закона РФ от 27 декабря 1991 г. N 2124-1 "О средствах массовой информации" под средством массовой информации понимается периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием (названием). Именно с ними законодатель в первую очередь связывает процесс распространения информации, и именно СМИ часто публикуют информацию о личной жизни граждан.

Естественно, что и большая часть конфликтных ситуаций, возникающих при неправомерном распространении персональных данных, составляют споры со СМИ.

Пример: управление Роскомнадзора по Пермскому краю и прокуратура г. Добрянка Пермского края провели совместную проверку по факту публикации в газете "Камские зори" списка граждан, вызываемых на призывную комиссию, а также списка граждан, оповещенных и не прибывших на медицинскую и призывную комиссии. В списках содержались персональные данные призывников.

В результате проверки установлено, что действия газеты противоречат требованиям [ч. 1 ст. 6](#) и [ч. 1 ст. 7](#) комментируемого закона. В связи с этим органом прокуратуры в отношении Муниципального учреждения "Редакция газеты Добрянского муниципального района "Камские зори" возбуждено дело по [ст. 13.11](#) КоАП, а управление Роскомнадзора по Пермскому краю вынесло газете предупреждение о недопустимости злоупотребления свободой массовой информации*(22).

В более серьезных случаях, например при неоднократных нарушениях законодательства о персональных данных, по постановлению Верховного суда РФ Роскомнадзор вправе принять решение о закрытии СМИ.

Пример: одна из газет Краснодарского края несколько раз опубликовала не только имя и фамилию несовершеннолетней, но и номер школы, в которой она обучается. После получения письменного предупреждения ведомства публикация персональных данных несовершеннолетних, нарушающая в том числе [Закон](#) РФ от 27 декабря 1991 г. N 2124-1, не прекратилась. Решением краевого суда деятельность газеты была прекращена, Верховный суд РФ в [определении](#) N 18-АПГ15-7 счел нарушение существенным, а это решение правомерным*(23).

Что же касается сети Интернет, то отношения, связанные с обработкой персональных данных в ней, также регулируются положениями комментируемого закона. Основным органом, который отслеживает факты нарушения прав субъектов персональных данных в Интернете, является Роскомнадзор. В частности, ответ на вопрос "Что делать, если мои персональные данные размещены на сайтах в сети Интернет без моего согласия?" присутствует в числе ответов на часто задаваемые вопросы на сайте ведомства. В данном случае рекомендуется предоставить в адрес Управления Роскомнадзора соответствующее обращение, указав максимально полную информацию об обстоятельствах нарушения прав (единовременно). Кроме того, присутствует и рекомендация при размещении персональных данных в публичных сообществах социальных сетей разграничивать вопросы защиты персональных данных и защиты чести, достоинства и деловой репутации*(24).

Полномочий Роскомнадзора по защите прав субъектов персональных данных достаточно много:

- запрашивать у информационного посредника документы, подтверждающие осуществление деятельности по обработке персональных данных в соответствии с требованиями законодательства в области персональных данных;
- направлять требование об удалении размещенной информации о персональных данных;
- блокировать ресурс и др.

Более того, [постановление](#) Правительства от 13 ноября 2019 г. N 1443 "О внесении изменения в Правила создания, формирования и ведения автоматизированной информационной системы "Реестр нарушителей прав субъектов персональных данных" предписывает операторам связи блокировать

нарушителей закона о защите персональных данных незамедлительно после получения уведомления Роскомнадзора^{*(25)}.

б) Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Предоставление персональных данных от их распространения отличается масштабом раскрытия персональных данных: в случае распространения информация раскрывается неопределенному кругу лиц, при предоставлении - определенному лицу или определенному кругу лиц.

Несмотря на то, что в случае предоставления персональных данных круг лиц ограничен, здесь так же возникает ряд практических вопросов.

Во-первых, это вопросы, связанные с предоставлением персональных данных по запросу государственных органов. Иногда операторы, во избежание рисков получения предписания от Роскомнадзора, отказывают в их передаче государственным органам, в том числе и ФАС. В одном из таких случаев ФАС запросила у оператора мобильной связи информацию о владельце телефонного номера, с которого поступали многочисленные рекламные сообщения. За отказ предоставить персональные данные организация была оштрафована. Суд счел, что ФАС действовал в соответствии с законом, а оператор связи обязан был предоставить запрошенные персональные данные.

Во-вторых, существует множество дел, связанных с предоставлением персональных данных банками.

Пример: Ростовским областным судом было рассмотрено дело по иску о предоставлении информации и взыскании морального вреда. Обстоятельства дела: истец получил кредитную карту в банке, далее банк сделал переуступку прав требования, новый банк направил истцу уведомление о необходимости явиться в офис банка для подписания документов. Владельца персональных данных смутило, что новый банк от него не получил согласия на обработку персональных данных, в связи с чем истец направил в банк заявление о предоставлении ему информации, связанной с его персональными данными.

В данном случае решение было вынесено в пользу первого банка в силу грамотно составленного согласия на обработку персональных данных, в котором было указано, что одной из целей обработки является сбор задолженности в случае передачи банком третьим лицам функций и (или) полномочий по обслуживанию кредита и сбору задолженности на основании заключаемых банком договоров с данными лицами^{*(26)}.

В Роскомнадзор поступают и жалобы в отношении кредитных учреждений на действия, связанные с передачей персональных данных без согласия клиентов. Граждане жалуются, что их данные незаконно передаются иным третьим лицам и не уничтожаются банками в случае отзыва согласия на обработку данных.

Роскомнадзор в данном случае поясняет, что зачастую отзыв согласия на обработку персональных данных не является основанием для прекращения обработки банками персональных данных при наличии существующих договорных отношений. Российское законодательство в области персональных данных предоставляет банкам право обрабатывать персональные данные граждан на основании заключенного договора, а также реализовывать свое право на взыскание задолженности в рамках агентской схемы и уступки права требования по кредитному договору (цессия).

Что же касается работодателей как операторов персональных данных, то здесь присутствуют также нормы ТК. В частности, в [ст. 88](#) ТК устанавливаются следующие требования к порядку передачи персональных данных работника:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных [ТК](#) или иными федеральными законами;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном [ТК](#) и иными федеральными законами;

- осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работников в порядке, установленном [ТК](#) и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

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

Термин "блокирование" применительно к персональным данным в отечественной практике впервые введен комментируемым законом, но до того уже использовался применительно к данным в [гл. 28 УК "Преступления в сфере компьютерной информации"](#). При этом нормативной дефиниции понятия "блокирование" УК не дает, что неоднократно подвергалось критике со стороны научного сообщества. Авторы комментариев к данной главе УК вынуждены были приводить самые разные определения:

- блокирование информации - отсутствие возможности доступа к информации или к ее части [*\(27\)](#);

- блокирование информации - создание условий, при которых возникает постоянная или временная невозможность осуществления блокируемой информацией своих функций [*\(28\)](#);

- блокирование - это совершение действий, приводящих к ограничению или закрытию правомерного доступа к компьютерной информации и не связанных с ее уничтожением [*\(29\)](#);

- блокирование информации - это невозможность ее использования при сохранности такой информации [*\(30\)](#).

Последнее определение кажется наиболее удачным с точки зрения передачи самой сути процесса блокирования и его отличия от процесса уничтожения.

В комментируемом законе законодатель определил блокирование персональных данных похоже по сути, а именно через временное прекращение каких-либо действий с персональными данными, подразумевая при этом, что персональные данные сохраняются. Косвенно подтверждает это [ч. 2 ст. 21](#) комментируемого закона, устанавливающая, что блокирование - обратимая операция, оно может быть снято.

8) Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Существует ряд ситуаций, когда оператор обязан прекратить обработку персональных данных: заблокировать или уничтожить их.

Законом установлены случаи, когда оператор обязан уничтожить персональные данные:

- владелец персональных данных требует уничтожить их ([ч. 3 ст. 20](#) комментируемого закона).

Срок уничтожения - 7 рабочих дней с момента поступления требования.

Здесь стоит вспомнить все те дела, в которых финансовыми организациями использовались данные потенциальных клиентов в случае отказа в кредитовании.

Пример: истец пришла в магазин бытовой техники, где намеревалась купить товар в кредит, обратилась к кредитному менеджеру, предоставила все необходимые документы, менеджер внес в базу данные истца. Истец, не дождавшись ответа из банка, отказалась от заключения договора, но с того времени ей постоянно поступают звонки из банка с требованием погасить задолженность по кредиту.

Суд удовлетворил требования истца, установив, что у банка не было законных оснований на обработку персональных данных истца (см. [апелляционное определение](#) Новосибирского областного суда от 18 июля 2017 г. по делу N 33-6839/2017).

Согласно обзорам практики Роскомнадзора это не единичный случай;

- оператор самостоятельно обнаружил, что неправомерно обрабатывает персональные данные ([ч. 3 ст. 21](#) комментируемого закона). Срок уничтожения - 10 рабочих дней с момента выявления оператором такого нарушения;

- достигнуты цели обработки персональных данных ([ч. 4 ст. 21](#) комментируемого закона). Срок уничтожения - 30 дней с момента достижения цели;

- владелец персональных данных отзывает согласие на обработку его персональных данных ([ч. 5 ст. 21](#) комментируемого закона). Срок уничтожения - 30 дней с момента поступления отзыва, если для

целей обработки данные больше не нужно сохранять.

Существует и исключение: если достигнуты цели обработки или владелец персональных данных отзывает их, оператор имеет право не уничтожать данные, если иное предусмотрено в заключенном сторонами договоре (соглашении) либо оператором осуществляется обработка персональных данных на законных основаниях без согласия субъекта персональных данных.

Это другая сторона взаимодействия, которую так же можно проиллюстрировать на примере хранения банками персональных данных клиентов после прекращения договорных отношений. Тут позиция Роскомнадзора отличается от приведенной выше.

В соответствии с [п. 1 ч. 1 ст. 7](#) Федерального закона от 7 августа 2011 г. N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" организации, осуществляющие операции с денежными средствами или иным имуществом, обязаны до приема на обслуживание идентифицировать клиента, представителя клиента и (или) выгодоприобретателя, за исключением случаев, установленных [пп. 1.1, 1.2 и 1.4](#) указанной статьи. Согласно [ч. 4 ст. 7](#) Федерального закона от 7 августа 2011 г. N 115-ФЗ банк вправе хранить документы, содержащие сведения, необходимые для идентификации личности, не менее пяти лет. Таким образом, хранение банками указанной информации предусмотрено [ч. 7 ст. 5](#) ФЗ "О персональных данных" [*\(31\)](#).

По правилам организации делопроизводства произвольное уничтожение документов не допускается, тем более содержащих персональные данные. Чтобы уничтожить персональные данные, нужно создать комиссию по уничтожению персональных данных (аналог экспертной комиссии) и утвердить акт об уничтожении персональных данных.

Способы уничтожения персональных данных законодатель делит на две категории:

- физическое уничтожение носителя;
- безвозвратное уничтожение информации из информационной системы.

Конкретный способ определяется каждой организацией в регламенте обработки персональных данных. Он может зависеть как от характера персональных данных, так и от вида носителя (информация на бумажном носителе уничтожается путем уничтожения носителя (шредирование, сжигание), а информация в информационной системе - путем удаления ее с носителя без возможности восстановления).

Для информационных систем, хранящих персональные данные, с уничтожением связан нюанс: авторы закона не предусмотрели возможность существования копий уничтожаемых данных, хотя очевидно, что данные можно считать уничтоженными не только в случае невозможности дальнейшего восстановления содержания данных в информационной системе, но и при одновременном уничтожении всех копий этих данных во всех других информационных системах, в том числе резервных.

9) Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

По сути данного определения обезличивание данных представляет собой операцию, порождающая новую информацию, не дающую возможности привязки персональных данных к конкретному лицу, на основании исходной. Таким образом, обезличивание подразумевает не уничтожение исходной информации, а ее трансформацию, из чего следует, что обезличенные персональные данные и исходные могут обрабатываться совместно, для различных целей. Обезличенные персональные данные могут использоваться в статистических или иных исследовательских целях без дополнительных ограничений ([п. 9 ст. 6](#) комментируемого закона).

Персональные данные обезличиваются за счет того, что некоторые данные (например, фамилия, имя, отчество) или связи между ними в процессе обработки скрываются или изменяются. В таком случае исходные данные возможно восстановить, используя специальную дополнительную информацию [*\(32\)](#). Для корректной обработки персональных данных и их полноценной безопасности в процессе обезличивания и восстановления критически важно сохранить все свойства исходной информации: ее полноту, структурные связи, семантическую целостность. При этом необходимо обеспечить определенный заданный уровень анонимности данных, определяющий стойкость системы к атакам по деобезличиванию [*\(33\)](#).

Основным методическим документом в данной области является [приказ](#) Роскомнадзора от 5 сентября 2013 г. N 996 "Об утверждении требований и методов по обезличиванию персональных данных". Приведем основные его положения.

Обезличивание персональных данных должно обеспечивать не только защиту от несанкционированного использования, но и возможность их обработки. Для этого обезличенные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых персональных данных.

К свойствам обезличенных данных относятся:

- полнота - сохранение всей информации о конкретных субъектах или группах субъектов, которая имелаась до обезличивания;
- структурированность - сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания;
- релевантность - возможность обработки запросов по обработке персональных данных и получения ответов в одинаковой семантической форме;
- семантическая целостность - сохранение семантики персональных данных при их обезличивании;
- применимость - возможность решения задач обработки персональных данных, стоящих перед оператором, осуществляющим обезличивание персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, без предварительного деобезличивания всего объема записей о субъектах;
- анонимность - невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации.

К наиболее перспективным и удобным для практического применения относятся следующие методы обезличивания:

- метод введения идентификаторов - замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным;
- метод изменения состава или семантики - изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений;
- метод декомпозиции - разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств;
- метод перемешивания - перестановка отдельных записей, а так же групп записей в массиве персональных данных.

Данные методы предложены, в основном, для государственных органов, для коммерческой организации они необязательны, и в компании могут применяться другие методы обезличивания.

Аналогичная обезличиванию процедура предусмотрена и [Регламентом ЕС](#) о защите персональных данных.

Под термином "псевдонимизация" понимается обработка персональных данных таким образом, что персональные данные не могут быть больше отнесены к определенному субъекту данных без использования дополнительной информации, при условии, что дополнительная информация хранится отдельно и подлежит применению технических и организационных мер, гарантирующих, что персональные данные не отнесены к идентифицированному или идентифицируемому физическому лицу.

Кроме того, в преамбуле Регламента уточняется, что персональные данные, подвергнутые псевдонимизации, которые могут быть соотнесены с физическим лицом при наличии дополнительной информации, должны рассматриваться в качестве информации об идентифицируемом лиц ([п. 26](#)), а также меры для стимулирования применения псевдонимизации при обработке персональных данных.

Удачным представляется уточнение о необходимости хранения отдельно и защиты дополнительной информации, позволяющей отнести персональные данные к определенным субъектам данных.

10) Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Согласно [п. 3 ст. 2](#) ФЗ "Об информации, информационных технологиях и о защите информации" информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

[Постановление](#) Правительства от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" определяет следующие виды информационных систем:

- информационная система, обрабатывающая специальные категории персональных данных. В ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;
- информационная система, обрабатывающая биометрические персональные данные,

обрабатывает сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных;

- информационная система, обрабатывающая общедоступные персональные данные. В такой системе обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со [ст. 8](#) комментируемого закона;

- информационная система, обрабатывающая иные категории персональных данных. В ней не обрабатываются персональные данные, указанные в предыдущих абзацах;

- информационная система, обрабатывающая персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников.

Для обеспечения защиты информационных систем персональных данных необходимо:

- уведомить регулятора о намерении проводить обработку персональных данных;
- собрать исходные данные;
- присвоить системе класс;
- спрогнозировать угрозы для структуры и составить модель защиты;
- спроектировать, реализовать, интегрировать и аттестовать систему защиты персональных данных;
- подобрать квалифицированный персонал, который будет вести обработку персональных данных^{*(34)}.

Для того чтобы классифицировать информационную систему персональных данных, необходимо знать степень (категорию), к которой относятся данные и определить их объем.

По объему системы делят на три типа:

- к первому относятся системы, насчитывающие свыше 100 000 субъектов в пределах Российской Федерации;

- ко второму - системы, в которых ведется обработка более 1 000 субъектов, которые живут в конкретном муниципальном образовании, заняты в экономике или конкретном органе государственной власти;

- к третьему - информационные системы с данными не более 1 000 субъектов, занятых в конкретной компании.

Проанализировав исходные данные, можно присвоить системе соответствующий класс:

- 1 класс - нарушения безопасности хранения и обработки персональных данных опасны, поскольку могут привести к серьезным пагубным последствиям для их обладателей;

- 2 класс - нарушение обработки и хранения персональных данных способно привести к ощутимым нежелательным последствиям;

- 3 класс - нарушения способны привести к незначительным последствиям;

- 4 класс - нарушения безопасности обрабатываемым данным ничем не угрожают.

Каждому классу соответствует свой уровень защищенности системы (подробнее об этом см. [постановление](#) Правительства от 1 ноября 2012 г. N 1119).

Регламентом ЕС о защите персональных данных предусмотрена похожая категория. Под термином "файловая система" понимается любой структурированный набор персональных данных, доступных в соответствии с определенными критериями, вне зависимости от того используется ли при этом централизованный, децентрализованный, функциональный или географический принцип.

Уточним, что перевод оригинального термина "filing system" дается в разных вариантах: файловая система, система данных, картотека. Из них первый вариант максимально близок к оригиналу, зато последний наиболее интуитивно понятен.

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

Введение данного термина диктуется необходимостью правовой защиты персональных данных за пределами Российской Федерации, поскольку юрисдикция российских властей в силу суверенитета иностранных государств не может распространяться на их территории.

Трансграничная передача представляется законодателем в качестве одного из самостоятельных этапов обработки персональных данных. По своей юридической природе рассматриваемый термин во многом приближен к обнародованию персональных данных, так как связан с их распространением неограниченному кругу лиц.

Подчиняясь общим правилам обработки персональных данных, в том числе и требованию сохранения их конфиденциальности, трансграничная передача в то же время имеет свои особенности

(подробнее о трансграничной передаче персональных данных см [комментарий](#) к ст. 12).

Отвечая на вопросы по поводу трансграничной передачи, Роскомнадзор уточняет, что закон налагает на оператора обязанность при осуществлении обработки собранных персональных данных путем систематизации, накопления, хранения, уточнения, извлечения, использовать базы данных, находящиеся на территории Российской Федерации. Таким образом, если для составления отчетности либо анализа информации, содержащей персональные данные, оператору требуется осуществить упомянутые формы обработки персональных данных, то такие действия должны осуществляться с использованием баз данных, находящихся на территории Российской Федерации.

Российский законодатель пошел по пути определения трансграничной передачи через термин "передача", подразумевающий доступ, предоставление и распространение, тогда как в Европе выбран другой термин.

В [Регламенте](#) ЕС о защите персональных данных под термином "трансграничная обработка" понимается:

- обработка персональных данных, которая осуществляется в контексте деятельности учреждений в нескольких государствах-членах ЕС контролера или осуществляющего обработку лица в Союзе, если контролер или лицо, осуществляющее обработку, учреждены в нескольких государствах-членах ЕС;
- обработка персональных данных, которая осуществляется в контексте деятельности единичного учреждения контролера или лица, осуществляющего обработку, в союзе, но которая существенно влияет или может существенно влиять на субъекты данных в нескольких государствах-членах ЕС.

Такой подход видится более правильным, поскольку в связи с персональными данными используется термин "обработка", именно его определение и присутствует в комментируемом законе, тогда как термина "передача" в нем нет. Кроме того, понятие "обработка" шире, чем понятие "передача".

В заключение сделаем общий комментарий в рамках сравнительного анализа с европейским законодательством.

Список терминов в [Регламенте](#) ЕС о защите персональных данных более развернутый, чем в комментируемом законе, например в нем описаны отдельные виды персональных данных: генетические данные, биометрические данные, данные в отношении здоровья.

Такой подход представляется более адекватным целям правового регулирования, чем разбросанность терминов по отдельным статьям ([ст. 10](#) "Специальные категории персональных данных", [ст. 11](#) "Биометрические персональные данные"). Кроме того, пока комментируемый закон в принципе не содержит понятия "генетические данные", хотя ратифицированный Российской Федерацией протокол, вносящий изменения в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, требует введения новой категории - генетических данных*(35).

[Статья 4. Законодательство Российской Федерации в области персональных данных](#)

1. Комментируемая [статья](#) устанавливает перечень основных актов, которые формируют систему законодательства в области защиты персональных данных:

1) [Конституция](#) - основной закон Российской Федерации, имеющий высшую юридическую силу, прямое действие и применяющийся на всей территории государства. Все нормативные правовые акты, принимаемые в Российской Федерации, не должны противоречить положениям Основного закона страны. Таким образом, правовую основу системы защиты персональных данных составляют положения Конституции.

Однако тут стоит помнить о том, что при выстраивании законодательства о персональных данных следует учитывать конституционные нормы, касающиеся не только прав человека и гражданина при обработке его персональных данных (см. [комментарий](#) к ст. 2), но и защиты прав и законных интересов иных участников отношений в указанной области: общества, государства и бизнеса.

Например, общественный интерес состоит в реализации членами общества конституционных прав на свободу слова и свободу поиска, получения и распространения информации любым законным способом ([ст. 29](#) Конституции). Удовлетворение данного интереса объясняет, в частности, наличие специальных оснований для обработки персональных данных без согласия субъекта для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности ([п. 7 ч. 1 ст. 6](#) комментируемого закона).

Похожие нормы есть и в [Регламенте](#) ЕС о защите персональных данных, где устанавливается, что в законодательстве государств-членов ЕС должны быть согласованы нормы, регулирующие свободу выражения мнений и свободу информации, включая свободу журналистского, научного,

художественного и (или) литературного самовыражения, с правом на защиту персональных данных согласно Регламенту.

Государственный интерес в области персональных данных состоит в их сборе и обработке с целью обеспечения реализации своих публичных функций. В рамках удовлетворения данного интереса в настоящий федеральный закон введена норма о возможности обработки специальных категорий данных без согласия субъекта, если такая обработка 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 (п. 7 ч. 2 ст. 10 комментируемого закона).

Коммерческий интерес при сборе и обработке персональных данных связан с созданием новых моделей ведения бизнеса, персонализации предоставляемых товаров и услуг, актуализации сферы их распространения, эффективного использования информационных технологий в конкурентной борьбе. Учет данных интересов иллюстрируют, например, нормы о возможности обработки персональных данных без согласия их субъекта, если 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 (п. 5 ч. 1 ст. 6 комментируемого закона).

Такой подход согласуется и с Регламентом ЕС о защите персональных данных, где буквально в первых же положениях преамбулы указывается, что принципы и правила защиты физических лиц при обработке их персональных данных вне зависимости от гражданства или места жительства лица должны соответствовать основным правам и свободам, в частности, праву на защиту персональных данных. Целью Регламента является содействие формированию пространства свободы, безопасности и правосудия и экономического союза, содействие экономическому и социальному прогрессу, укреплению и сближению экономик в рамках внутреннего рынка, а также содействие благосостоянию физических лиц.

2) Международные договоры Российской Федерации, то есть соглашения, заключенные Россией с иностранными государствами, международной организацией либо с иным образованием, обладающим правом заключать международные договоры, в письменной форме и регулируемые международным правом, независимо от того, содержатся такие соглашения в одном документе или в нескольких связанных между собой документах, а также независимо от их конкретных наименований.

Международные договоры играют важную роль в защите основных прав и свобод человека, в Российской Федерации же в соответствии с Конституцией они являются составной частью правовой системы государства наряду с общепризнанными принципами и нормами международного права. Учитывая все нарастающий объем трансграничной передачи персональных данных, международные договоры приобретают в законодательстве о персональных данных особый статус.

Среди договоров и соглашений, в которых могут встречаться нормы о защите персональных данных, следует назвать:

- договоры об избегании двойного налогообложения;
- соглашения об обмене информацией в различных сферах;
- соглашения о сотрудничестве в различных сферах.

Примером такого документа может стать Соглашение между Правительством Российской Федерации и Правительством Республики Кипр об избежании двойного налогообложения в отношении налогов на доходы и капитал, заключенное в г. Никозии 5 декабря 1998 г. Данное соглашение в числе прочего устанавливает следующие параметры международного взаимодействия, касающегося защиты персональных данных:

страны-участники обязаны предоставлять друг другу всю информацию, касающуюся исполнения соглашения. Эти данные представляют собой сведения о компаниях и лицах, их финансовых операциях и налоговых выплатах. Но предоставляются они только органам, имеющим отношение к взысканию налоговых выплат;

предоставляется только публичная информация, не являющаяся коммерческой или профессиональной тайной;

нельзя отказать в ответ на запрос только по той причине, что сведения находятся у банка, другой финансовой организации, номинального держателя, доверительного управляющего или несут в себе информацию об имущественном статусе какого-то лица^{*(36)}.

3) В систему законодательства в области персональных данных помимо Конституции, международных договоров и комментируемого закона включены и иные законы. При этом комментируемая статья содержит прямое указание на то, что законодательство в области персональных

данных складывается исключительно из норм федерального законодательства. Подобный подход связан с [подп. "в" п. 1 ст. 71](#) Конституции, согласно которому регулирование прав и свобод человека и гражданина отнесено к исключительному ведению Российской Федерации.

Такая позиция прослеживается и в решениях Конституционного Суда РФ, который неоднократно отмечал, что именно Российской Федерации принадлежит принципиальное первичное конституционно-правовое регулирование прав и свобод, установление их единых федеральных стандартов, способов, средств и порядка защиты.

Федеральное законодательство в рассматриваемой сфере условно можно разделить на две группы:

- а) законы, принятые до комментируемого закона и приведенные в соответствие с ним;
- б) законы, принятые на основании и в исполнение положений комментируемого закона.

В целом, здесь можно назвать, например:

ТК (в части защиты персональных данных работника, [гл. 14](#));

[Федеральный закон](#) от 15 ноября 1997 г. N 143-ФЗ "Об актах гражданского состояния";

[Федеральный закон](#) от 12 августа 1995 г. N 144-ФЗ "Об оперативно-розыскной деятельности";

[Федеральный закон](#) от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации";

[Закон](#) РФ от 21 июля 1993 г. N 5485-I "О государственной тайне" и другие законы.

2. Несмотря на то, что согласно [ч. 1](#) комментируемой статьи законодательство в области персональных данных складывается исключительно из норм федерального законодательства, государственные органы, Банк России, органы местного самоуправления при этом правомочны регулировать рассматриваемую группу правоотношений в части, касающейся конкретизации условий обработки персональных данных.

Принимаемые ими нормативные акты должны соответствовать установленным федеральными законами общим принципам и не могут придать им смысл, который означает по сути ограничение прав и свобод, а также устанавливать не предусмотренные федеральными законами ограничения деятельности операторов или возлагать на операторов не предусмотренные федеральными законами обязанности. Для придания им легитимности принятые нормативные документы подлежат обязательному официальному опубликованию.

Введение такой нормы обусловлено построением системы законодательства в области персональных данных при условии соблюдения строгой иерархичности. Правовую основу построения системы защиты персональных данных составляют положения Конституции, в [ст. 22, 23](#) которой содержатся нормы, провозглашающие основные права личности, касающиеся частной жизни. На органы государственной власти возлагается обязанность обеспечить каждому возможность ознакомления с документами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

2.1. Важная роль в организации работы с персональными данными принадлежит органам исполнительной власти (Президенту, Правительству и другим органам государственной власти), нормативные правовые акты которых создают организационную основу применения соответствующих законодательных положений, обеспечивая повседневное регулирование обработки и защиты персональных данных. К таковым актам относятся, например:

[Указ](#) Президента от 30 мая 2005 г. N 609 "Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела";

[Указ](#) Президента от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера";

[Указ](#) Президента от 17 марта 2008 г. N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";

[распоряжение](#) Президента от 10 июля 2001 г. N 366-рп "О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных";

[постановление](#) Правительства от 21 марта 2012 г. N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных";

[постановление](#) Правительства от 13 июня 2012 г. N 584 "Об утверждении положения о защите информации в платежной системе";

[постановление](#) Правительства от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

[постановление](#) Правительства от 1 ноября 2012 г. N 1119 "Об утверждении требований к

защите персональных данных при их обработке в информационных системах персональных данных";

[приказ](#) Роскомнадзора от 3 декабря 2012 г. 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";

[приказ](#) Роскомнадзора от 30 мая 2017 г. N 94 "Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения";

[приказ](#) Роскомнадзора от 29 января 2016 г. N 82 "О Консультативном совете при уполномоченном органе по защите прав субъектов персональных данных";

[приказ](#) Роскомнадзора от 30 октября 2018 г. N 159 "О внесении изменений в Методические рекомендации по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения, утвержденные приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30 мая 2017 года N 94";

[приказ](#) Министерства энергетики от 14 октября 2014 г. N 724 "О персональных данных в Министерстве энергетики Российской Федерации";

[приказ](#) Минспорта от 27 февраля 2019 г. N 168 "О персональных данных в Министерстве спорта Российской Федерации";

[приказ](#) Федерального казначейства от 31 января 2020 г. N 7н "Об обработке персональных данных в Федеральном казначействе и территориальных органах Федерального казначейства" и др.

2.2. Вторым субъектом, способным принимать нормативные правовые акты по отдельным вопросам, касающимся обработки персональных данных, является Банк России. В силу [Положения](#) Банка России от 22 сентября 2017 г. N 602-П "О правилах подготовки нормативных актов Банка России" нормативные акты Банка России издаются по вопросам, отнесенным к компетенции Банка России [Федеральным законом](#) от 10 июля 2002 г. N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)" и другими федеральными законами.

Нормативные акты Банка России издаются в следующих формах:

инструкция Банка России;

положение Банка России;

указание Банка России.

2.3. Третьим из уполномоченных комментируемой статьей субъектов является орган местного самоуправления. Согласно [п. 1 ст. 7](#) Федерального закона от 6 октября 2003 г. N 131-ФЗ "Об общих принципах организации местного самоуправления в Российской Федерации" по вопросам осуществления отдельных государственных полномочий, переданных органам местного самоуправления федеральными законами и законами субъектов РФ, могут приниматься муниципальные правовые акты на основании и во исполнение положений, установленных соответствующими федеральными законами и (или) законами субъектов РФ. Конкретных видов муниципальных правовых актов в законе не приводится.

3. Согласно [ч. 3](#) комментируемой статьи особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами Российской Федерации с учетом положений настоящего федерального закона.

В настоящее время особенности обработки персональных данных, осуществляемой без использования средств автоматизации, регулируются нормами [Положения](#) об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утв. [постановлением](#) Правительства от 15 сентября 2008 г. N 687.

Согласно данному [Положению](#) 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. При этом 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.

С учетом норм комментируемого [закона](#) и указанного [постановления](#) Правительства во многих органах государственной власти были приняты положения об обработке персональных данных с включением в них отдельного раздела, регулирующего правила обработки персональных данных, осуществляемой без использования средств автоматизации, или отдельные правила, например:

Положение об обработке персональных данных в центральном аппарате Федеральной службы по надзору в сфере транспорта, утв. **приказом** Ространснадзора от 21 января 2013 г. N АК-35фс и т.д.

В других органах государственной власти пошли по пути разработки отдельных положений, например;

Положение о защите персональных данных работников Фонда социального страхования Российской Федерации, обрабатываемых без использования средств автоматизации, утв. **приказом** ФСС от 21 января 2014 г. N 10;

Правила обработки персональных данных в Вооруженных Силах РФ, утв. **приказом** Министра обороны от 4 декабря 2019 г. N 707 "О персональных данных в Вооруженных Силах Российской Федерации", и др.

4. **Частью 4** комментируемой статьи определено, что если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены настоящим федеральным законом, применяются правила международного договора.

Комментируемая норма фактически повторяет положения **ч. 4 ст. 15** Конституции и **п. 2 ст. 5** Федерального закона от 15 июня 1995 г. N 101-ФЗ "О международных договорах Российской Федерации" о превосходстве применения международных договоров Российской Федерации по отношению к национальному законодательству. В настоящем федеральном законе это положение сформулировано очень лаконично, вслед за ч. 4 ст. 15 Конституции оставляя без четкого ответа вопрос о том, что же выше - международный договор или Конституция. Однако **Федеральным законом** от 8 декабря 2020 г. N 429-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации" в комментируемую статью была внесена **ч. 5**, в которой разъясняется порядок соотношения в российском законодательстве положений Конституции и международных договоров. Решения межгосударственных органов, принятые на основании положений международных договоров в их истолковании, противоречащем Конституции, не подлежат исполнению. Изменения внесены в статью в соответствии с поправками в Конституцию.

Порядок и способы взаимодействия национального права и международных договоров находятся полностью на усмотрении государства. Например, вступившие в силу для Франции международные договоры и соглашения, решения о согласии на обязательность которых принимались без участия парламента (то есть не на основании закона), не обладают приоритетом по отношению к законам. В Польше международные договоры, ратифицированные с согласия парламента, выраженного в законе, имеют приоритет перед законом (ст. 91 Конституции Республики Польша), в то время как договоры, ратифицированные без согласия, выраженного в законе, не обладают приоритетом перед законом^{*(37)}.

В Российской Федерации международные договоры обладают приоритетом перед внутригосударственными законодательными нормами, если эти договоры ратифицированы и опубликованы в соответствии с установленным законодательством порядком. Именно ратификация придает международному договору юридическую силу федерального закона. Нератифицированные международные (межгосударственные, межправительственные, межведомственные) договоры не обладают подобным иерархическим приоритетом.

Кроме того, имеется и ряд других условий приоритетного применения международных договоров перед местным законодательством:

отсутствие противоречий с конституцией;

невозможность согласовать норму закона с договорными положениями;

верховенство договоров над противоречащими нормами законов;

отсутствие последующего противоречащего договору законодательства (для государств, в которых договоры обладают одинаковым с ординарными законами статусом);

самоисполнимость договорных положений;

принцип взаимности.

Последствием приоритетного применения международных договоров является замена договорным положением противоречащей нормы закона.

Для практической реализации комментируемых норм следует учитывать и тот факт, что устанавливаемые международным договором правила подлежат применению в случаях, если:

1) Российская Федерация в лице компетентных органов государственной власти выразила свое согласие на обязательность для нее международного договора посредством одного из действий:

подписание договора;

обмен документами, образующими договор;

ратификация договора;

утверждение договора;

принятие договора;

присоединение к договору;

применение любого другого способа выражения согласия, о котором условились договаривающиеся стороны (ст. 6 Федерального закона от 15 июля 1995 г. N 101-ФЗ "О международных договорах Российской Федерации");

2) международный договор вступил в силу для Российской Федерации.

Такое положение смягчает норму Конституции и закреплено в п. 4 постановления Пленума Верховного Суда РФ от 10 октября 2003 г. N 5 "О применении судами общей юрисдикции общепризнанных принципов и норм международного права и международных договоров Российской Федерации".

В п. 5 постановления Пленума Верховного Суда РФ от 31 октября 1995 г. N 8 "О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия" говорится о том, что действуют непосредственно только положения официально опубликованных международных договоров, не требующие издания внутрисударственных актов для их применения. Таким образом, Верховный Суд РФ сузил перечень международных договоров, применяемых судами, и по умолчанию исключил из применения судами как принципы международного права, так и международные обычаи*(38).

В силу изложенного, для целей комментируемого закона особое значение имеют международные нормы, закрепленные в Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.), поскольку данный акт был ратифицирован Россией посредством принятия Федерального закона от 19 декабря 2005 г. N 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных", а 10 октября 2018 г. представитель России подписал в Страсбурге протокол, вносящий изменения в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. Конвенция на сегодняшний день является единственным масштабным международным документом в сфере защиты персональных данных, носящим юридически обязывающий характер.

Цель Конвенции обозначена в ее ст. 1 и состоит в обеспечении на территории каждой стороны для каждого физического лица, независимо от его гражданства или местожительства, уважения его прав и основных свобод, и в частности его права на неприкосновенность частной жизни, в отношении автоматизированной обработки касающихся его персональных данных ("защита данных"). Конвенция закрепляет суверенность подходов, связанных с защитой прав субъектов персональных данных. Принятие мер защиты на территории Российской Федерации рассматривается в рамках национального законодательного поля и является исключительной компетенцией российского уполномоченного органа (Роскомнадзор).

Особый интерес представляют те изменения, которых требует протокол, вносящий изменения в Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. Новшества, закрепленные протоколом, условно можно разделить на три группы:

требования к принципам пропорциональности, минимизации и законности сбора, обработки и хранения персональных данных. Эти принципы уже содержатся в ст. 5 комментируемого закона;

введение новой категории конфиденциальных данных - генетических данных. Законопроект N 744029-7 "О внесении изменений в статью 11 Федерального закона "О персональных данных" в части обработки биометрических персональных данных" находится на рассмотрении*(39);

определение новых прав, предоставляемых гражданам, для управления своими персональными данными при их обработке на основе математических алгоритмов, искусственного интеллекта и т.д. Также вводится обязанность операторов персональных данных уведомлять уполномоченный надзорный орган об утечках, устанавливается четкий режим трансграничных потоков данных.

Вопросы применения новшеств третьей группы активно обсуждаются на различных площадках с участием органов власти и операторского сообщества*(40).

Глава 2. Принципы и условия обработки персональных данных

Статья 5. Принципы обработки персональных данных

1. Настоящая статья определяет принципы обработки персональных данных. Часть 1 комментируемой статьи предусматривает принципы законности и справедливости обработки персональных данных - обработка персональных данных должна осуществляться на законной и справедливой основе.

Согласно п. 3 ст. 3 настоящего федерального закона обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств

автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Несмотря на то, что комментируемая [статья](#) так и называется "принципы обработки персональных данных", однако эти принципы содержатся и в иных статьях главы 2 настоящего федерального закона. К числу этих принципов обработки персональных данных относятся:

- законность ([ч. 1 ст. 5](#));
- справедливость ([ч. 1 ст. 5](#));
- направленность на достижение конкретных целей и результатов (целевой характер) ([ч. 2, 4, 5 ст. 5](#));
- оправданность и достаточность объема ([ч. 5 ст. 5](#));
- точность, актуальность (достоверность), достаточность ([ч. 6 ст. 5](#));
- самостоятельность по отношению к иным базам данных ([ч. 3 ст. 5](#));
- сохранность как свойство удобства пользования и мера защиты, принцип сохранности персональных данных ([ч. 7 ст. 5](#));
- конфиденциальность персональных данных с сочетанием общедоступности персональных данных определенных видов ([ст. 7, 8](#));
- согласование обработки персональных данных с волеизъявлением субъекта персональных данных ([ст. 6, 9, 11](#));
- недопущение обработки персональных данных о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждений, состояния здоровья, интимной жизни ([ст. 10](#)).

Только соблюдение всех установленных комментируемым законом принципов обработки персональных данных в комплексе, во взаимосвязи подразумеваемых юридических требований может обеспечить законность в качестве принципа обработки персональных данных, и в качестве принципа обращения и защиты персональных данных.

2. Закрепленные [ч. 1](#) комментируемой статьи принципы носят базовый характер, на них основываются иные принципы обработки персональных данных и, как более широкая категория, принципы обращения, защиты персональных данных.

Принцип законности имеет универсальное содержание. Безотносительно к сфере и объектам правового регулирования он означает, что развитие общественных отношений, осуществление тех или иных значимых для них действий должно осуществляться в строгом соответствии с требованиями законодательства, с учетом основополагающих принципов реализации отраслевых общественных отношений, установленных актами законодательства. При этом, под законодательством в данном случае понимаются не только, в буквальном смысле, акты законодательного уровня, но и подзаконные акты, но не противоречащие законам.

В связи с анализом принципа законности в сфере защиты персональных данных заметим, что этот принцип подразумевает соблюдение иных установленных настоящим федеральным законом требований и ограничений, также по своей природе имеющих значение принципов защиты персональных данных, а непосредственно - принципов обработки персональных данных.

Помимо принципа законности в [ч. 1](#) комментируемой статьи установлен также принцип справедливости обработки персональных данных. Принцип справедливости относится к числу универсальных правовых принципов.

Справедливость в ракурсе содержания установленных правом категорий означает "представление о должной и гармоничной организации социальных институтов, политико-правовое измерение которой определяется содержанием свободы и равенства"^{*(41)}. Справедливость должна быть положена в основу всех регулируемых правом (законодательными и подзаконными актами) общественных отношений, категорий и понятий, им соответствующих. Считается, что ключевым в определении справедливости выступают понятия "мера", "соразмерность", "адекватность"^{*(42)}.

Данные элементы содержания понятия справедливости применительно к правовому режиму персональных данных и принципам их обработки получают выражение в нормах комментируемой статьи: ограничение объема обработки персональных данных достижением конкретных целей (соразмерность, адекватность обработки персональных данных) ([чч. 2, 4, 5](#)), достаточность персональных данных (понимание меры, соразмерности применительно к обработке персональных данных) ([ч. 6](#)).

Закрепленные в настоящей статье положения получают дальнейшую детализацию в подзаконных нормативных правовых актах, в том числе ведомственных, регламентирующих правила обработки персональных данных сотрудников и служащих в органах государственной власти и

местного самоуправления, например:

в [приказе](#) МЧС от 31 октября 2019 г. N 626 "Об обработке и обеспечении защиты персональных данных в Министерстве Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий";

в [приказе](#) Рослесхоза от 30 октября 2019 г. N 1264 "Об обработке персональных данных в Федеральном агентстве лесного хозяйства";

в [приказе](#) Росархива от 22 апреля 2019 г. N 61 "Об обработке персональных данных в Федеральном архивном агентстве";

в [приказе](#) Росстандарта от 11 июля 2019 г. N 1628 "О персональных данных Федерального агентства по техническому регулированию и метрологии, его межрегиональных территориальных управлений и подведомственных организаций";

в [приказе](#) Следственного комитета РФ от 11 января 2017 г. N 10 "Об обработке персональных данных сотрудников, федеральных государственных гражданских служащих, работников Следственного комитета Российской Федерации, кандидатов на государственную службу (работу) в системе Следственного комитета Российской Федерации" и др.

3. Соблюдение указанных выше принципов - важная гарантия защиты прав физических лиц при обработке персональных данных, провозглашенных актами международного права в числе основных прав граждан. Данным вопросам в законодательстве ЕС посвящены:

[п. 1 преамбулы](#) Регламента ЕС о защите персональных данных;

[п. 1 преамбулы](#) Директивы ЕС о защите физических лиц при обработке персональных данных.

В соответствии с [п. 2 преамбулы](#) Регламента ЕС о защите персональных данных принципы и правила защиты физических лиц при обработке их персональных данных вне зависимости от гражданства или места жительства лица должны соответствовать основным правам и свободам, в частности, праву на защиту персональных данных. Целью Регламента является содействие формированию пространства свободы, безопасности и правосудия и экономического союза, содействие экономическому и социальному прогрессу, укреплению и сближению экономик в рамках внутреннего рынка, а также содействие благосостоянию физических лиц.

[Пункт 39 преамбулы](#) Регламента предписывает, что любая обработка персональных данных должна быть законной и справедливой. Для физических лиц прозрачность обработки состоит в том, что относящиеся к ним персональные данные собираются, используются, просматриваются или иным образом обрабатываются, а также в том, в какой степени персональные данные обрабатываются или будут обрабатываться. Принцип прозрачности требует, чтобы любая информация или сообщения в отношении обработки указанных персональных данных были легкодоступны и понятны и составлены на ясном и простом языке. Указанный принцип касается, в частности, информации относительно личности контролера и целей обработки, а также иной информации, которая гарантирует справедливую и прозрачную обработку в отношении соответствующих физических лиц и их права на получение подтверждения и сообщения относительно того, какие относящиеся к ним персональные данные обрабатываются.

Физические лица должны быть осведомлены о рисках, нормах, гарантиях и правах в отношении обработки персональных данных и о том, как осуществлять свои права в отношении указанной обработки. В частности, определенные цели, для которых обрабатываются персональные данные, должны быть ясными и законными, они должны определяться в ходе сбора персональных данных.

Персональные данные должны быть соответствующими, уместными и ограниченными тем, что необходимо для целей, относительно которых они обрабатываются. В частности, это требует гарантии того, что срок, в течение которого хранятся персональные данные, был ограничен строгим минимумом.

Персональные данные должны обрабатываться, только если цель обработки не могла быть достигнута иным способом.

Для того чтобы гарантировать, что персональные данные не хранятся дольше положенного, контролер должен установить сроки для их уничтожения или для периодического пересмотра. Необходимо принять обоснованные меры, чтобы гарантировать, что неточные персональные данные были исправлены или удалены.

Персональные данные должны обрабатываться таким образом, чтобы гарантировать их соответствующую защиту и конфиденциальность, включая предотвращение несанкционированного доступа или использования персональных данных и оборудования, используемого для обработки.

Приведенные международные нормы соответствуют нормам, установленным в национальном законодательстве о персональных данных.

Обработка персональных данных также считается законной, если она необходима для защиты жизненно важных интересов субъекта данных или другого физического лица. Обработка персональных данных, основанная на жизненном интересе другого физического лица, должна в принципе

осуществляться только в случае, если она не может быть проведена на ином законном основании.

Некоторые типы обработки могут служить как общественному интересу, так и жизненно важным интересам субъекта данных, например, если обработка необходима в гуманитарных целях, в том числе для контроля эпидемий и их распространения или в чрезвычайных ситуациях гуманитарного характера, в частности во время техногенных или природных катастроф ([п. 46 преамбулы](#) Регламента ЕС о защите персональных данных, [п. 26 преамбулы](#) Директивы ЕС о защите физических лиц при обработке персональных данных).

Более того, с позиций международного права закрепленные комментируемой статьей принципы обработки персональных данных выступают, по сути, принципами защиты персональных данных. В соответствии с [п. 26 преамбулы](#) Регламента ЕС о защите персональных данных принципы защиты данных должны применяться в отношении любой информации, касающейся идентифицированного или идентифицируемого физического лица. Подвергнутые псевдонимизации персональные данные, которые могут быть соотнесены с физическим лицом посредством использования дополнительной информации, должны рассматриваться в качестве информации об идентифицируемом физическом лице. В целях установления того, является ли физическое лицо идентифицируемым, следует принять во внимание все средства, с высокой степенью вероятности используемые контролером или иным лицом, для того чтобы прямо или косвенно идентифицировать физическое лицо, например, выявление. При определении того, используются ли средства с достаточной степенью вероятности для идентификации физического лица, следует обратить внимание на все объективные факторы, такие как расходы на идентификацию и количество времени, необходимого для идентификации, с учетом имеющихся на момент обработки технологий и технологических разработок.

4. Помимо указанных принципов обработки персональных данных, охватываемых содержанием принципа законности в этой сфере и выражающих принципы защиты персональных данных, в международном праве провозглашен принцип прозрачности. Так, в соответствии с [пп. 58, 60 преамбулы](#) Регламента ЕС о защите физических лиц при обработке персональных данных принцип прозрачности требует, чтобы любая информация, предоставляемая общественности или субъекту данных, была лаконичной, легкодоступной и понятной, и чтобы использовался ясный и простой язык, и дополнительно, при необходимости, использовались визуальные элементы. Указанная информация может предоставляться в электронной форме, например, если она адресована общественности, на интернет-сайте.

Это имеет существенное значение в ситуациях, когда вследствие большого количества участников и сложности необходимой техники субъекты данных не могут узнать и понять, кем и для каких целей относящиеся к ним персональные данные собираются, например, в случае рекламы в интернете.

Принципы справедливой и прозрачной обработки требуют, чтобы субъект данных был проинформирован о наличии процесса обработки и ее целях. Контролер должен предоставить субъекту данных всю дополнительную информацию, необходимую для обеспечения справедливой и прозрачной обработки, с учетом особых обстоятельств и условий, в которых обрабатываются данные. Кроме этого, субъект данных должен быть проинформирован о наличии профиля и его последствиях. Если персональные данные получены от субъекта данных, он также должен быть проинформирован о том, обязан ли он предоставлять персональные данные, а также о последствиях их непредставления.

Указанная информация может предоставляться совместно со стандартизированными графическими обозначениями, для того чтобы в отчетливо видимой, понятной и четкой форме дать общее представление о запланированной обработке. Если графические обозначения представлены в электронной форме, они должны быть машиночитаемы.

Для того чтобы гарантировать справедливую и прозрачную обработку в отношении субъекта данных, с учетом особых обстоятельств и контекста, в котором обрабатываются персональные данные, контролер должен использовать соответствующие математические и статистические методы для формирования профиля, имплементировать технические и организационные меры в целях гарантии того, что факторы, которые приводят к неточностям персональных данных, исправлены, а риски возникновения ошибок минимизированы, защитить персональные данные таким образом, чтобы принять во внимание потенциальные риски для интересов и прав субъекта данных и не допустить дискриминационного воздействия на физических лиц на основе расового или этнического происхождения, политических убеждений, религии и воззрений, членства в профессиональном союзе, генетических предрасположенностей, состояния здоровья или сексуальной ориентации, или не допустить принятия мер, которые могут иметь указанное воздействие. Автоматизированный процесс принятия решения и формирование профиля на основе особых категорий персональных данных должны осуществляться только при определенных условиях ([п. 71 преамбулы](#) Регламента ЕС о защите персональных данных).

Принципы обработки персональных данных в ракурсе использования их в судебной деятельности и при функционировании иных уполномоченных учреждений государства предусмотрены отдельно в специальных актах (см. Директиву ЕС о защите физических лиц при обработке персональных данных компетентными органами - [ст. 1](#) и иные положения).

5. [Часть 2](#) комментируемой статьи закрепляет требования к целям обработки персональных данных - обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

По сути, речь идет о таком принципе обработки персональных данных, обращения информации, содержащей персональные данные, как направленность на достижение конкретных целей и результатов (целевой характер).

[Часть 2](#) комментируемой статьи применяется взаимосвязано с ее [чч. 4 и 5](#), предусматривающими требования относительно видов (состава) обрабатываемых персональных данных - как исключительно отвечающих заявленным целям обработки и не могущих носить избыточный характер (см. также [комментарий](#) к ст. 7 в части состава субъектов и их полномочий, имеющих доступ к персональным данным и использующим их с определенными целями, в том числе для раскрытия персональных данных третьим лицам).

Общий подход к целям сбора персональных данных, подразумеваемых в настоящем федеральном законе ([ч. 2, 4, 5 ст. 5](#)), очерчен в [Рекомендациях](#) Роскомнадзора по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", от 31 июля 2017 г.

Согласно [п. 3.2](#) Рекомендаций обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Цели обработки персональных данных могут происходить, в том числе, из анализа правовых актов, регламентирующих деятельность оператора, целей фактически осуществляемой оператором деятельности, а также деятельности, которая предусмотрена учредительными документами оператора, и конкретных бизнес-процессов оператора в конкретных информационных системах персональных данных (по структурным подразделениям оператора и их процедурам в отношении определенных категорий субъектов персональных данных).

Надо заметить, что подход к целям обработки персональных данных, содержащийся в законодательстве Российской Федерации, базируется на нормах международного права. Согласно [п. 4 преамбулы](#) Регламента ЕС о защите персональных данных целью обработки персональных данных является служба человечеству. Право на защиту персональных данных не является абсолютным правом; его необходимо рассматривать относительно его функции в обществе, оно должно быть уравнено с другими основными правами в соответствии с принципом пропорциональности.

Цели обработки конкретных видов персональных данных подразумеваются в законодательных актах, регламентирующих обращение информации с персональными данными в рамках конкретных отраслевых правоотношений, а также актами, предусматривающими полномочия различных субъектов запрашивать персональные данные у их носителей, обрабатывать и использовать персональные данные в рамках своей деятельности.

Например, [ст. 86](#) ТК конкретизирует цель обработки персональных данных работника работодателем и его представителями: обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Иной пример можно взять из положений ЖК. В целях формирования, ведения реестра собственников помещений в многоквартирном доме управляющими организациями, правлением товарищества собственников жилья, жилищного или жилищно-строительного кооператива, иного специализированного потребительского кооператива в реестр включаются (собираются, обрабатываются) следующие сведения, позволяющие идентифицировать собственников помещений в данном многоквартирном доме:

фамилия, имя, отчество (при наличии) собственника помещения в многоквартирном доме;

полное наименование и основной государственный регистрационный номер юридического лица, если собственником помещения в многоквартирном доме является юридическое лицо;

номер помещения в многоквартирном доме, собственником которого является физическое или юридическое лицо;

сведения о размерах принадлежащих им долей в праве общей собственности на общее имущество собственников помещений в многоквартирном доме.

Соответственно, персональные данные собираются и обрабатываются в целях получения данных сведений для содержательного наполнения реестра собственников помещений в многоквартирном доме (по анализу буквально закрепленных в [ч. 3.1 ст. 45 ЖК](#) нормативных положений).

Органы ФСБ в общей направленности своей деятельности на обработку персональных данных реализуют полномочия получать на безвозмездной основе от государственных органов, предприятий, учреждений и организаций независимо от форм собственности информацию, необходимую для достижения конкретной цели, а именно выполнения возложенных на органы федеральной службы безопасности обязанностей ([ст. 13](#) Федерального закона от 3 апреля 1995 г. N 40-ФЗ "О федеральной службе безопасности").

В отдельных случаях цели обработки персональных данных прямо указаны в статье закона (например, [ст. 86 ТК](#), [ч. 3.1 ст. 45 ЖК](#), [ст. 13](#) Федерального закона от 3 апреля 1995 г. N 40-ФЗ "О федеральной службе безопасности"), в других - подразумеваются как цель, соответствующая общей направленности деятельности субъекта, запрашивающего те или иные персональные данные, обрабатывающего персональные данные (например, [ч. 6 ст. 184.4-1](#) Федерального закона от 26 октября 2002 г. N 127-ФЗ "О несостоятельности (банкротстве)"; [подп. 2 ч. 1 ст. 64](#) Федерального закона от 2 октября 2007 г. N 229-ФЗ "Об исполнительном производстве").

Установление комментируемым законом ограничения на обработку персональных данных в виде определения конкретных, заранее определенных и законных целей сбора соответствующей информации и недопущения обработки персональных данных, несовместимой с целями их сбора, в свою очередь, вызвано необходимостью защиты персональной информации, обрабатываемой с целями:

защиты прав и безопасности детей (см. [Методические рекомендации](#) по созданию и размещению в сети Интернет и средствах массовой информации видеосюжетов о детях, оставшихся без попечения родителей, а также иной производной информации указанной категории детей с целью реализации права детей жить и воспитываться в семье, направленные [письмом](#) Минобрнауки от 8 октября 2015 г. N ВК-2569/07).

На защиту прав детей в сфере информации обращают внимание и международные акты. Например, в соответствии с [п. 38 преамбулы](#) Регламента ЕС о защите физических лиц при обработке персональных данных дети нуждаются в особой защите своих персональных данных, так как они в меньшей степени осознают риски, последствия, соответствующие гарантии и права при обработке персональных данных. Указанная особая защита должна, в частности, применяться в отношении использования персональных данных детей в целях маркетинга или создания личного профиля или профиля пользователя и сбора персональных данных детей при использовании услуг, предлагаемых непосредственно детям;

из соображений научной этики в сфере науки и образования (см. [письмо](#) Минобрнауки от 11 октября 2018 г. N МН-06.4/571 "О размещении информации");

недопущения вмешательства в личную жизнь человека и гражданина, получения о человеке и гражданине несанкционированных сведений с целью, например, ограничения его в правах и свободах, разглашения конфиденциальных сведений, дискриминации по тем или иным основаниям, унижения человеческого достоинства и по иным целям. В соответствии со [ст. 10](#) настоящего федерального закона обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается.

Заметим, [ч. 3 ст. 13](#) настоящего федерального закрепила правило: права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.

[6. Часть 3](#) комментируемой статьи устанавливает запрет объединения баз персональных данных, содержащих данные, обработка которых осуществляется в целях, несовместимых между собой. Соответственно, не должны быть объединены информационные системы персональных данных как совокупности содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Названное положение выражает, по сути, принцип самостоятельности по отношению к иным базам данных как самостоятельный принцип обработки персональных данных. Цель установления и соблюдения данного принципа на практике - обеспечить независимость одних персональных данных от других, их объективность, не допустить нарушение информационных и иных прав граждан в связи с аккумулярованием в базах данных информации, обрабатываемой в разных целях, вследствие чего

потенциально гражданам может быть причинен вред.

В конечном счете в **ч. 3** комментируемой статьи подразумевается обеспечение режима безопасности персональных данных. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные, или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора (**п. 3** Требований к защите персональных данных при их обработке в информационных системах персональных данных, утв. [постановлением](#) Правительства от 1 ноября 2012 г. N 1119).

На практике получили распространение судебные дела о взыскании денежных средств в пользу граждан в связи с причинением им морального вреда по причине использования полученных персональных данных в различных базах данных, функциональное предназначение которых не связано между собой (см., например, [апелляционное определение](#) Алтайского краевого суда от 27 мая 2020 г. по делу N 33-2930/2020).

Комментируемый запрет сочетается с положениями, закрепленными в **ст. 13** настоящего федерального закона, предусматривающими особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных. Такие информационные системы создаются в пределах полномочий государственных и муниципальных органов.

Наряду с установленным **ч. 3** комментируемой статьи ограничением, следует учитывать международные нормы о гарантиях свободного движения персональных данных между государствами - членами ЕС, соответственно, между находящимися в их ведении информационными системами, содержащими персональные данные (**п. 3** преамбулы Регламента ЕС о защите персональных данных).

7. **Часть 4** комментируемой статьи устанавливает ограничения на обработку персональных данных: обработке подлежат только персональные данные, которые отвечают целям их обработки. Данное ограничение обусловлено необходимостью защиты граждан от необоснованного сбора о них информации личного характера, не отвечающей в каждом конкретном случае определенным целям и задачам участия граждан в общественных отношениях.

Комментируемая норма применяется взаимосвязано с нормами, закрепленными в **чч. 2 и 5** рассматриваемой статьи, предусматривающими принцип обработки персональных данных, обращения информации, содержащей персональные данные, а именно направленность на достижение конкретных целей и результатов (целевой характер) (**ч. 2**) и требование недопущения избыточного характера содержания и объема обрабатываемых персональных данных - как исключительно отвечающего заявленным целям обработки (**ч. 5**).

См. судебную практику по вопросам применения **ч. 4** рассматриваемой статьи: [определение](#) Судебной коллегии по гражданским делам Верховного Суда РФ от 12 ноября 2019 г. N 14-КГ19-15, 2-2794/18; [постановление](#) Одиннадцатого арбитражного апелляционного суда от 23 июля 2019 г. N 11АП-8725/2019 по делу N А65-8941/2019; [постановление](#) Пятнадцатого арбитражного апелляционного суда от 17 апреля 2019 г. N 15АП-2477/2019 по делу N А53-38819/2018.

8. **Часть 5** комментируемой статьи уточняет принципиальный подход настоящего федерального закона к целям обработки персональных данных: 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.

В данном случае подразумевается целевой характер обработки персональных данных, сопоставленный с требованиями их достаточности для формирования информационной базы соответствующего общественного отношения. Избыточность означает выход за пределы необходимого содержания в части сбора, обработки и распространения персональных данных (см. [определение](#) Судебной коллегии по гражданским делам Верховного Суда РФ от 12 ноября 2019 г. N 14-КГ19-15, 2-2794/18).

Требование достаточности обрабатываемых персональных данных для соблюдения определенных целей их обработки в рамках выполнения определенных задач деятельности получает дальнейшую детализацию о видах деятельности, правовом статусе задействованных субъектов.

Например, **п. 2 ст. 14** Федерального закона от 21 июля 1997 г. N 118-ФЗ "Об органах принудительного исполнения Российской Федерации" устанавливает правило: информация, в том числе персональные данные, в объеме, необходимом для исполнения сотрудником органов принудительного исполнения служебных обязанностей в соответствии с законодательством Российской Федерации об исполнительном производстве, предоставляется по требованию сотрудника органов принудительного исполнения в виде справок, документов и их копий безвозмездно и в установленный им срок. Речь идет об объеме обрабатываемых персональных данных и иной информации в деятельности органов принудительного исполнения служебных обязанностей.

Также законодательство предусматривает права нотариуса на получение персональных данных - исключительно для совершения нотариальных действий, то есть деятельности, находящейся в пределах компетенции нотариуса ([ст. 15](#) Основ законодательства РФ о нотариате от 11 февраля 1993 г. N 4462-1).

[Статья 86](#) ТК закрепляет общие требования при обработке персональных данных работника и гарантии их защиты. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться [Конституцией](#), ТК и иными федеральными законами. Тем самым в действиях работодателя не должна допускаться избыточность в сборе персональных данных работников. Граждане-работники подлежат увольнению в случае незаконного разглашения персональных данных иных работников (по вопросу реализации на практике данной нормы см., например: [апелляционное определение](#) Оренбургского областного суда от 12 сентября 2017 г. по делу N 33-6316/2017).

С требованием закона к содержанию и объему обрабатываемых персональных данных связано и другое правило: недопущение обработки персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни ([ст. 10](#) настоящего федерального закона). В случае если в обработку попадают категории персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных, то такая информационная система является информационной системой, обрабатывающей специальные категории персональных данных ([п. 5](#) Требований к защите персональных данных при их обработке в информационных системах персональных данных, утв. постановлением Правительства от 1 ноября 2012 г. N 1119).

[Часть 5](#) комментируемой статьи применяется взаимосвязано с [чч. 2 и 4](#) этой же статьи, предусматривающими принцип обработки персональных данных, обращения информации, содержащей персональные данные, а именно направленность на достижение конкретных целей и результатов (целевой характер) ([ч. 2](#)) и требование ограничения действий по обработке персональных данных осуществлением их только по отношению к тем персональным данным, которые отвечают целям их обработки, предусмотренным специальным законодательством ([ч. 4](#)).

9. [Часть 6](#) комментируемой статьи предусматривает следующие требования, предъявляемые к обработке персональных данных: при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

В содержании [ч. 6](#) речь идет о нескольких элементах правового режима обработки персональных данных, предъявляемых к обработке принципов-требований, а именно:

точность персональных данных - корректность и всесторонность персональных данных, соответствие их содержания действительности. Неточность персональных данных может привести к тому, что на практике соответствующая информация будет признана ложной (см. [апелляционное определение](#) Московского городского суда от 16 октября 2018 г. по делу N 33-35593/2018);

достаточность персональных данных. О достаточности персональных данных в аспекте недопущения их избыточности для достижения целей обработки персональных данных речь идет также в [ч. 5](#) комментируемой статьи;

актуальность - соответствие содержания персональных данных действительности с учетом вносимых в них изменений.

Принятие мер по удалению или уточнению неполных или неточных данных возлагается на оператора. Возложение данной обязанности на оператора объясняется тем, что обработка персональных данных в большинстве случаев необходима для осуществления прав и законных интересов операторов, а не только граждан - носителей персональных данных, обратившихся к оператору за осуществлением тех или иных действий.

Принятие мер по удалению или уточнению неполных или неточных данных может быть возложено на третьих лиц, в случае если оператор в силу [ч. 3 ст. 6](#) комментируемого закона поручил обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не

предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта.

В таком случае лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со [ст. 19](#) комментируемого закона.

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.

Возможность удаления персональных данных связана с реализацией правового режима их хранения (см. подробнее [комментарий](#) к ч. 7 ст. 5).

Использование недостоверной информации, содержащей персональные данные - поводы для судебных споров, в ходе рассмотрения которых информация квалифицируется как ложная (см., например: [апелляционное определение](#) Московского городского суда от 16 октября 2018 г. по делу N 33-35593/2018; [апелляционное определение](#) Московского городского суда от 8 ноября 2016 г. по делу N 33-44065/2016).

10. [Часть 7](#) комментируемой статьи закрепляет требования к организации хранения персональных данных как составляющей принципа сохранности персональных данных при их аккумулировании и обработке. Принцип сохранности выражает свойство удобства пользования персональными данными и меру их защиты.

Элементами принципа сохранности персональных данных выступают следующие требования:

к форме хранения персональных данных - хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных;

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

К хранению документации, в том числе документов с персональными данными, предъявляются нормативные требования, детализируемые и подзаконными нормативными актами, например:

[постановлением](#) Правительства от 6 июля 2008 г. N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";

[постановлением](#) Правительства от 29 июня 2018 г. N 747 "Об установлении требований к фиксации действий при размещении в электронной форме в единой системе идентификации и аутентификации сведений, необходимых для регистрации гражданина Российской Федерации в указанной системе, и иных сведений, предусмотренных федеральными законами, а также при размещении биометрических персональных данных гражданина Российской Федерации в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации";

[постановлением](#) Правительства от 30 июня 2018 г. N 772 "Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации";

[постановлением](#) Правительства от 28 декабря 2018 г. N 1703 "Об утверждении Правил предоставления оператором единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным

гражданина Российской Федерации, в Министерство внутренних дел Российской Федерации и Федеральную службу безопасности Российской Федерации сведений, содержащихся в указанной системе";

постановление Правительства от 14 июля 2018 г. N 820 "Об установлении требований к проведению идентификации гражданина Российской Федерации государственными органами и организациями, осуществляющими размещение в электронной форме в единой системе идентификации и аутентификации сведений, необходимых для регистрации гражданина Российской Федерации в указанной системе, и иных сведений, предусмотренных федеральными законами, а также размещающими сведения в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации";

приказом Росархива от 20 декабря 2019 г. N 236 "Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения";

приказом Минкомсвязи от 25 июня 2018 г. N 321 "Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации";

методическими рекомендациями Банка России от 14 февраля 2019 г. N 4-МР по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации";

приказом ФСБ от 16 декабря 2016 г. N 771 "Об утверждении Порядка получения, учета, хранения, классификации, использования, выдачи и уничтожения биометрических персональных данных об особенностях строения папиллярных узоров пальцев и (или) ладоней рук человека, позволяющих установить его личность, получения биологического материала и осуществления обработки геномной информации в рамках осуществления пограничного контроля";

приказом Росавиации от 17 июня 2016 г. N 492 "Об утверждении порядка сбора, накопления и хранения органами аттестации (аттестующими организациями) данных аттестации и сведений, связанных с обработкой персональных данных аттестуемых лиц" и др.

Хранение персональных данных необходимо должным образом организовать, обеспечить в силу того, что всегда имеется угроза их информационной безопасности. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия (**п. 6** Требований к защите персональных данных при их обработке в информационных системах персональных данных, утв. **постановлением** Правительства от 1 ноября 2012 г. N 1119).

Постановление Правительства от 1 ноября 2012 г. N 1119 предусматривает типы угроз безопасности персональных данных. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение **п. 5 ч. 1 ст. 18.1** комментируемого закона, и в соответствии с нормативными правовыми актами, принятыми во исполнение **ч. 5 ст. 19** комментируемого закона*(43).

При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных (**п. 8-13** Требований к защите персональных данных при их обработке в информационных системах персональных данных, утв. **постановлением** Правительства от 1 ноября 2012 г. N 1119). Речь в данном случае идет, по сути, о защищенности при хранении персональных данных.

Необходимость решения проблемы сохранности и защиты информации с персональными данными обосновывается в европейском законодательстве. Согласно **п. 6 преамбулы** Регламента ЕС о защите персональных данных в связи с быстрым развитием технологий и глобализацией появились новые проблемы, связанные с защитой персональных данных. Масштаб сбора и обмена персональными данными существенно увеличился. Технологии позволяют частным компаниям и органам государственной власти в рамках осуществления своей деятельности использовать персональные данные в беспрецедентном масштабе. В последнее время физические лица все чаще делают доступной личную информацию. Технологии изменили экономическую и социальную жизнь, они должны и далее

облегчать свободное движение персональных данных в Союзе, а также их передачу третьим странам и международным организациям, при этом необходимо обеспечить высокий уровень защиты персональных данных. О внесении исправлений и удалении информации речь идет в гл. 3 Регламента (ст. 16-20).

См. судебную практику по вопросам применения ч. 7 комментируемой статьи в части хранения и уничтожения персональных данных: [постановление](#) Арбитражного суда Волго-Вятского округа от 27 ноября 2019 г. N Ф01-6281/2019 по делу N А82-782/2019; [постановление](#) Арбитражного суда Московского округа от 15 января 2018 г. N Ф05-18981/2017 по делу N А40-81171/17-149-793; [постановление](#) Арбитражного суда Центрального округа от 23 апреля 2019 г. N Ф10-1367/2019 по делу N А62-11017/2017; [апелляционное определение](#) Московского городского суда от 14 июня 2019 г. по делу N 33-25479/2019; [апелляционное определение](#) Московского городского суда от 18 февраля 2019 г. по делу N 33-7630/2019.

В большинстве инициированных споров истцы полагают, что хранение сведений об их персональных данных (без перевода в архивные фонды автоматизированных оперативно-справочных картотек) нарушает их права на неприкосновенность частной жизни, личную и семейную тайну; не соответствует целям обработки персональных данных, создает препятствия для реализации их прав в будущем (см. подробнее: [апелляционное определение](#) Апелляционной коллегии Верховного Суда РФ от 10 мая 2018 г. N АПЛ18-143).

Статья 6. Условия обработки персональных данных

1. **Часть 1** комментируемой статьи к условиям обработки персональных данных относит соблюдение принципов и правил, предусмотренных настоящим федеральным законом (см. [комментарий](#) к ст. 5). Данная норма не подлежит расширительному толкованию, а значит, правила обработки персональных данных могут устанавливаться иными законодательными актами только в том случае, если это прямо предусмотрено комментируемым законом.

Близкие по своей правовой природе нормы содержатся в ст. 6 Регламента ЕС о защите персональных данных, согласно которой государства-члены ЕС исходя из общих формулировок оснований обработки персональных данных вправе сохранить или предусмотреть более конкретные условия и требования. Общими же константами законной обработки персональных данных на территории Евросоюза являются:

(а) субъект данных дал согласие на обработку своих персональных данных для одной или нескольких конкретных целей;

(б) обработка необходима для исполнения договора, в котором субъект данных является одной из сторон, или для принятия мер по требованию субъекта данных до заключения договора;

(с) обработка необходима для соблюдения юридической обязанности, объектом которой является контролер;

(d) обработка необходима для защиты жизненных интересов субъекта данных или другого физического лица;

(е) защита необходима для выполнения задачи, осуществляемой в интересах государства или при осуществлении государственной власти, закрепленной за контролером;

(f) обработка необходима для целей обеспечения законных интересов контролера или третьей стороны, за исключением случаев, когда такие интересы перекрываются интересами или основными правами и свободами субъекта данных, которые требуют защиты персональных данных, в частности, если субъектом данных является ребенок.

Также ч. 1 комментируемой статьи определены случаи, в которых допускается обработка персональных данных:

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

Подробнее о данном основании см. [комментарий](#) к ст. 9.

2) Обработка персональных данных без или независимо от согласия субъекта персональных данных возможна, если она 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.

Рассматриваемая норма включает два самостоятельных основания для обработки персональных данных. Первое связано с реализацией норм, заложенных в международных договорах, ратифицированных Российской Федерацией. Так, например, согласно п. "b" ч. 1 ст. 7 Договора между Российской Федерацией и Королевством Камбоджа о выдаче от 1 февраля 2017 г.*⁽⁴⁴⁾ запрос о выдаче должен включать полное имя лица, выдача которого запрашивается, сведения о его гражданстве, месте жительства или месте пребывания и, по возможности, описание его внешности с приложением

фотографии и отпечатков пальцев, а также другие сведения, позволяющие разыскать и идентифицировать это лицо. Частным случаем обработки персональных данных на основании международного договора является реализация соглашения о реадмиссии (см. [п. 2.3](#) комментария к ст. 10).

Второе основание обработки персональных данных, предусмотренное комментируемым пунктом, - осуществление и выполнение возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей. Оно имеет многочисленные бланкетные отсылки к иным законодательным актам и является общим основанием обработки персональных данных оператором, выполняющим публично-правовые функции.

Например, обработка персональных данных государственных служащих осуществляется на основании комментируемой нормы, положений [ТК](#), [Федерального закона](#) от 27 июля 2004 г. N 79-ФЗ "О государственной гражданской службе Российской Федерации", [Федерального закона](#) от 25 декабря 2008 г. N 273-ФЗ "О противодействии коррупции". Согласно [абз. 4](#) и [5 ст. 15](#) [Федерального закона](#) от 1 апреля 1996 г. N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования" страхователь обязывается представлять органам ПФР сведения о застрахованных лицах. Следует отметить, что обязанность возлагается на страхователей, которыми согласно [абз. 4 ст. 1](#) данного закона могут выступать:

юридические лица;

международные организации;

семейные (родовые) общины коренных малочисленных народов Севера, Сибири и Дальнего Востока Российской Федерации;

граждане, в том числе иностранные, лица без гражданства, проживающие на территории Российской Федерации, и индивидуальные предприниматели, осуществляющие прием на работу по трудовому договору, а также заключающие договоры гражданско-правового характера, на вознаграждения по которым в соответствии с законодательством РФ начисляются страховые взносы;

органы службы занятости в отношении безработных, а также организации, в которых лица, осужденные к лишению свободы, привлекаются к труду (приравниваются к страхователям).

Рассматриваемое основание имеет крайне широкую сферу действия, а следовательно, и спектр целевых предназначений, что может спровоцировать злоупотребление оператором персональных данных соответствующими дискреционными полномочиями. Аналогичная ситуация складывается и в отношении предусмотренного [п. \(е\) ч. 1 ст. 6](#) Регламента ЕС о защите персональных данных условия законности обработки персональных данных "защита необходима для выполнения задачи, осуществляемой в интересах государства или при осуществлении государственной власти, закрепленной за контролером". Осознавая это, разработчики указанного Регламента в [чч. 3 и 4 ст. 6](#) предусмотрели правовой "противовес" возможности злоупотребления правом. Согласно этим нормам указанная цель обработки персональных данных должна определяться в рамках указанного юридического основания и быть необходимой для выполнения задачи, осуществляемой в интересах государства или при осуществлении государственной власти, закрепленной за контролером. Законодательство Союза или государства-члена ЕС при этом должно соответствовать цели государственных интересов и быть пропорциональным в отношении законной цели. Указанное юридическое основание, среди прочего, может содержать конкретные положения для применения норм Регламента:

общие условия, регулирующие законность обработки контролером;

типы данных, подлежащих обработке;

соответствующие субъекты данных;

субъекты, которым могут быть раскрыты данные, и цели, для которых персональные данные раскрываются;

целевое ограничение;

сроки хранения;

процедуры и процесс обработки данных, в том числе меры, гарантирующие законную и справедливую обработку.

[Частью 4 ст. 6](#) Регламента предусмотрены индикаторы, позволяющие надзирающим органам оценить правомерность определения оператором персональных данных цели (условия, основания) их обработки, если она не основана на "согласии субъекта данных или на законодательстве". В частности, контролеру предписывается принять во внимание:

(а) любую связь между целями, для которых были получены персональные данные, и целями предполагаемой последующей обработки;

(б) обстановку, в которой собирались персональные данные, в частности, отношения между субъектами данных и контролером;

(с) характер персональных данных, в частности, производится ли обработка особых категорий данных, согласно [ст. 9](#), или производится ли обработка персональных данных, связанных с судимостями и преступлениями, согласно [ст. 10](#);

(d) возможные последствия предполагаемой последующей обработки для субъектов данных;

(е) существование средств по обеспечению безопасности, которые могут включать в себя криптографическое закрытие или псевдонимизацию.

3) Обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах. Согласно [ст. 118](#) Конституции правосудие в России осуществляется только судом, а судебная власть осуществляется посредством конституционного, гражданского, арбитражного, административного и уголовного судопроизводства. Судопроизводство представляет собой урегулированную нормами процессуального права деятельность суда, участвующих в деле лиц и других участников процесса, а также органов исполнения судебных решений по разрешению юридических дел.

Содержание конкретного вида судопроизводства обусловлено задачами соответствующего юридического процесса. Так, согласно [ст. 2](#) ГПК задачами гражданского судопроизводства являются правильное и своевременное рассмотрение и разрешение гражданских дел в целях защиты нарушенных или оспариваемых прав, свобод и законных интересов граждан, организаций, прав и интересов Российской Федерации, субъектов РФ, муниципальных образований, других лиц, являющихся субъектами гражданских, трудовых или иных правоотношений.

В соответствии со [ст. 1.2](#) КоАП задачами законодательства об административных правонарушениях выступают защита личности, охрана прав и свобод человека и гражданина, охрана здоровья граждан, санитарно-эпидемиологического благополучия населения, защита общественной нравственности, охрана окружающей среды, установленного порядка осуществления государственной власти, общественного порядка и общественной безопасности, собственности, защита законных экономических интересов физических и юридических лиц, общества и государства от административных правонарушений, а также предупреждение административных правонарушений.

Участвующее в судопроизводстве лицо наделяется специальным правовым статусом (истец, ответчик, потерпевший, подозреваемый, свидетель, специалист и т.д.), в связи с чем требуется идентификация его личности, для правонарушителя (подозреваемого, обвиняемого) - определение состояния психического здоровья, а для специалиста и эксперта - уровень образования и квалификации.

Помимо того, согласно [ст. 73](#) УПК при производстве по уголовному делу, среди прочего, подлежат доказыванию: виновность лица в совершении преступления, форма его вины и мотивы; обстоятельства, характеризующие личность обвиняемого; обстоятельства, исключающие преступность и наказуемость деяния; обстоятельства, смягчающие и отягчающие наказание; обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания. Каждая из перечисленных позиций связана с истребованием и оценкой персональных данных того или иного участника производства.

Отечественное законодательство о персональных данных практически не регламентирует вопросы обработки данных субъекта до того момента, когда он приобретает специальный процессуальный статус, не охвачена его регулированием и виктимологическая профилактика (информационно-психологическое воздействие на потенциальную жертву преступления). Европейский законодатель в данной сфере проявляет большую гибкость, предусматривая в [ч. 1 ст. 1](#) Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами в качестве оснований обработки персональных данных предотвращение, расследование, выявление или уголовное преследование преступлений или исполнение уголовных наказаний, включая защиту от угроз общественной безопасности и предотвращение таких угроз. В [ст. 6](#) Директивы закреплена обязанность для операторов разграничивать персональные данные не только по основанию обработки, но и по категории субъекта персональных данных. В частности, предписывается уделять внимание следующим категориям:

(a) лица, в отношении которых имеются серьезные основания полагать, что они совершили или собираются совершить уголовное преступление;

(b) лица, осужденные за совершение уголовного преступления;

(с) жертвы уголовного преступления или лица, в отношении которых с учетом определенных фактов имеются основания полагать, что они могут стать жертвами уголовного преступления;

(d) другие лица, связанные с уголовным преступлением, например лица, которые могут быть призваны дать показания в ходе расследования уголовного преступления или последующего производства по уголовному делу; лица, которые могут представить информацию об уголовных преступлениях; контактные лица или сообщники субъектов, указанных в [пунктах \(a\) и \(b\)](#).

4) Обработка персональных данных необходима для исполнения судебного акта, акта другого

органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве.

Согласно [ст. 2](#) Федерального закона от 2 октября 2007 г. N 229-ФЗ "Об исполнительном производстве" задачами исполнительного производства являются правильное и своевременное исполнение судебных актов, актов других органов и должностных лиц, а в предусмотренных законодательством случаях исполнение иных документов в целях защиты нарушенных прав, свобод и законных интересов граждан и организаций, а также в целях обеспечения исполнения обязательств по международным договорам Российской Федерации.

Принудительное исполнение судебных актов, актов других органов и должностных лиц возлагается на Федеральную службу судебных приставов и ее территориальные органы (ФССП). Именно эта служба создает и ведет, в том числе в электронном виде, банк данных, содержащий сведения, необходимые для осуществления задач по принудительному исполнению судебных актов, актов других органов и должностных лиц. На период размещения персональных данных должника (фамилия, имя, отчество, дата рождения, место рождения, фактический адрес) в этой информационной системе они считаются общедоступными и хранятся до достижения задач исполнительного производства.

Следует отметить, что согласно [абз. 2 п. 7.4](#) Порядка создания и ведения банка данных в исполнительном производстве ФССП в электронном виде, утв. [приказом](#) ФССП от 12 мая 2012 г. N 248, содержащиеся в нем персональные данные не должны размещаться в форме "открытых данных".

5) Обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов РФ, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных [Федеральным законом](#) от 27 июля 2010 г. N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", включая регистрацию субъекта персональных данных на портале Госуслуг и (или) региональных порталах государственных и муниципальных услуг.

Рассматриваемая норма коррелирует с положениями [ч. 4 ст. 7](#) Федерального закона от 27 июля 2010 г. N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", согласно которой для обработки персональных данных не требуется получение согласия заявителя как субъекта персональных данных при:

регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг и на региональных порталах государственных и муниципальных услуг, так как сам факт добровольной регистрации подразумевает подобное согласие;

предоставлении государственной или муниципальной услуги на основании заявления субъекта персональных данных.

[Перечень](#) сведений, находящихся в распоряжении органов и организаций, участвующих в предоставлении государственных или муниципальных услуг, и необходимых для предоставления государственных услуг федеральными органами исполнительной власти и органами государственных внебюджетных фондов утвержден [распоряжением](#) Правительства от 29 июня 2012 г. N 1123-р. К таковым, в частности, относятся сведения о:

- государственной регистрации рождения;
- государственной регистрации заключения брака;
- государственной регистрации расторжения брака;
- государственной регистрации установления отцовства;
- государственной регистрации перемены имени;
- лишении матери (отца) ребенка родительских прав;
- отмене усыновления (удочерения) ребенка;
- ограничении матери (отца) ребенка в родительских правах;
- отобрании ребенка при непосредственной угрозе жизни или его здоровью (по месту жительства ребенка).

Информационный обмен персональными данными в ходе предоставления государственных и муниципальных услуг реализуется, в том числе, посредством Единой системы межведомственного электронного взаимодействия (СМЭВ), [положение](#) о которой утверждено [постановлением](#) Правительства от 8 сентября 2010 г. N 697.

Среди основополагающих задач СМЭВ выделено обеспечение информационного взаимодействия в электронной форме между государственными органами, банками и иными организациями, а также оператором единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их

проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина в целях обеспечения идентификации гражданина с применением информационных технологий без его личного присутствия.

6) 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.

В соответствии со [ст. 420](#) ГК договором является соглашение двух или нескольких лиц об установлении, изменении или прекращении гражданских прав и обязанностей. Граждане и юридические лица свободны в заключении договора. Понуждение к заключению договора не допускается, за исключением случаев, когда обязанность заключить договор предусмотрена ГК, законом или добровольно принятым обязательством.

Справедливо, что в случае добровольного вступления субъекта персональных данных в договорные правоотношения, для исполнения договора не требуется дополнительного с его стороны согласия на обработку персональных данных. При этом следует отметить, что объем и содержание обрабатываемых персональных данных должны соответствовать целям и предмету договора, не являться избыточными.

Гражданско-правовой статус поручителя закреплен в [ст. 361](#) ГК. Таковым признается лицо, которое по договору поручительства обязуется перед кредитором другого лица отвечать за исполнение последним его обязательства полностью или в части. Договор поручительства может быть заключен в обеспечение как денежных, так и неденежных обязательств, а также в обеспечение обязательства, которое возникнет в будущем.

Определение выгодоприобретателя дано в [ст. 3](#) Федерального закона от 7 августа 2001 г. N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" - это лицо, к выгоде которого действует клиент, в том числе на основании агентского договора, договоров поручения, комиссии и доверительного управления, при проведении операций с денежными средствами и иным имуществом.

Объем обрабатываемых на основании договорных отношений персональных данных зависит от предмета и условий соглашения. Так, согласно [ст. 65](#) ТК работодатель вправе требовать предоставления от поступающего на работу лица паспортных данных, сведений об образовании, опыте и месте (местах) работы, причинах увольнения, информации о наличии судимости и нахождении на наркологическом учете в медицинской организации.

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

По общему правилу гражданин самостоятельно принимает решение о разглашении сведений о состоянии своего здоровья. Однако, независимо от его желания, они могут быть переданы в порядке и на основаниях, указанных в [ст. 13](#) Федерального закона от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в РФ":

в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю, с учетом положений [п. 1 ч. 9 ст. 20](#) Федерального закона от 21 ноября 2011 г. N 323-ФЗ;

при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений (как правило, в условиях режимов чрезвычайного положения, чрезвычайной ситуации или повышенной готовности);

по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора, 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, а также в связи с исполнением осужденным обязанности пройти лечение от наркомании и медицинскую и (или) социальную реабилитацию;

в целях осуществления уполномоченными федеральными органами исполнительной власти контроля за исполнением лицами, признанными больными наркоманией либо потребляющими наркотические средства или психотропные вещества без назначения врача либо новые потенциально опасные психоактивные вещества, возложенной на них при назначении административного наказания судом обязанности пройти лечение от наркомании, диагностику, профилактические мероприятия и (или) медицинскую реабилитацию;

в случае оказания медицинской помощи несовершеннолетнему в соответствии с [п. 2 ч. 2 ст. 20](#),

а также несовершеннолетнему, не достигшему возраста, установленного [ч. 2 ст. 54](#) Федерального закона от 21 ноября 2011 г. N 323-ФЗ, 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 проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти и федеральных государственных органов, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

в целях расследования несчастного случая на производстве и профессионального заболевания, а также несчастного случая с обучающимся во время пребывания в организации, осуществляющей образовательную деятельность, и в соответствии с [ч. 6 ст. 34.1](#) Федерального закона от 4 декабря 2007 г. N 329-ФЗ "О физической культуре и спорте в Российской Федерации" несчастного случая с лицом, проходящим спортивную подготовку и не состоящим в трудовых отношениях с физкультурно-спортивной организацией, не осуществляющей спортивной подготовки и являющейся заказчиком услуг по спортивной подготовке, во время прохождения таким лицом спортивной подготовки в организации, осуществляющей спортивную подготовку, в том числе во время его участия в спортивных соревнованиях, предусмотренных реализуемыми программами спортивной подготовки;

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

в целях осуществления учета и контроля в системе обязательного социального страхования;

в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с [Федеральным законом](#) от 21 ноября 2011 г. N 323-ФЗ.

8) Обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных [Федеральным законом](#) от 3 июля 2016 г. N 230-ФЗ "О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон "О микрофинансовой деятельности и микрофинансовых организациях", либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных.

Данное основание имеет дискретный характер, а его применение может быть обусловлено широким спектром причин и условий. Речь идет об обработке персональных данных:

на основании публичного (общественного) интереса (обеспечение безопасности жизни и здоровья граждан, обороны и безопасности государства, охраны окружающей природной среды, обнаружение и раскрытие угроз демократическому правовому государству и гражданскому обществу, общественной безопасности и т.д.);

или в связи с эксплуатацией источника повышенной опасности (оружие, боеприпасы, транспорт и транспортная инфраструктура, ядовитые, радиоактивные, взрывчатые вещества, наркотические средства, энергетика и т.д.);

а также для защиты интересов национальной безопасности в отдельных отраслях экономики и управления (предоставление государственных и муниципальных услуг; обеспечение миграционного и паспортно-регистрационного режима; банковская деятельность и денежно-финансовые переводы; организация пропускного режима и видеоконтроль трудовой деятельности работников организации; обеспечение возможности распорядиться находящемся в законной собственности имуществом или исполнить условия договора, в том числе, посредством взыскания задолженности).

Согласно определениям Конституционного Суда РФ от [12 февраля 2019 г. N 274-О](#) и [N 275-О](#) публичный интерес усматривается и в распространении фото и видеоизображения лица, которое является публичной фигурой (занимает государственную или муниципальную должность, играет существенную роль в общественной жизни в сфере политики, экономики, искусства, спорта или любой иной области), а обнародование и использование изображения осуществляется в связи с политической или общественной дискуссией или интерес к данному лицу является общественно значимым.

Следует подчеркнуть, что, используя комментируемое основание обработки персональных данных, оператор принимает на себя риски и ответственность за причинение тем самым субъекту персональных данных ущерба, нарушение его прав и законных интересов.

Иными словами, с уверенностью о возможности применения данного основания можно говорить при наличии устоявшейся казуальной судебной практики, а также в случаях, предусмотренных [ч. 5](#)

ст. 6 Федерального закона от 3 июля 2016 г. N 230-ФЗ, согласно которой сведения о должнике, просроченной задолженности и ее взыскании, а также любые другие персональные данные должника независимо от его согласия кредитор вправе передавать определенным в данном законе органам и организациям при заключении договора и в ходе переговоров о заключении договора, предусматривающего уступку права требования, передачу права требования в залог, осуществление действий, направленных на возврат просроченной задолженности, или наделении соответствующими полномочиями путем выдачи доверенности.

9) 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.

Названное основание обработки персональных данных обеспечивает реализацию журналистской, научной, литературной или иной творческой деятельности. Согласно **ст. 2** Закона РФ от 27 декабря 1991 г. N 2124-1 "О средствах массовой информации" под средством массовой информации понимается периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием (названием).

Рассматриваемое основание имеет два основных направления применения.

С одной стороны, персональные данные могут потребоваться для допуска к осуществлению указанных видов деятельности, с другой же - субъект этой деятельности в целях полноценной реализации представленных ему прав уполномочивается на обработку персональных данных третьих лиц.

В качестве примеров можно привести положения **ст. 10** Закона РФ от 27 декабря 1991 г. N 2124-1, согласно которой для регистрации СМИ в уполномоченный орган необходимо предоставить, в том числе, сведения об его учредителе (соучредителях), а также **ст. 48** того же закона и положения принимаемых на ее основе нормативных актов, определяющих порядок аккредитации журналистов в государственных органах, органах местного самоуправления, организациях, учреждениях, органах общественных объединений.

Так, согласно **Правилам** аккредитации журналистов и технических специалистов средств массовой информации при Государственной Думе Федерального Собрания Российской Федерации, утв. распоряжением Председателя Государственной Думы от 2 июля 2015 г. N 175р-1, заявка на аккредитацию средства массовой информации при Государственной Думе должна содержать фамилию, имя, отчество, псевдоним (при наличии), должность, паспортные данные (серия, номер, дата и место рождения адрес регистрации), телефоны (домашний, рабочий, мобильный) и адрес электронной почты аккредитуемого журналиста.

Аналогичные по своей правовой природе положения в сфере научной деятельности содержатся в **Федеральном законе** от 23 августа 1996 г. N 127-ФЗ "О науке и государственной научно-технической политике" и в **постановлении** Правительства от 24 сентября 2013 г. N 842 "О порядке присуждения ученых степеней" в части официальной оценки научной квалификации посредством государственной системы научной аттестации.

С другой стороны, комментируемое основание обеспечивает возможность обработки субъектами журналистской, научной, литературной и иной творческой деятельности персональных данных для достижения соответствующих профессиональных интересов. Следует подчеркнуть, что если научно-техническая и журналистская деятельность имеют прямые или косвенные нормативные толкования, то сущность и содержание литературной и иной творческой деятельности с позиции юриспруденции исчерпывающе описать попросту невозможно, что дает возможность для ее расширительной трактовки.

В **ст. 3** Основ законодательства Российской Федерации о культуре от 9 октября 1992 г. N 3612-1 содержится определение творческой деятельности - это создание культурных ценностей и их интерпретация. Сами же культурные ценности представляют собой нравственные и эстетические идеалы, нормы и образцы поведения, языки, диалекты и говоры, национальные традиции и обычаи, исторические топонимы, фольклор, художественные промыслы и ремесла, произведения культуры и искусства, результаты и методы научных исследований культурной деятельности, имеющие историко-культурную значимость здания, сооружения, предметы и технологии, уникальные в историко-культурном отношении территории и объекты.

Так же как и в предыдущем пункте, рассматриваемое основание обработки персональных данных не должно быть использовано для причинения вреда, посягательства на честь и достоинство, нарушения прав и законных интересов субъекта персональных данных. Пределы использования персональных данных в целях осуществления указанных видов творческой деятельности могут быть

прямо определены в законодательстве. Например, согласно **п. 8 ч. 1 ст. 5** Федерального закона от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" фактически запрещается публичный оборот информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

10) Обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в **ст. 15** настоящего федерального закона, при условии обязательного обезличивания персональных данных.

Согласно **п. 9 ст. 3** комментируемого закона обезличивание персональных данных представляет собой действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

В статистических целях персональные данные обрабатываются органами государственной власти и органами местного самоуправления, общественными объединениями, учреждениями и организациями. Например, на сайте Росстата (<https://rosstat.gov.ru>) размещается статистическая информация с результатами проводимых переписей населения, в которой содержатся персональные данные, в том числе специальные категории персональных данных (см. **комментарий** к ст. 10). На сайте Минздрава (<https://minzdrav.gov.ru>) размещаются данные о заболеваемости граждан и рождаемости, здоровья матери и ребенка, а на сайте МВД (<https://мвд.рф/Deljatelnost/statistics>) - статистические сведения о лицах, совершивших преступления.

Наиболее известными негосударственными субъектами социологической обработки персональных данных являются Фонд общественного мнения (<https://fom.ru>) и Левада-центр (<https://www.levada.ru>). Вместе с тем представленные в указанных информационных ресурсах персональные данные не позволяют идентифицировать конкретного человека, они выступают предметом социологического, демографического и криминологического анализа.

Не могут без согласия субъекта обрабатываться персональные данные в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации (см. **комментарий** к ст. 15).

Следует отметить, что согласно **ч. 3 ст. 4** Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами в научных, статистических или исторических целях обработка персональных данных может быть осуществлена в форме архивирования.

11) Обработка персональных данных, полученных в результате обезличивания персональных данных, осуществляется в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных **Федеральным законом** от 24 апреля 2020 г. N 123-ФЗ "О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных", в порядке и на условиях, которые предусмотрены указанным законом.

Именно названным **законом** комментируемая норма введена в настоящую **статью** с 1 июля 2020 г. Она легализует формально неопределенный перечень исключений из правил обработки персональных данных на территории г. Москвы (подробнее см. **п. 3** комментария к ст. 10).

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

Сведения со статусом обязательного доверения являются особой разновидностью информации наравне с информацией ограниченного доступа и информацией, чей оборот запрещен или ограничен на территории России. Перечень подобных сведений приведен в **ч. 4 ст. 8** ФЗ "Об информации, информационных технологиях и о защите информации":

нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

информация о состоянии окружающей среды;

информация о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

информация, накапливаемая в открытых фондах библиотек, музеев, а также в государственных,

муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

информация, содержащаяся в архивных документах архивных фондов (за исключением сведений и документов, доступ к которым ограничен законодательством);

иная информация, недопустимость ограничения доступа к которой установлена федеральными законами.

Например, в соответствии с нормами [ст. 14](#) Федерального закона от 22 декабря 2008 г. N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации" в сети Интернет размещаются фамилии, имена и отчества председателя суда, заместителей председателя суда, судей, руководителя аппарата суда; информация об участниках судебного процесса. При этом согласно [ч. 4 ст. 15](#) названного закона из текстов решений исключаются:

а) фамилии, имена и отчества участников судебного процесса, дата и место рождения, место жительства или пребывания, номера телефонов, реквизиты паспорта или иного документа, удостоверяющего личность, ИНН - физического лица, основной государственный регистрационный номер индивидуального предпринимателя, страховой номер индивидуального лицевого счета;

б) сведения о месте нахождения земельного участка, здания, сооружения, жилого дома, квартиры, транспортного средства, иные сведения об имуществе и о находящихся в банках или иных кредитных организациях денежных средствах участников судебного процесса, если эти сведения относятся к существу дела.

Другим примером могут служить нормы [Федерального закона](#) от 25 декабря 2008 г. N 273-ФЗ "О противодействии коррупции" и [Указа](#) Президента от 8 июля 2013 г. N 613 "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", регламентирующие основания и порядок размещения в сети Интернет сведений о доходах, об имуществе и обязательствах имущественного характера лиц, замещающих определенные должности государственной или муниципальной службы.

2. [Часть 1.1](#) комментируемой статьи устанавливает, что обработка персональных данных объектов государственной охраны и членов их семей осуществляется с учетом особенностей, предусмотренных [Федеральным законом](#) от 27 мая 1996 г. N 57-ФЗ "О государственной охране". Согласно п. 14.1 ст. 15 этого закона обработка персональных данных объектов государственной охраны и членов их семей может осуществляться с согласия органов государственной охраны.

3. [Часть 2](#) комментируемой статьи содержит отсылку к [ст. 10](#) и [11](#) настоящего федерального закона, устанавливающим особый порядок обработки специальных категорий персональных данных, а также биометрических персональных данных.

4. [Части 3-5](#) комментируемой статьи определяют основания и порядок поручения оператора обработки персональных данных третьему лицу на основании согласия субъекта персональных данных, а также ответственность оператора персональных данных за нарушение установленного законом порядка. Основанием такого поручения вариативно могут выступать:

договор, в том числе государственный или муниципальный контракт;

принятый государственным или муниципальным органом соответствующий акт управления.

В поручении оператора должны быть определены:

перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных (сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение);

цели обработки;

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

требования к защите обрабатываемых персональных данных в соответствии со [ст. 19](#) комментируемого закона.

На лицо, осуществляющее обработку персональных данных по поручению, возлагается обязанность соблюдения принципов и правил обработки персональных данных, распространяющихся на оператора персональных данных. При этом само это лицо не обязано получать согласие субъекта персональных данных на обработку его персональных данных. Эта обязанность возлагается исключительно на оператора. Соответственно, именно оператор персональных данных несет предусмотренную законом публично-правовую ответственность и частноправовую ответственность

перед субъектом персональных данных за нарушение порядка поручения обработки персональных данных третьему лицу. В свою очередь, лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Пример: 1 сентября 2009 г. между ООО "Н2" и собственниками помещений в многоквартирном доме заключен договор управления многоквартирным домом. В списке собственников жилых помещений данного дома указана М.

1 января 2012 г. между ООО "Н1" и ООО "Н2" заключен договор на оказание юридических услуг по представлению интересов заказчика в юрисдикционных органах, согласно которому ООО "Н1" как исполнитель принимает на себя обязательство представлять ООО "Н2" как заказчика в судах общей юрисдикции всех инстанций по взысканию задолженности граждан, проживающих в многоквартирных жилых домах г. Перми. Приложением к данному договору является перечень должников ООО "Н2" по состоянию на 2 декабря 2011 г., в котором помимо адреса, указаны фамилия и инициалы граждан, сумма задолженности и номер лицевого счета.

При первичном рассмотрении дела в мировом суде должностное лицо ООО "Н1" привлечено к административной ответственности по [ст. 13.11](#) КоАП. Судья исходил из того, что ООО "Н1" не поручалась обработка персональных данных М. в соответствии с [ч. 3 ст. 6](#) комментируемого закона.

При обжаловании решения в районном суде требования ООО "Н1" также были оставлены без удовлетворения, при этом в решении судья указал, что согласие субъекта персональных данных на их обработку третьим лицом не требовалось бы только в случае получения данного согласия оператором.

В [постановлении](#) Пермского краевого суда от 3 октября 2012 г. N 44А-834-2012 по данному делу отмечается, что судебные инстанции не учли положения [ч. 4 ст. 6](#) комментируемого закона, освобождающие лицо, осуществляющее обработку персональных данных по поручению оператора, от обязанности получать согласие субъекта таких данных на их обработку. Применение данных положений не поставлено в зависимость от выполнения оператором обязанностей в соответствии с положениями [ч. 3 ст. 6](#) комментируемого закона. Более того, в [ч. 5](#) приведенной статьи указано, что в случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Таким образом, заключил Суд, в действиях должностного лица ООО "Н1" не усматривается нарушения порядка сбора, хранения, использования или распространения информации о гражданах.

Несколько иной подход к определению правового статуса "субоператора" персональных данных прослеживается в европейском законодательстве. Согласно [ч. 5 ст. 22](#) Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами, если обрабатывающее данные третье лицо в нарушение законодательно определенных требований определяет цели и способы обработки, такое лицо должно считаться контролером в отношении указанной обработки.

Иными словами, рассматриваемая норма вводит презумпцию наличия правового статуса оператора персональных данных у любого субъекта, который, получив от иного оператора на условиях конфиденциальности и для достижения конкретной цели персональные данные, осуществляет их обработку вне определенных этим оператором рамок. Подобная презумпция позволяет вменять субъекту статус оператора персональных данных, а следовательно и привлекать его к соответствующей ответственности в случае нарушения конституционных прав человека и гражданина.

[Статья 7. Конфиденциальность персональных данных](#)

Комментируемая [статья](#) предусматривает распространение на персональные данные принципа-требования соблюдения конфиденциальности. Закрепленный принцип распространяется на действия операторов и иных лиц, получивших доступ к персональным данным иных лиц. Данное требование имеет следующее содержание: операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Таким образом, первичное условие раскрытия информации третьим лицам - наличие согласия субъекта, чьи персональные данные оказываются в ведении операторов и иных лиц по различным основаниям. Согласие субъекта на обработку его персональных данных должно быть конкретным, информированным и сознательным, в противном случае можно доказать фактическое отсутствие такого согласия. При этом обязанность доказать наличие такого согласия или обстоятельств, в силу которых такое согласие не требуется, возлагается на оператора либо иное третье лицо, получившее в связи с осуществлением своей основной деятельности доступ к персональным данным. Согласие должно содержать перечень действий с персональными данными путем их буквального перечисления, общее описание используемых оператором способов обработки персональных данных (см. [подробнее комментарий](#) к ст. 9).

Рассматриваемое правило нацелено на защиту персональных данных, защиту информационной безопасности участников общественных отношений, выступает гарантией неразглашения несанкционированных сведений.

Положение, предусмотренное комментируемой [статьей](#), трансформировано в отраслевое законодательство, детализируясь применительно к конкретным правоотношениям, развивающимся в конкретных отраслях и сферах государства и общества. Например, в развитие требований комментируемой статьи в сфере труда, организации взаимоотношений между работодателем и работником [ст. 88](#) ТК предусматривает, что при передаче персональных данных работника работодатель должен соблюдать следующие требования:

не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных [ТК](#) или иными федеральными законами;

не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном ТК и иными федеральными законами;

осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;

разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

передавать персональные данные работника представителям работников в порядке, установленном [ТК](#) и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

Можно привести и иные примеры применения закрепленного рассматриваемой статьей ограничения в рамках различных отраслевых правоотношений. В частности, в сфере науки и образования указанное ограничение подразумевает, что не допускается размещение в открытом доступе контактной информации (то есть персональных данных) лиц, представивших заявление о лишении ученой степени или апелляцию на решение диссертационного совета по вопросу присуждения ученой степени ([письмо](#) Минобрнауки от 11 октября 2018 г. N МН-06.4/571).

По вопросам применения комментируемой [статьи](#) уполномоченными субъектами применительно к персональным данным, значимым для различных отраслей и сфер, принимаются подзаконные разъясняющие, детализирующие законоположения акты, в том числе правоприменительного характера, например:

применительно к сфере науки и образования - [письмо](#) Минобрнауки от 8 октября 2015 г. N ВК-2569/07, [письмо](#) Минобрнауки от 11 октября 2018 г. N МН-06.4/571;

применительно к сфере оформления недвижимости, межевания, ведения кадастра - [письмо](#) ФГБУ "ФКП Росреестра" от 5 мая 2014 г. N 11-1635-КЛ, письмо Минэкономразвития от 4 сентября 2014 г. N Д23и-3079;

применительно к сфере труда, взаимоотношений работника и работодателя - письмо Роскомнадзора от 7 февраля 2014 г. N 08КМ-3681 "О передаче работодателем третьим лицам сведений о заработной плате работников" и др.

Применительно к распространению персональных данных, например в сети Интернет, как форме раскрытия персональных данных третьим лицам (точнее, неопределенному кругу лиц), приняты специальные правила, также относящиеся к отраслевым общественным отношениям, например:

[приказ](#) Минобрнауки от 16 апреля 2014 г. N 326 "Об утверждении Порядка размещения в информационно-телекоммуникационной сети "Интернет" информации, необходимой для обеспечения порядка присуждения ученых степеней";

[методические рекомендации](#) по созданию и размещению в сети Интернет и средствах массовой информации видеосюжетов о детях, оставшихся без попечения родителей, а также иной производной информации указанной категории детей с целью реализации права детей жить и

воспитываться в семье, направленные [ПИСЬМОМ](#) Минобрнауки от 8 октября 2015 г. N ВК-2569/07.

Комментируемая [статья](#), по сути, предполагает бланкетную норму. Исходя из ее буквального содержания, специальными федеральными законами может быть предусмотрена возможность (разрешение) для операторов и иных лиц, получивших доступ к персональным данным, раскрывать третьим лицам и распространять персональные данные без согласия субъекта персональных данных - как исключение из содержания принципа конфиденциальности персональных данных.

Согласно системному анализу законодательства Российской Федерации, "иное", то есть разрешение закона получать и обрабатывать персональные данные без согласия субъекта персональных данных, предусмотрено специальными актами законодательства. Например, действуют следующие нормы:

1) Негосударственный пенсионный фонд вправе с учетом требований, закрепленных в [ч. 3 ст. 6](#) комментируемого закона, поручить обработку персональных данных организациям, которые в соответствии с договором осуществляют ведение пенсионных счетов в случаях, если указание на такие организации содержится в правилах фонда, а также иным организациям, если это необходимо для исполнения пенсионного договора, договора об обязательном пенсионном страховании. Речь идет о персональных данных вкладчиков - физических лиц, страхователей - физических лиц, участников, застрахованных лиц, выгодоприобретателей, правопреемников участников и застрахованных лиц. В указанных случаях фонд не обязан получать согласие субъектов персональных данных на дачу поручения обработки персональных данных третьим лицам ([ст. 15](#) Федерального закона от 7 мая 1998 г. N 75-ФЗ "О негосударственных пенсионных фондах").

2) Негосударственный пенсионный фонд может передать конфиденциальную информацию о вкладчиках - физических лицах, страхователях - физических лицах, участниках, застрахованных лицах, выгодоприобретателях и правопреемниках участников и застрахованных лиц, их персональные данные специализированному депозитарию фонда в связи с осуществлением им функций, предусмотренных [Федеральным законом](#) от 7 мая 1998 г. N 75-ФЗ "О негосударственных пенсионных фондах" и другими федеральными законами, правопреемникам участников и застрахованных лиц, а также в установленных законодательством Российской Федерации случаях по требованию следственных, судебных, налоговых органов, Банка России, Агентства по страхованию вкладов ([ст. 15](#) Федерального закона от 7 мая 1998 г. N 75-ФЗ "О негосударственных пенсионных фондах").

3) Страхователи применительно к сфере трудовых правоотношений (данный статус имеют, как правило, работодатели) предоставляют в соответствующий орган ПФР сведения о работающих у них застрахованных лицах без их согласия. Речь идет о персональных данных следующего содержания:

страховой номер;

фамилия, имя, отчество, фамилия, которая была у физического лица при рождении;

дата рождения;

место рождения;

пол;

адрес постоянного места жительства;

серия и номер паспорта или удостоверения личности, дата выдачи документов, на основании которых в индивидуальный лицевой счет включены необходимые сведения, наименование выдавшего их органа;

гражданство.

Также дополнительно представляются сведения следующего перечня:

страховой номер индивидуального лицевого счета;

фамилия, имя и отчество;

дата приема на работу (для застрахованного лица, принятого на работу данным страхователем в течение отчетного периода) или дата заключения договора гражданско-правового характера, на вознаграждение по которому в соответствии с законодательством начисляются страховые взносы;

дата увольнения (для застрахованного лица, уволенного данным страхователем в течение отчетного периода) или дата прекращения договора гражданско-правового характера, на вознаграждение по которому в соответствии с законодательством Российской Федерации начисляются страховые взносы;

периоды деятельности, включаемые в стаж на соответствующих видах работ, определяемый особыми условиями труда, работой в районах Крайнего Севера и приравненных к ним местностях;

другие сведения, необходимые для правильного назначения страховой пенсии и накопительной пенсии;

суммы пенсионных взносов, уплаченных за застрахованное лицо, являющееся субъектом системы досрочного негосударственного пенсионного обеспечения;

периоды трудовой деятельности, включаемые в профессиональный стаж застрахованного лица,

являющегося субъектом системы досрочного негосударственного пенсионного обеспечения;

документы, подтверждающие право застрахованного лица на досрочное назначение страховой пенсии по старости.

Страхователь также представляет в территориальные органы ПФР либо через МФЦ сведения, предусмотренные [ч. 4 ст. 9](#) Федерального закона от 30 апреля 2008 г. N 56-ФЗ "О дополнительных страховых взносах на накопительную пенсию и государственной поддержке формирования пенсионных накоплений":

общая сумма перечисляемых средств, включающая в себя сумму всех перечисляемых дополнительных страховых взносов на накопительную пенсию (сумму всех уплачиваемых взносов работодателя);

номер платежного поручения и дата его исполнения;

страховой номер индивидуального лицевого счета каждого застрахованного лица;

фамилия, имя и отчество каждого застрахованного лица;

сумма перечисляемых дополнительных страховых взносов на накопительную пенсию каждого застрахованного лица (сумма взносов работодателя, уплачиваемых в пользу каждого застрахованного лица);

период уплаты.

Страхователем представляются сведения о каждом работающем у него застрахованном лице (включая лиц, заключивших договоры гражданско-правового характера, предметом которых являются выполнение работ, оказание услуг, договоры авторского заказа, договоры об отчуждении исключительного права на произведения науки, литературы, искусства, издательские лицензионные договоры, лицензионные договоры о предоставлении права использования произведения науки, литературы, искусства, в том числе договоры о передаче полномочий по управлению правами, заключенные с организацией по управлению правами на коллективной основе):

страховой номер индивидуального лицевого счета;

фамилия, имя и отчество;

ИНН (при наличии у страхователя данных об идентификационном номере налогоплательщика застрахованного лица) ([подпп. 1-8 п. 2 ст. 6](#), [ст. 9](#), [ст. 11](#) Федерального закона от 1 апреля 1996 г. N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования").

Федеральный закон от 1 апреля 1996 г. N 27-ФЗ в [п. 1 ст. 9](#) закрепил следующие случаи предоставления страхователем указанных сведений о работающих у него застрахованных лицах ПФР как третьему лицу:

при начальной регистрации застрахованных лиц для индивидуального (персонифицированного) учета в системе обязательного пенсионного страхования;

при приеме на работу граждан или при заключении с гражданами договоров гражданско-правового характера, на вознаграждения по которым в соответствии с законодательством Российской Федерации начисляются страховые взносы, если в отношении этих физических лиц не открыт индивидуальный лицевой счет;

при ликвидации, реорганизации юридического лица, прекращении физическим лицом деятельности в качестве индивидуального предпринимателя, снятии с регистрационного учета в качестве страхователя - работодателя адвоката, нотариуса, занимающегося частной практикой;

при изменении соответствующих сведений.

4) Работодатель вправе предоставить третьим лицам персональные данные работника без его согласия в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных [ст. 88](#) ТК или иными федеральными законами. К иным федеральным законам в данном случае могут быть отнесены, например, следующие федеральные законы:

Федеральный закон от 2 октября 2007 г. N 229-ФЗ "Об исполнительном производстве" ([ч. 10 ст. 65](#));

Федеральный закон от 1 апреля 1996 г. N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования" ([ст. 9](#), [11](#));

Федеральный закон от 7 февраля 2011 г. N 3-ФЗ "О полиции" ([ст. 13](#));

Федеральный закон от 17 января 1992 г. N 2202-1 "О прокуратуре Российской Федерации" ([п. 2.1 ст. 4](#));

Федеральный закон от 21 июля 1997 г. N 118-ФЗ "Об органах принудительного исполнения Российской Федерации" ([п. 2 ст. 12](#), [п. 2 ст. 14](#)).

5) Любой субъект, будь то гражданин, организация вне зависимости от организационно-правовой формы, обязан предоставлять сведения о персональных данных без согласия лиц, которых эти данные характеризуют, по запросу полиции в связи с расследуемыми уголовными

делами и находящимися в производстве делами об административных правонарушениях, а также в связи с проверкой зарегистрированных в установленном порядке заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях, разрешение которых отнесено к компетенции полиции ([ст. 13](#) Федерального закона от 7 февраля 2011 г. N 3-ФЗ "О полиции").

6) Любой субъект, будь то гражданин, организация вне зависимости от организационно-правовой формы, обязан предоставлять сведения о персональных данных, находящихся в их ведении, по запросу органов прокуратуры ([п. 2.1 ст. 4](#) Федерального закона от 17 января 1992 г. N 2202-1 "О прокуратуре Российской Федерации").

7) Поднадзорные Центральному банку РФ организации (в том числе банковские и небанковские кредитные организации) и участники платежной системы Российской Федерации обязаны представлять Центральному Банку РФ документы и иную необходимую информацию, в том числе содержащую персональные данные о клиентах кредитных организаций и иных субъектах, обратившихся к платежной системе Российской Федерации. Согласие данных субъектов не требуется ([п. 3 ст. 32](#) Федерального закона от 27 июня 2011 г. N 161-ФЗ "О национальной платежной системе").

8) Центральный банк РФ в установленном им порядке вправе запрашивать и получать на безвозмездной основе от федеральных органов исполнительной власти, их территориальных органов и иных лиц необходимую информацию, в отношении которой установлены требования, обеспечивающие ее конфиденциальность, в том числе информацию, содержащую персональные данные и касающуюся деятельности некредитных финансовых организаций (их руководителей, учредителей (участников), и в установленном им порядке осуществлять действия по обработке персональных данных ([ст. 76.7](#) Федерального закона от 10 июля 2002 г. N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)").

По вопросам порядка обращения информации, в том числе содержащей персональные данные, с участием Центрального банка РФ приняты специальные акты:

положение Банка России от 27 декабря 2017 г. N 625-П "О порядке согласования Банком России назначения (избрания) кандидатов на должности в финансовой организации, уведомления Банка России об избрании (прекращении полномочий), назначении (освобождении от должности) лиц, входящих в состав органов управления, иных должностных лиц в финансовых организациях, оценки соответствия квалификационным требованиям и (или) требованиям к деловой репутации лиц, входящих в состав органов управления, иных должностных лиц и учредителей (акционеров, участников) финансовых организаций, направления членом совета директоров (наблюдательного совета) финансовой организации информации в Банк России о голосовании (о непринятии участия в голосовании) против решения совета директоров (наблюдательного совета) финансовой организации, направления запроса о предоставлении Банком России информации и направления Банком России ответа о наличии (отсутствии) сведений в базах данных, предусмотренных статьями 75 и 76.7 Федерального закона от 10 июля 2002 г. N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)", а также о порядке ведения таких баз";

инструкция Банка России от 27 июля 2018 г. N 190-И "О перечне документов, подтверждающих соблюдение лицензионных условий и представляемых для получения лицензии на осуществление деятельности инвестиционного фонда, лицензии управляющей компании на осуществление деятельности по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами, лицензии на осуществление деятельности специализированного депозитария инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, порядке предоставления лицензии, переоформления документа, подтверждающего наличие лицензии, оформления и представления документов для получения лицензии и переоформления документа, подтверждающего наличие лицензии, форме заявления о предоставлении лицензии, форме документа, подтверждающего наличие лицензии, порядке ведения реестров лицензий и порядке предоставления выписок из них";

указание Банка России от 21 декабря 2017 г. N 4658-У "О порядке и сроке направления уведомления лицом, которое прямо или косвенно получило право распоряжения 10 и более процентами голосов, принадлежащих на голосующие акции (доли), составляющие уставный капитал профессионального участника рынка ценных бумаг, микрокредитной компании, ломбарда, а также о порядке запроса Банком России информации о лицах, которые прямо или косвенно имеют право распоряжения 10 и более процентами голосов, принадлежащих на голосующие акции (доли), составляющие уставный капитал профессионального участника рынка ценных бумаг, микрокредитной компании, ломбарда".

9) Граждане и организации предоставляют по требованию сотрудника органов принудительного исполнения информацию, в том числе персональные данные об иных лицах без их согласия, в объеме, необходимом для деятельности органов принудительного исполнения ([п. 2 ст. 14](#) Федерального закона

от 21 июля 1997 г. N 118-ФЗ "Об органах принудительного исполнения Российской Федерации").

10) Предоставление сведений в рамках проведения уполномоченными субъектами антикоррупционных мероприятий осуществляется в соответствии с Федеральными законами от 3 декабря 2012 г. N 230-ФЗ "О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам", от 25 декабря 2008 г. N 273-ФЗ "О противодействии коррупции" с последующим размещением в сети Интернет персональных данных, допустимых для того размещения (п. 4 ст. 8 Федерального закона от 3 декабря 2012 г. N 230-ФЗ; п. 4 ст. 8.1 Федерального закона от 25 декабря 2008 г. N 273-ФЗ "О противодействии коррупции").

11) Оператор связи имеет право предоставить персональные данные, поручить обработку персональных данных абонента-гражданина третьему лицу в целях заключения и (или) исполнения договора об оказании услуг связи, стороной которого является абонент-гражданин, и (или) в целях осуществления прав и законных интересов оператора связи или абонента-гражданина. В таком случае согласие абонента-гражданина на это поручение, в том числе на передачу его персональных данных такому третьему лицу, обработку персональных данных таким третьим лицом в соответствии с поручением оператора связи, не требуется (п. 1 ст. 53 Федерального закона от 7 июля 2003 г. N 126-ФЗ "О связи").

12) Физические и юридические лица, являющиеся учредителями или участниками юридического лица или иным образом контролирующие его, обязаны представлять данному юридическому лицу имеющуюся у них информацию (в том числе персональные данные), необходимую для установления его бенефициарных владельцев.

Юридическое лицо обязано представлять имеющуюся документально подтвержденную информацию о своих бенефициарных владельцах либо о принятых мерах по установлению в отношении своих бенефициарных владельцев сведений, предусмотренных абз. 2 подп. 1, п. 1 ст. 7 Федерального закона от 7 августа 2001 г. N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма", по запросу уполномоченного органа или налоговых органов (п. 5, 6 ст. 6.1 Федерального закона от 7 августа 2001 г. N 115-ФЗ)*(45).

13) Налоговые органы, таможенные органы, ПФР, ФСС, кредитные организации представляют персональные данные по запросу государственного заказчика в рамках государственного оборонного заказа. Перечень информации и документов, порядок и сроки их представления определяются соглашением о взаимодействии налоговых органов, таможенных органов, ПФР, ФСС с государственным заказчиком (абз. 4 ст. 6.2 Федерального закона от 29 декабря 2012 г. N 275-ФЗ "О государственном оборонном заказе").

14) Разрешается обращение (взаимообмен, обработка) информации, содержащей персональные данные, в целях предоставления государственных и муниципальных услуг, между органами, предоставляющими государственные услуги, органами, предоставляющими муниципальные услуги, иными государственными органами, органами местного самоуправления, подведомственными государственными органами или органами местного самоуправления, многофункциональными центрами (ч. 4 ст. 7 Федерального закона от 27 июля 2010 г. N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг").

15) Нотариус имеет право на получение персональных данных от конкретного лица о третьих лицах для совершения нотариальных действий (ст. 15 Основ законодательства Российской Федерации о нотариате от 11 февраля 1993 г. N 4462-1).

16) Органы федеральной службы безопасности имеют право на получение персональных данных для выполнения возложенных на них обязанностей от любых субъектов, деятельность которых и находящаяся в ведении которых информация могут быть необходимы для выяснения фактических обстоятельств органами федеральной службы безопасности (ст. 13 Федерального закона от 3 апреля 1995 г. N 40-ФЗ "О федеральной службе безопасности").

17) Совет по совершенствованию третейского разбирательства вправе запрашивать у некоммерческих организаций, при которых создаются постоянно действующие арбитражные учреждения, органов государственной власти и органов местного самоуправления, иных организаций документы и сведения, в том числе содержащие персональные данные (ч. 7 ст. 44 Федерального закона от 29 декабря 2015 г. N 382-ФЗ "Об арбитраже (третейском разбирательстве) в Российской Федерации").

18) Субъекты официального статистического учета в целях формирования официальной статистической информации получают от респондентов первичные статистические данные и административные данные, в том числе содержащие сведения, отнесенные к персональным данным (ч. 9 ст. 5 Федерального закона от 29 ноября 2007 г. N 282-ФЗ "Об официальном статистическом учете и системе государственной статистики в Российской Федерации").

Из приведенного перечня положений федеральных законов, допускающих раскрывать третьим лицам и распространять персональные данные без согласия субъекта персональных данных, видно, что

в большинстве случаев соответствующая информация предоставляется по запросам уполномоченных субъектов.

При этом важно учитывать наличие у субъекта необходимого полномочия на запрос информации с персональными данными. Иными словами, персональные данные могут быть предоставлены по запросам не любого субъекта. Несмотря на очевидность данного подразумеваемого комментируемой статьей требования, на практике имеется немало правовых споров о его несоблюдении.

Пример: решение от 7 апреля 2019 г., [постановление](#) Пятого арбитражного апелляционного суда от 22 мая 2019 г., [постановление](#) Арбитражного суда Дальневосточного округа от 25 июля 2019 г. по делу N A24-1527/2019 вынесены в связи с обращением финансового управляющего с иском к краевому управлению МВД о признании незаконным отказа в предоставлении информации о наличии или отсутствии у должника-гражданина судимости за совершение умышленного преступления в сфере экономики, а также о привлечении к административной ответственности. Суд отказал в удовлетворении иска, суды вышестоящих инстанций оставили решение суда в силе. Отказ в удовлетворении иска мотивирован отсутствием правовых оснований предоставления органами внутренних дел Российской Федерации сведений по запросам финансовых управляющих в отношении физических лиц. Оспариваемый отказ соответствует закону и не нарушает права и законные интересы финансового управляющего (см. также аналогичные судебные решения: [постановление](#) Арбитражного суда Дальневосточного округа от 20 июня 2019 г. N Ф03-2342/2019 по делу N A51-19080/2018; [постановление](#) Арбитражного суда Дальневосточного округа от 16 ноября 2018 г. N Ф03-5016/2018 по делу N A59-1219/2018; [постановление](#) Арбитражного суда Северо-Кавказского округа от 17 сентября 2018 г. N Ф08-7169/2018 г. по делу N A63-14832/2017).

Вопросы применения и толкования комментируемой нормы на практике послужили предметом внимания Конституционного Суда РФ, который вынес ряд актов в отношении настоящего федерального закона в пределах своей компетенции, например:

[определение](#) Конституционного Суда РФ от 23 июня 2015 г. N 1537-О "Об отказе в принятии к рассмотрению жалобы граждан Барановой Елены Валентиновны и Тыщенко Елены Владимировны на нарушение их конституционных прав положениями статьи 7 Федерального закона "О персональных данных", пункта 7 статьи 55 Федерального закона "О связи" и части 1 статьи 18 Федерального закона "О рекламе";

[определение](#) Конституционного Суда РФ от 28 января 2016 г. N 100-О "Об отказе в принятии к рассмотрению жалобы гражданина Шалбина Дмитрия Алексеевича на нарушение его конституционных прав статей 7 Федерального закона "О персональных данных";

[определение](#) Конституционного Суда РФ от 9 февраля 2016 г. N 220-О "Об отказе в принятии к рассмотрению жалобы граждан Матросовой Татьяны Акимовны и Рассказовой Людмилы Анатольевны на нарушение их конституционных прав положением пункта 6 статьи 181.4 Гражданского кодекса Российской Федерации";

[определение](#) Конституционного Суда РФ от 7 июля 2016 г. N 1423-О "Об отказе в принятии к рассмотрению жалобы религиозной организации "Церковь евангельских христиан "Назарет" на нарушение конституционных прав и свобод подпунктом 2 пункта 4 статьи 181.2 Гражданского кодекса Российской Федерации".

Пример: соответствие комментируемой статьи [Конституции](#) было поставлено под сомнение, в связи с чем в 2016 году имело место обращение в Конституционный Суд РФ. Как следует из материалов судебного дела, гражданин Ш. - директор организации, осуществляющей управление многоквартирными домами, постановлением мирового судьи, оставленным без изменений постановлением вышестоящего суда, за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) был привлечен к административной ответственности, предусмотренной [ст. 13.11](#) КоАП.

Суды указали, что нарушение выразилось в передаче персональных данных жильцов, имеющих долги по оплате коммунальных услуг, без их согласия организации, оказывающей Ш. юридические услуги, в том числе по взысканию соответствующей задолженности в судебном порядке. Совершение данного правонарушения подтверждено договором на оказание юридических услуг, копиями исковых заявлений и доверенности. По мнению заявителя, оспариваемое законоположение ограничивает право на получение квалифицированной юридической помощи, а потому противоречит [ст. 48](#) Конституции.

Конституционный Суд РФ, изучив представленные материалы, не нашел оснований для принятия данной жалобы к рассмотрению. Как пояснил Конституционный Суд РФ, управляющая организация, с тем чтобы иметь возможность осуществлять деятельность по управлению

многоквартирным домом, обязана получить у собственников и нанимателей жилых помещений согласие на обработку персональных данных, в том числе на их передачу третьим лицам, причем данное согласие может быть включено в качестве условия в договор управления многоквартирным домом. Минстрой, утвердивший [приказом](#) от 31 июля 2014 г. N 411/пр Примерные условия договора управления многоквартирным домом и [методических рекомендаций](#) по порядку организации и проведению общих собраний собственников помещений в многоквартирных домах, также рекомендовал включать в такие договоры условие о порядке информационного взаимодействия между управляющей организацией и собственниками или пользователями помещений в многоквартирном доме, в том числе состав, порядок, случаи и сроки предоставления информации, связанной с порядком обработки персональных данных собственников и пользователей помещений в многоквартирном доме ([подп. "д" п. 12](#)). В приложение к договору рекомендовано включать порядок обработки персональных данных граждан, в том числе собственников помещений в многоквартирном доме и пользователей помещений в многоквартирном доме, для целей исполнения договора управления ([подп. "з" п. 25](#)).

Принимая во внимание указанную обязанность управляющей организации, оспариваемое положение комментируемой статьи, обуславливающее возможность предоставления оператором персональных данных третьему лицу согласием на то субъекта персональных данных, не может рассматриваться как нарушающее конституционное право на получение квалифицированной юридической помощи ([ст. 48 Конституции](#)) в указанном заявителем аспекте (см. [определение Конституционного Суда РФ](#) от 28 января 2016 г. N 100-О).

В связи с несанкционированным сообщением персональных данных третьим лицам, разглашением конфиденциальной информации, то есть с несоблюдением положений комментируемой статьи, в судебной практике рассмотрено немало юридических споров. Зачастую они вызваны опубликованием материалов, содержащих персональные данные, в газетах и журналах (см. [постановление](#) Арбитражного суда Волго-Вятского округа от 20 марта 2018 г. N Ф01-449/2018 г. по делу N А43-11782/2017), иных средствах массовой информации, в сети Интернет ([постановление](#) Арбитражного суда Московского округа от 27 февраля 2019 г. N Ф05-1619/2019 г. по делу N А41-20183/18).

[Статья 8. Общедоступные источники персональных данных](#)

1. [Часть 1](#) комментируемой статьи раскрывает сущность, цель создания и примерное содержание общедоступных источников персональных данных (далее - ОИПД).

В качестве цели названо информационное обеспечение без указания обеспечиваемой деятельности или процесса. Полагаем, подобная формулировка указывает на максимально широкую интерпретацию причинного комплекса создания ОИПД, оставляя его на усмотрение лица или организации, создающих такой источник. Очевидно, что данное лицо или организация будут являться операторами персональных данных, содержащихся в общедоступном источнике.

Сущность ОИПД, соответственно, заключается в обеспечении доступа к персональным данным формально неопределенного круга заинтересованных лиц. Законодателем в качестве примеров приведены такие формы ОИПД, как справочники и адресные книги, что позволяет судить об их предназначении - обеспечение служебной и межличностной коммуникации. Вместе с тем, дискреционная формулировка "в том числе" указывает на неопределенный перечень целей и форм создания ОИПД.

На сегодняшний день наиболее крупными ОИПД являются социальные сети: "ВКонтакте" (ежемесячное посещение 40,97 млн. человек), "Instagram" (33,9 млн. человек), "Одноклассники" (24 млн. человек) и "Facebook" (22,2 млн. человек).

В комментируемой [части](#) закреплён примерный перечень персональных данных, которые могут содержаться в общедоступном источнике: фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии. Содержание конкретного ОИПД может как включать не указанные выше данные, так и не содержать некоторые из них.

Следует отметить, что ОИПД формируется только на основании письменного согласия субъекта персональных данных, что не позволяет отнести к таковым базы и банки персональных данных, которые создаются на основании прямых законодательных указаний. Данное обстоятельство не исключает из перечня потенциальных операторов ОИПД государственные и муниципальные органы, так как для обеспечения собственных нужд ими также могут создаваться ОИПД (например, телефонный справочник с данными сотрудников). Независимо от ведомственной принадлежности и организационной формы оператор, создающий ОИПД, должен получить согласие на обработку персональных данных каждого субъекта.

В соответствии с [п. 10 ч. 1 ст. 6](#) и [п. 2 ч. 2 ст. 10](#) комментируемого закона без согласия субъекта могут быть обработаны персональные данные, сделанные им общедоступными. Согласно [п. 3](#)

ч. 4 ст. 18 комментируемого закона оператор освобождается от обязанности уведомить субъекта об обработке персональных данных в случае, если персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника. Следовательно, необходимо различать общедоступные персональные данные и общедоступные источники персональных данных, при этом основания разграничения этих двух категорий в настоящем федеральном законе не разъяснены.

Общедоступные персональные данные являются разновидностью общедоступной информации, чье определение раскрыто в **ст. 7** ФЗ "Об информации, информационных технологиях и о защите информации", - это 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.

Полагаем, общедоступные персональные данные выступают содержанием как ОИПД, так и информационных систем (баз и банков данных), которые формируются, обновляются и эксплуатируются на основании требований законодательства. Так, согласно **ч. 4 ст. 22** комментируемого закона общедоступными являются персональные данные, содержащиеся в реестре операторов, который ведется уполномоченным органом по защите прав субъектов персональных данных (Роскомнадзором) в силу требований **п. 3 ч. 5 ст. 23** комментируемого закона. Указанный реестр не может быть признан ОИПД, однако содержащиеся в нем персональные данные очевидно являются общедоступными.

2. Согласно **ч. 2** комментируемой статьи сведения о субъекте персональных данных должны быть в любое время исключены из ОИПД по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов, в качестве которых зачастую выступают Роскомнадзор и прокуратура.

Неопределенность момента исключения персональных данных из открытого источника, обусловленная формулировкой "в любое время", нивелируется принципами обработки персональных данных (см. [комментарий](#) к ст. 2) и обязанностями оператора персональных данных (см. [комментарий](#) к ч. 1 ст. 21).

Следует говорить об обязанности оператора исключить персональные данные из общедоступного источника незамедлительно после получения заявления субъекта персональных данных об исключении обнаруженных им в ОИПД сведений или об отзыве ранее данного согласия на обработку персональных данных (см. [комментарий](#) к ч. 2 ст. 9). Заявитель не обязан обосновывать мотив и основания исключения персональных данных из общедоступного источника, однако он и его данные должны быть точно идентифицированы.

В связи с этим представляется, что обязательными содержательными элементами такого заявления должны быть:

- фамилия, имя, отчество и адрес (место регистрации) субъекта персональных данных;
- полные выходные данные издания или сетевой адрес ОИПД в сети Интернет;
- однозначно интерпретируемое требование об исключении персональных данных заявителя-субъекта из общедоступного источника.

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

Комментируемая **статья** состоит из девяти частей и определяет правовую сущность, порядок и условия подачи, а также отзыва согласия субъекта персональных данных на обработку его персональных данных. Согласие имеет гражданско-правовую, диспозитивную природу и обеспечивает защиту конфиденциальности персональных данных посредством установления обязанности оператора персональных данных получить однозначно интерпретируемое и верифицируемое согласие субъекта персональных данных на их обработку.

Исключения из этого правила должны быть прямо определены в законе и вытекать либо из положений **ч. 3 ст. 55** Конституции, либо из договорных отношений между субъектом и оператором персональных данных.

Часть 1 комментируемой статьи определяет общий порядок подачи согласия субъекта персональных данных на обработку его персональных данных и условия, при котором его получение позволяет оператору обрабатывать такие данные.

Так, субъект персональных данных принимает решение о предоставлении его данных и дает конкретное, информированное и сознательное согласие на их обработку свободно, своей волей и в своем интересе. Иными словами, условиями допустимости принятия оператором персональных данных согласия выступают:

- добровольность согласия, опирающаяся на осознание субъектом возможности отказа от дачи согласия, и отсутствие принуждения субъекта персональных данных к даче согласия;

активность субъекта персональных данных выражается в предоставлении согласия посредством активных действий, исключающих ошибочное толкование его намерения;

конкретность согласия выражается в точном определении перечня раскрываемых персональных данных и также идентификации личности субъекта персональных данных при даче согласия;

информированность согласия обеспечивается посредством сообщения субъекту персональных данных целей, сроков, способов и средств обработки данных, информации о получающих к ним доступ операторах, а также иной значимой информации;

осознанность выражается в понимании правовых последствий дачи согласия, она также обусловлена полной дееспособностью дающего согласие субъекта.

Субъект персональных данных или его законный представитель вправе дать согласие на обработку персональных данных в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

Исследователи выделяют следующие типичные формы дачи согласия:

письменный документ, подписанный собственноручной подписью субъекта персональных данных;

согласие в устной форме при условии аудиальной или видеоаудиальной его фиксации, о которых субъект персональных данных должен быть предупрежден заблаговременно;

согласие в конклюдентной форме (предоставление визитной карточки, предоставление анкеты или резюме, письменного обращения к оператору персональных данных с указанием собственных персональных данных);

электронный документ, подписанный **простой электронной подписью** в виде СМС;

электронная форма с простой электронной подписью в виде "галочки";

согласие в электронном письме с авторизованного адреса электронной почты субъекта персональных данных;

электронная форма с проставлением обычной "галочки"*(46).

Подача согласия на обработку персональных данных субъектом в определенной форме предусмотрена ч. 4 комментируемой статьи. Согласно этой норме в предусмотренных федеральным законом случаях обработка персональных данных осуществляется на основании согласия субъекта персональных данных только в письменной форме: на бумажном носителе с собственноручной подписью субъекта или в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Подобные требования предъявляются к обработке специальной категории персональных данных (см. **комментарий** к п. 1 ч. 2 ст. 10), биометрических данных (см. **комментарий** к ч. 1 ст. 11), а также при трансграничной передаче персональных данных (см. **комментарий** к п. 1 ч. 4 ст. 12).

Письменное согласие субъекта персональных данных на бумажном носителе должно включать в себя следующие реквизиты:

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

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

наименование или 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;

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

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

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

подпись субъекта персональных данных.

Бланк типового согласия на обработку персональных данных размещен на официальном сайте Роскомнадзора (<https://54.rkn.gov.ru/protection/docsamples>).

Составление письменного согласия субъекта персональных данных в форме электронного документа не всегда позволяет включить в него все указанные выше реквизиты, что обусловлено особенностями подписания его электронной подписью. Вместе с тем это обстоятельство не освобождает

оператора от обязанности стремиться включить в согласие максимальное число этих реквизитов. Разновидности электронных подписей нормативно закреплены в [ст. 5](#) Федерального закона от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".

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

[Неквалифицированной электронной подписью](#) является электронная подпись, которая: получена в результате криптографического преобразования информации с использованием ключа электронной подписи; позволяет определить лицо, подписавшее электронный документ; позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания; создается с использованием средств электронной подписи.

[Квалифицированной электронной подписью](#) является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам: ключ проверки электронной подписи указан в квалифицированном сертификате; для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с [Федеральным законом](#) от 6 апреля 2011 г. N 63-ФЗ.

[Часть 5](#) комментируемого закона содержит отсылочную норму к нормативному правовому акту Правительства, устанавливая особый порядок получения согласия в форме электронного документа в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг.

Согласно [п. 2](#) постановления Правительства РФ от 25 июня 2012 г. N 634 "О видах электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг" при обращении за получением государственных и муниципальных услуг допускается использование простой электронной подписи и (или) усиленной квалифицированной электронной подписи. Порядок использования простой электронной подписи при оказании государственных и муниципальных услуг утвержден [постановлением](#) Правительства РФ от 25 января 2013 г. N 33, а усиленной квалифицированной электронной подписи, - [постановлением](#) Правительства РФ от 25 августа 2012 г. N 852.

[Часть 2](#) комментируемой статьи предусматривает возможность отзыва ранее данного согласия на обработку персональных данных соответствующим субъектом. Очевидно, что к процедуре отзыва предъявляются те же требования и условия, что и к процедуре дачи согласия на обработку персональных данных (см. [комментарий](#) к ч. 1 настоящей статьи), при этом форма подачи отзыва специально не оговаривается. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить их обработку, если имеются основания для обработки персональных данных независимо от согласия субъекта персональных данных (см. комментарии к [пп. 2-11 ч. 1 ст. 6](#), [ч. 2 ст. 10](#) и [ч. 2 ст. 11](#)). В отношении одних и тех же персональных данных могут иметь место одно и более оснований для обработки без согласия субъекта, при этом доказывание наличия таких оснований возлагается на оператора.

Согласно [ч. 3](#) комментируемой статьи обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, позволяющих обрабатывать персональные данные независимо от согласия субъекта персональных данных, возлагается на оператора. Адресатом представления доказательств могут выступать как сам субъект персональных данных, так и органы государственной власти (например, Роскомнадзор) или прокуратура.

Согласие на обработку персональных данных субъекта, ограниченно дееспособного или недееспособного в силу возраста или на основании судебного решения, дается его (законным) представителем ([ч. 6](#) комментируемой статьи). Таковыми для несовершеннолетних выступают родители, а также при их отсутствии, - опекуны или попечители, в том числе должностные лица учреждений, в которых они содержатся, воспитываются или обучаются. Законный представитель ограниченно дееспособного совершеннолетнего лица определяется судом. Представитель дееспособного совершеннолетнего лица может быть определен им самостоятельно посредством составления доверенности. По общему правилу срок действия доверенности определяется в ее тексте, при отсутствии же подобного упоминания срок ее действия по умолчанию составляет один год со дня подписания доверенности. Дата подписания (составления, выдачи) доверенности является обязательным реквизитом, без него доверенность ничтожна. Комментируемый закон не предусматривает обязанность нотариального заверения выданной доверенности, однако подобное действие может существенно упростить верификацию полномочий представителя субъекта персональных данных и ускорить рассмотрение его обращения оператором персональных данных. В случае смерти субъекта обработка

его персональных данных может быть осуществлена на основании согласия, которое дают наследники субъекта персональных данных, или согласия, которое было дано самим субъектом персональных данных при жизни ([ч. 7](#) комментируемой статьи).

При получении согласия на обработку персональных данных от (законного) представителя субъекта персональных данных оператор обязан удостовериться в его полномочиях посредством истребования соответствующего официального документа (свидетельство о рождении, удостоверение опекуна, попечителя, приемного родителя, патронатного воспитателя, договора, доверенности и т. д.).

Наличие оснований, позволяющих обрабатывать персональные данные независимо от согласия субъекта персональных данных, устанавливается и подтверждается оператором в форме, обусловленной правовой сущностью применяемого основания (см. комментарии к [пп. 2-11 ч. 1 ст. 6](#), [ч. 2 ст. 10](#) и [ч. 2 ст. 11](#)). Например, основанием обработки персональных данных согласно [п. 4 ч. 1 ст. 6](#) комментируемого закона будет являться регистрация субъекта персональных данных на портале государственных (муниципальных) услуг или предоставление субъекту персональных данных государственной или муниципальной услуги на основании его заявления. Бремя ответственности за ненадлежащим образом проведенную проверку наличия оснований для обработки персональных данных ложится на оператора. Следует отметить, что при подтверждении наличия указанных выше оснований оператор вправе осуществлять оборот персональных данных, полученных как от самого субъекта или его (законного) представителя, так и от третьих лиц, обладающих этими персональными данными на законных основаниях ([ч. 8](#) комментируемой статьи).

[Федеральным законом](#) от 30 декабря 2020 г. N 519-ФЗ комментируемая статья дополнена [ч. 9](#), согласно которой требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, устанавливаются уполномоченным органом по защите прав субъектов персональных данных (см. [комментарий](#) к [ст. 23](#)).

Таким образом, Роскомнадзор сможет посредством ведомственного нормотворчества дополнять форму и содержание согласия на обработку персональных данных, оперативно реагируя на развитие информационных правоотношений, появление новых информационно-телекоммуникационных технологий и изменения в административной судебной практике применения комментируемого закона.

[Статья 10](#). Специальные категории персональных данных

1. Комментируемая статья содержит пять частей, в которых определяются специальные категории персональных данных ([ч. 1](#)), специальные основания их обработки ([ч. 2](#)), специальные условия обработки отдельных специальных категорий персональных данных ([чч. 2.1 и 3](#)), а также условия незамедлительного прекращения обработки персональных данных ([ч. 4](#)).

[Частью 1](#) комментируемой статьи к специальным категориям персональных данных (далее - СКПД) отнесены сведения, касающиеся:

- расовой и национальной принадлежности;
- политических взглядов;
- религиозных убеждений;
- философских убеждений;
- состояния здоровья;
- интимной жизни.

Аналогичный объем "особых категорий персональных данных" свойственен и для Европейского союза. Так, Регламент ЕС о защите персональных данных в [ч. 1 ст. 9](#) содержит следующие нормативные установления: обработка персональных данных, раскрывающих расовое или этническое происхождение, политические взгляды, религиозные убеждения или философские воззрения, членство в профессиональном союзе, а также обработка генетических данных, биометрических данных для однозначной идентификации физического лица, данных касающихся здоровья, половой жизни или сексуальной ориентации физического лица, должна быть запрещена.

Исключения из этого правила применительно к обороту персональных данных в рамках уголовного процесса предусмотрены [ст. 10](#) Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами, данная норма допускает возможность оборота специальных категорий персональных данных в следующих случаях:

- (а) если это разрешено законодательством ЕС или государства-члена ЕС;
- (б) если это необходимо для защиты жизненных интересов субъекта данных или другого физического лица; или
- (с) если такая обработка относится к персональным данным, которые субъект данных явно сделал общедоступными.

Отметим широту формулировок приведенных оснований, а также то обстоятельство, что первое из них апеллирует не к конкретным обстоятельствам, а к законодательным установлениям широкого

перечня нормативных актов.

Согласно отечественному законодательству специальные категории персональных данных обеспечены особыми механизмами защиты от разглашения, сбора и оборота по сравнению с простыми разновидностями персональных данных.

Обработка СКПД не допускается за исключением случаев, предусмотренных [чч. 2 и 2.1](#) комментируемой статьи. Подобный законодательный подход обусловлен потенциальной опасностью использования названных сведений в качестве основания ограничения прав субъекта персональных данных, создания угрозы для их жизни и (или) здоровья. Помимо того, расовая и национальная принадлежность, политические взгляды, религиозные и философские убеждения, являясь критериями деления нации на социальные группы, в кризисной ситуации могут выступить основой для экстремистских и сепаратистских проявлений, которые представляют для многонациональной и многоконфессиональной Российской Федерации существенную опасность.

Комментируемый закон не обязывает операторов СКПД оценивать предназначение сбора и обработки сведений, в то время как европейский законодатель в [ч. 3 ст. 11](#) Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами акцентирует внимание на запрете формирования профиля, которое ведет к дискриминации в отношении физических лиц на основе специальных категорий персональных данных. Иными словами, если обрабатываемые на законной основе СКПД используются или могут быть использованы для дискриминации субъекта персональных данных, их оборот должен быть прекращен.

Напомним, что дискриминация является самостоятельным составом административного правонарушения ([ст. 5.62](#) КоАП) и преступления ([ст. 136](#) УК), а также мотивом нескольких уголовно наказуемых деяний (например, [п. "л" ч. 2 ст. 105](#) УК - убийство по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы).

Расовая принадлежность в отечественной исторической ретроспективе достаточно редко становилась причиной раскола общества или основой для дискриминации той или иной части общества. С.И. Ожегов дает следующее толкование понятию "раса" - исторически сложившаяся группа человечества, объединенная общностью наследственных физических признаков (цветом кожи, глаз, волос, формой черепа и др.), обусловленных общностью происхождения и первоначального расселения. Традиционно выделяются европеоидная, монголоидная и негроидная расы.

Сам термин "раса", возникнув в среде ученых-антропологов, с конца XX века подвергается научной критике со стороны самих антропологов, в том числе, из опасения способствовать распространению расизма, - системы взглядов, связывающих фенотипические и генотипические признаки человека с его биологическим, психологическими и интеллектуальными возможностями.

Показательным в этом контексте является [п. 37 преамбулы](#) Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами, согласно которому персональные данные, которые по своей природе являются особенно конфиденциальными в контексте основных прав и свобод, нуждаются в особой защите, так как особенности их обработки могут привести к существенному риску для основных прав и свобод. Указанные персональные данные должны включать в себя персональные данные, раскрывающие расовое и этническое происхождение. При этом делается специальная оговорка - использование термина "расовое происхождение" в настоящей Директиве не означает, что Европейский Союз одобряет теории, которые пытаются установить существование отдельных человеческих рас.

Географическое положение и история Российской Федерации, а также особенности экспансивной политики ее правителей на протяжении сотен лет обусловили культурную ассимиляцию и генетическое смешение представителей европеоидной и монголоидной рас, низкую внутрисоциальную напряженность по мотивам расовой принадлежности на территории страны.

Упоминание расовой принадлежности в тексте комментируемой статьи в большей степени является данью уважения международному праву. В Декларации ООН о расе и расовых предрассудках от 27 ноября 1978 г. закреплены нормы, которые в полной мере должны быть распространены и на национальные предрассудки:

все люди принадлежат к одному и тому же виду и имеют общее происхождение. Они рождаются равными в достоинстве и в правах, и все они составляют неотъемлемую часть человечества ([ч. 1 ст. 1](#));

многообразие форм жизни и право на различие ни при каких обстоятельствах не могут служить предлогом для расовых предрассудков; ни юридически, ни фактически они не могут служить оправданием какой бы то ни было дискриминационной практики ([ч. 2 ст. 1](#));

все народы мира обладают равными способностями, позволяющими им достигнуть самого высокого уровня интеллектуального, технического, социального, экономического, культурного и политического развития ([ч. 4 ст. 1](#));

всякая теория, приписывающая превосходство или неполноценность отдельным расовым или этническим группам, которая давала бы право одним людям господствовать над другими или отвергать других, якобы низших по отношению к ним, или основывающая суждения об оценке на расовых различиях, научно несостоятельна и противоречит моральным и этическим принципам человечества (ч. 1 ст. 2);

любое препятствие, затрудняющее свободный расцвет личности и свободную коммуникацию между людьми, основанное на расовых или этнических воззрениях, противоречит принципу равенства в достоинстве и правах; оно является недопустимым (ч. 1 ст. 4);

в рамках своей компетенции и в соответствии со своими конституционными положениями государство принимает все надлежащие меры, включая законодательные, в особенности в области образования, культуры и информации, в целях предотвращения, запрещения и ликвидации расизма, расовой пропаганды, расовой сегрегации и апартеида, и содействует распространению знаний и результатов соответствующих исследований (ч. 2 ст. 6).

Конституционной основой противодействия расовой, а равно и национальной, религиозной и иной экстремистской дискриминации выступают следующие положения **Конституции**:

ч. 5 ст. 13, согласно которой запрещается создание и деятельность общественных объединений, цели или действия которых направлены на, в том числе, разжигание социальной, расовой, национальной и религиозной розни;

ч. 2 ст. 19, устанавливающая, 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.

В совокупности с **ч. 3 ст. 55** Основного закона, которой предусмотрена возможность ограничения федеральным законом прав и свобод человека и гражданина в целях защиты основ конституционного строя и безопасности государства, приведенные нормы предоставляют органам публичной власти возможность ограничивать оборот информации, касающейся расовой и национальной принадлежности человека, его религиозных и иных воззрений и предпочтений.

Следует отметить, что признание конфиденциальности информации о расовой и национальной принадлежности не является общепризнанной практикой даже в кругу развитых государств. Так, криминальная статистика США традиционно разделяет преступность белого, черного, латиноамериканского, индейского и азиатского населения страны (см., например: <https://ucr.fbi.gov>). Аналогичная стратификация общества используется в сфере образования, медицины и социальной защиты. Подобное положение вещей, хотя и дает специалистам дополнительные данные для анализа, однако свидетельствует о наличии межрасовой напряженности среди населения и может способствовать эскалации внутригосударственного межэтнического напряжения и возникновению массовых беспорядков.

Национальная принадлежность - это принадлежность человека к определенной этнической общности людей, отличающейся особенностями языка, культуры, психологии, традиций, обычаев, образа жизни. Важность защиты населения страны от национальной дискриминации признается в России одной из приоритетных задач обеспечения национальной безопасности. **Преамбула** к Конституции начинается словами: "Мы, многонациональный народ Российской Федерации, соединенные общей судьбой на своей земле". В Конституции содержатся специальные нормы, выступающие непосредственной правовой базой для комментируемой **статьи**:

согласно **ч. 1 ст. 26** каждый вправе определять и указывать свою национальную принадлежность, при этом никто не может быть принужден к определению и указанию своей национальной принадлежности;

согласно **ч. 2 ст. 29** не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду, а равно пропаганда социального, расового, национального, религиозного или языкового превосходства.

Первая из приведенных конституционных норм обуславливает отнесение рассматриваемой категории персональных данных к конфиденциальной информации со специальным статусом, а вторая - особый порядок обработки таких данных.

Российское государство на протяжении всей своей истории придавало большое значение "национальному вопросу". В Российской империи, например, с 1791 по 1917 годы существовала черта оседлости для еврейского населения, применялись ограничения в политических и трудовых правах представителей не титульной нации. Советское правительство проводило крайне радикальные эксперименты с целью снижения межнациональной напряженности, в рамках которых поражаются в

правах и принудительно переселялись целые народы. В послевоенном СССР ущемление прав национальных меньшинств было не столь ярко выраженным, однако государственный учет национальной принадлежности оставался обязательным, в паспорте гражданина СССР существовала графа "Национальность". В паспорте гражданина РФ указание национальности не предусмотрено, а следовательно, запрещено ([Положение](#) о паспорте гражданина РФ, утв. [постановлением](#) Правительства от 8 июля 1997 г. N 828).

Политические взгляды как разновидность персональных данных представляют собой результат субъективного восприятия человеком политики, как социального явления. В широком смысле политика представляет собой сферу деятельности, связанную с отношениями между социальными группами, сутью которой является определение форм, задач и содержания внешней и внутренней деятельности государства. Внутренняя политика охватывает основные направления деятельности государства, партий (экономическая, социальная, культурная, техническая политика), внешняя - сферу отношений между государствами.

В наиболее обобщенном виде политические взгляды человека включают в себя систему убеждений и взглядов на политическое устройство страны, деятельность политических партий и лидеров, экономику, устройство гражданского общества, право и правосудие.

Преследование гражданина РФ в связи с его политическими убеждениями является основанием для предоставления ему статуса вынужденного переселенца в соответствии с [Законом](#) РФ от 19 февраля 1993 г. N 4530-1 "О вынужденных переселенцах", а преследование иностранного гражданина или лица без гражданства - статуса беженца в соответствии с [Федеральным законом](#) от 19 февраля 1993 г. N 4528-1 "О беженцах".

Нормы о недопустимости дискриминации кого-либо на основании политических взглядов содержатся в [ФЗ](#) "Об информации, информационных технологиях и о защите информации", [Закоме](#) РФ от 19 апреля 1991 г. N 1032-1 "О занятости населения в Российской Федерации", [Федеральном законе](#) от 12 августа 1995 г. N 144-ФЗ "Об оперативно-розыскной деятельности" и иных нормативных актах.

Не могут быть признаны СКПД политические убеждения, которые в соответствии [Федеральным законом](#) от 25 июля 2002 г. N 114-ФЗ "О противодействии экстремистской деятельности" признаны экстремистскими.

Религиозные убеждения представляют собой индивидуальную систему верований и обусловлены отношением человека к религии. Атеизм в этом контексте может быть отнесен как к религиозным, так и к философским убеждениям.

Согласно [ч. 1 ст. 14](#) Конституции Россия является светским государством, и никакая религия не может устанавливаться в качестве государственной или обязательной. В [ст. 28](#) Конституции каждому 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. В соответствии с [п. 5 ст. 3](#) Федерального закона от 26 сентября 1997 г. N 125-ФЗ "О свободе совести и о религиозных объединениях" 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.

Законодательные ограничения свободы совести и вероисповедания, свободы слова и права на распространение информации обеспечивают противодействие возникновению деструктивных сект, нарушающих права человека, а также воспрепятствуют миссионерской деятельности, если она несовместима с уважением к свободе мысли, совести и религии и к иным конституционным правам и свободам.

Злоупотребление в сфере распространения религиозной информации признается наказуемым. Так, [ст. 5.26](#) КоАП "Нарушение законодательства о свободе совести, свободе вероисповедания и о религиозных объединениях" охватывает широкий перечень деликтов от воспрепятствования деятельности религиозной организации до незаконной миссионерской деятельности, а [ч. 1 ст. 148](#) УК предусматривает ответственность за публичные действия, выражающие явное неуважение к обществу и совершенные в целях оскорбления религиозных чувств верующих.

Лексема "философские убеждения", которая использована для обозначения СКПД, не встречается в иных отечественных нормативных актах, относительно ее трактовки не сформировано судебной или административной практики. Чрезмерно широкой трактовкой было бы отнесение к философским убеждениям любых суждений о мире, человеке и человеческой жизни. Наиболее близкими по юридическому значению к рассматриваемой формулировке являются [чч. 1 и 2 ст. 13](#) Конституции, которыми декларируется тезис об идеологическом плюрализме и запрещается установление государственной или обязательной идеологии, а также [ч. 3 ст. 29](#) Конституции, согласно

которой никто не может быть принужден к выражению своих мнений и убеждений или отказу от них.

Философские убеждения представляют собой субъективные взгляды человека на правила социального взаимодействия, которые прямо не могут быть отнесены к религиозным убеждениям или политическим взглядам, хотя и близки к ним по своему генезису. Примером философских убеждений могут быть идеи пацифизма, вегетарианства, плюрализма, патриотизма, изоляционизма или мультикультурализма, гомофобии или одобрения нетрадиционных сексуальных отношений. Возникновение новых социальных идеологий обусловлено развитием общества, гуманитарных наук в целом и права в частности, в связи с чем приведение даже более-менее полного перечня таких идеологий невозможно.

Законодательством предусмотрены ограничения свободы публичного высказывания мнений и убеждений, в первую очередь, экстремистского, деструктивного и непристойного характера. Примером могут выступать нормы [ст. 6.21](#) КоАП, предусматривающие административную ответственность за пропаганду нетрадиционных сексуальных отношений среди несовершеннолетних. Помимо того, реализация связанных с философскими убеждениями прав граждан может быть сопряжена с определенными процедурными формальностями.

Пример: в [постановлении](#) Конституционного Суда РФ от 23 ноября 1999 г. N 16-П "По делу о проверке конституционности абзацев третьего и четвертого пункта 3 статьи 27 Федерального закона от 26 сентября 1997 года "О свободе совести и о религиозных объединениях" в связи с жалобами Религиозного общества Свидетелей Иеговы в городе Ярославле и религиозного объединения "Христианская церковь Прославления" рассматривалась жалоба на решение Кировского районного суда города Ярославля от 18 мая 1999 года.

Члену указанного общества было отказано в удовлетворении жалобы на действия призывной комиссии, которая не предоставила ему возможность замены военной службы альтернативной гражданской службой. Суд пришел к выводу, что члены религиозной организации, не имеющей документа, подтверждающего ее существование на соответствующей территории, не пользуются правом, согласно которому гражданин Российской Федерации в случае, если его убеждениям или вероисповеданию противоречит несение военной службы, имеет право на замену ее альтернативной гражданской службой.

Следующей разновидностью СКПД является информация о состоянии здоровья. Согласно [ст. 2](#) Федерального закона от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации" здоровьем признается состояние физического, психического и социального благополучия человека, при котором отсутствуют заболевания, а также расстройства функций органов и систем организма.

Информация о состоянии здоровья охватывается не только правовым институтом персональных данных, но и выступает содержанием трех видов информации со статусом ограниченного доступа: служебной (следственной) и профессиональной (врачебной) тайны, а также информации о частной жизни лица (личная и семейная тайны).

Рассматриваемая информация при передаче пациентом ее в медицинское учреждение охраняется в режиме врачебной тайны. При этом сведения о медицинских обследованиях, вмешательствах и лечении персональными данными не являются (см. [постановление](#) Конституционного Суда РФ от 13 января 2020 г. N 1-П).

Обработка информации о состоянии здоровья является наиболее четко урегулированным процессом по сравнению с нормативной регламентацией обработки иных видов персональных данных.

Следует отметить единство взглядов отечественного и зарубежного законодателя на вопрос толкования правовой сущности персональных данных, касающихся состояния здоровья. Согласно [п. 24 преамбулы](#) Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами связанные со здоровьем персональные данные должны включать в себя все данные, которые относятся к состоянию здоровья субъекта данных и раскрывают информацию о прошлом, текущем и будущем физическом или психологическом состоянии здоровья субъекта данных. К таким данным относятся:

- информация о физическом лице, собранная в ходе регистрации или предоставления медицинских услуг;

- номер, символ или знак, присвоенные физическому лицу для однозначной идентификации указанного лица в медицинских целях;

- информация, полученная в результате исследования или обследования части тела или телесного материала, включая генетические данные и биологические образцы;

- любая иная медицинская информация, например, о заболевании, инвалидности, риске заболевания, медицинском анамнезе, клиническом лечении или о физиологическом или медико-биологическом состоянии субъекта данных, независимо от источника данных, например, они

могут быть получены от врача или другого медицинского работника, больницы, медицинского оборудования или в результате диагностики в лабораторных условиях.

Информация об интимной жизни человека является разновидностью сведений о частной жизни лица, чья неприкосновенность гарантирована [ст. 23](#) Конституции. Эти персональные данные могут охраняться в режиме личной или семейной тайны. Искажение или неправомерный оборот информации об интимной жизни лица могут посягать на его честь и достоинство. Само слово "интимный" толкуется как касающийся личной жизни человека, его отношений с близкими людьми; касающийся области чувств, сокровенный, глубоко личный; находящийся в тесной дружественной связи, отношениях; лишенный официальности.

В связи с размытостью формулировки и явно индивидуально-чувственным наполнением содержания категории "информация об интимной жизни человека" привести исчерпывающий перечень видов данной информации не представляется возможным, однако к таковым однозначно следует отнести информацию о сексуальных предпочтениях, сексуальных отношениях и половых партнерах субъекта персональных данных, а также о действиях, непосредственно связанных или предшествующих сексуальным отношениям: сведения о факте обращения в службы знакомства, сведения о встречах с потенциальным половым партнером, а равно информация, передаваемая оператору персональных данных (посреднику) или потенциальному половому партнеру, с целью удовлетворения сексуальных потребностей.

Нарушение запрета на разглашение информации об интимной жизни является наказуемым как для оператора, так и для физического лица (в том числе полового партнера), которому она была доверена.

Пример: [определением](#) Первого кассационного суда общей юрисдикции от 27 января 2020 г. по делу N 88-1680/2020 была оставлена без удовлетворения кассационная жалоба К. по факту увольнения его со службы из Федеральной службы войск национальной гвардии РФ. в связи с совершением проступка, порочащего честь сотрудника органов внутренних дел. Основанием к увольнению послужило заключение по результатам служебной проверки, проведенной по заявлению В., с которой К. проживал совместно.

В ходе проверки установлено, что неизвестным лицом был осуществлен неправомерный доступ к электронной почте В., в результате чего в социальной сети "ВКонтакте" были опубликованы ее фотографии интимного характера. По сведениям, полученным в ходе проведения оперативно-разыскных мероприятий, доступ к персональной странице В. осуществлялся с абонентского номера, оформленного на К.

В заключении по результатам служебной проверки сделан вывод о совершении К. проступка, порочащего честь сотрудника войск национальной гвардии, выразившегося в неправомерном доступе к персональной странице в социальной сети и опубликовании фотографий интимного характера гражданки В., что повлекло за собой нарушение неприкосновенности частной жизни.

Сведение интимной жизни человека исключительно к удовлетворению сексуальных потребностей является очевидной ошибкой, однако такие личные проявления, как дружба, любовь, личная привязанность, романтические отношения и т.д. не могут иметь четкого юридического толкования, что не исключает, вместе с тем, возможность отнесения их к интимной сфере жизни человека уполномоченным должностным лицом или судом при рассмотрении конкретного юридического дела.

2. [Частью 2](#) комментируемой статьи нормативно закреплены исключения из общего запрета на запрашивание, получение и обработку СКПД. Аналогичные исключения содержатся в [ч. 2 ст. 9](#) Регламента ЕС о защите персональных данных и [ст. 10](#) Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами. Согласно данным нормам общий запрет на обработку особых (специальных) категорий персональных данных не применяется в случае, если:

(а) субъект данных дал прямое согласие на обработку указанных персональных данных для одной или нескольких установленных целей, кроме случаев, когда законодательство Союза или государства-члена ЕС предусматривает, что запрет на обработку особых категорий персональных данных не может быть отменен субъектом данных;

(б) обработка необходима в целях исполнения обязательств и особых прав контролера или субъекта данных в сфере трудового законодательства, права социального обеспечения и социальной защиты постольку, поскольку это допускается законодательством Союза или государства-члена ЕС или коллективным договором согласно законодательству государства-члена ЕС, предусматривающему соответствующие средства защиты основных прав и интересов субъекта данных;

(с) обработка необходима для защиты жизненных интересов субъекта данных или другого физического лица, если субъект данных физически или юридически неспособен дать свое согласие;

(d) обработка осуществляется фондом, объединением или некоммерческой организацией в рамках их законной деятельности с соответствующими гарантиями в политических, философских, религиозных или профсоюзных целях и при условии, что обработка относится исключительно к членам, бывшим членам организации или лицам, которые осуществляют постоянный контакт с нею в связи с ее целями, и что персональные данные не раскрываются третьим лицам без согласия на это субъекта персональных данных;

(e) обработка относится к персональным данным, которые субъект данных явно сделал общедоступными;

(f) обработка необходима для предъявления, исполнения или защиты судебных исков или в случаях, когда суды действуют в пределах своей судебской дееспособности;

(g) обработка необходима по причинам особого общественного интереса на основании законодательства Союза или государства-члена ЕС, которое должно быть пропорционально преследуемой цели, должно соответствовать сущности права на защиту данных и предусматривать приемлемые и конкретные меры для защиты основных прав и интересов субъекта данных;

(h) обработка необходима в целях превентивной или профессиональной медицины, для оценки трудоспособности работника, для диагностики медицинского состояния, предоставления медицинской или социальной помощи или лечения или для управления системами и услугами здравоохранения и социального обеспечения на основании законодательства Союза или государства-члена ЕС или на основании договора с работником здравоохранения и в соответствии с условиями и гарантиями, указанными в [Регламенте](#) и [Директиве](#).

(i) обработка необходима по причинам общественного интереса в области народного здравоохранения, например, защиты от серьезных трансграничных угроз здоровью или для обеспечения высоких стандартов качества и надежности медицинского обслуживания и лекарственных средств или медицинской техники, на основании законодательства Союза или государства-члена ЕС, которое предусматривает приемлемые и конкретные меры для защиты прав и свобод субъекта данных, в частности, профессиональной тайны;

(j) обработка необходима для целей архивизации информации в интересах государства, для научных, исторических или статистических целей, основанных на законодательстве Союза или государства-члена ЕС, которое должно быть пропорционально преследуемой цели, должно соответствовать сущности права на защиту данных и предусматривать приемлемые и конкретные меры для защиты основных прав и интересов субъекта данных.

Отечественное законодательство (в части комментируемой статьи) к обстоятельствам, позволяющим осуществлять сбор и иные формы обработки специальных категорий персональных данных, относит следующие:

1) Субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных ([п. 1 ч. 2](#) комментируемой статьи). Порядок получения такого согласия раскрыт в [комментарии](#) к ст. 9.

2) Обработка персональных данных разрешена субъектом персональных данных для распространения, в том числе имеет статус общедоступной информации. Правовое регулирование оборота общедоступных источников персональных данных рассмотрено в [комментарии](#) к ст. 8, а особые запреты и условия обработки персональных данных, разрешенных субъектом персональных данных для распространения, предусмотрены [ст. 10.1](#) настоящего федерального закона. Необходимо помнить, что по требованию субъекта персональных данных эти сведения должны быть исключены из общедоступного источника персональных данных.

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

В обобщенном виде реадмиссия - согласие государства на прием обратно на свою территорию своих граждан (а также, в некоторых случаях, иностранцев, прежде находившихся или проживавших в этом государстве), которые подлежат депортации из другого государства. В [Соглашении](#) между Правительством РФ и Правительством Турецкой Республики о реадмиссии от 18 января 2011 г. она определена, как передача компетентными органами запрашивающего государства и прием компетентными органами запрашиваемого государства в соответствии с условиями и процедурой, предусмотренной Соглашением, лиц, въехавших или находящихся на территории запрашивающего государства в нарушение действующего в нем законодательства по вопросам въезда, выезда и пребывания иностранных граждан и лиц без гражданства.

Обработка персональных данных при реадмиссии требуется для идентификации передаваемого лица и оформления соответствующих миграционных документов при перемещении его через границу, при этом из числа СКПД чаще других обрабатываются сведения о национальной принадлежности, религиозных убеждениях и состоянии здоровья.

4) Обработка персональных данных осуществляется в соответствии с [Федеральным законом](#) от 25 января 2002 года N 8-ФЗ "О Всероссийской переписи населения". В соответствии с [ч. 1 ст. 6](#) данного закона в рамках переписи населения могут быть обработаны такие СКПД, как: национальная принадлежность; отношения с членами домохозяйства (в том числе, с так называемыми сожителями); миграционные действия (в том числе, связанная с политическими или религиозными убеждениями причина въезда в РФ). Сообщение сведений в рамках переписи населения является добровольным, принуждение опрашиваемых предоставить о себе указанные выше сведения не допускается.

Согласно данным переписи населения России 2010 года из 142,8 млн человек свою национальность добровольно указали 137,2 млн респондентов, наиболее многочисленными национальностями в России являются: русские (111 млн человек), татары (5,31 млн человек), украинцы (1,92 млн человек), башкиры (1,58 млн человек), чуваша (1,43 млн человек), чеченцы (1,43 млн человек), армяне (1,18 млн человек).

5) Обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством и пенсионным законодательством. При этом субъект либо сам заинтересован в передаче СКПД, либо передача сведений осуществляется его законными представителями в его интересах. Обработка данной категории персональных данных осуществляется при наличии письменного согласия субъекта.

В соответствии с [п. 5 ст. 6.4](#) Федерального закона от 17 июля 1999 г. N 178-ФЗ "О государственной социальной помощи" персональные данные, содержащиеся в Федеральном регистре лиц, имеющих право на получение государственной социальной помощи, предоставляются органам исполнительной власти субъектов РФ безвозмездно, при этом последние обязаны соблюдать конфиденциальность полученных персональных данных и обеспечивать их безопасность при обработке. Учитывая то обстоятельство, что согласно [ст. 6.1](#) указанного закона к категориям граждан, подлежащим учету в Регистре, отнесены инвалиды и дети-инвалиды, данные о них должны быть отнесены к СКПД.

ТК определяет общие правила оборота СКПД в рамках трудовых правоотношений. Согласно [п. 6 ст. 81](#) ТК разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника, является грубым нарушением работником трудовых обязанностей и является основанием для расторжения трудового договора.

Защите персональных данных работника всецело посвящена гл. 14 ТК. Согласно [ст. 86](#) ТК работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся в соответствии с законодательством РФ к СКПД, в том числе о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных ТК и иными федеральными законами. Помимо того, в соответствии со [ст. 88](#) ТК при передаче персональных данных работника работодатель не вправе запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

Трудовые правоотношения отчасти охватываются и страховым законодательством, в связи с чем следует обратить внимание и на нормы [ст. 9](#) Федерального закона от 28 декабря 2013 г. N 400-ФЗ "О страховых пенсиях". Страховая пенсия по инвалидности устанавливается на основании сведений об инвалидности, содержащихся в федеральном реестре инвалидов, или документов, поступивших от федеральных учреждений медико-социальной экспертизы, независимо от причины инвалидности, продолжительности страхового стажа застрахованного лица, продолжения инвалидом трудовой и (или) иной деятельности, а также от того, наступила ли инвалидность в период работы, до поступления на работу или после прекращения работы.

Согласно [ст. 5.1](#) Федерального закона от 24 ноября 1995 г. N 181-ФЗ "О социальной защите инвалидов в Российской Федерации" в федеральный реестр инвалидов включаются в том числе:

сведения об инвалидности (группа, причина, ограничение жизнедеятельности, нарушенная функция организма, степень утраты профессиональной трудоспособности инвалида, дата установления инвалидности, срок, на который установлена инвалидность, потребности в мерах социальной защиты);

сведения об индивидуальных программах реабилитации или абилитации инвалидов и о программах реабилитации инвалидов, инвалидность которых наступила вследствие несчастных случаев на производстве и профессиональных заболеваний, включая сведения о рекомендованных в них реабилитационных мероприятиях, технических средствах реабилитации инвалидов, об услугах и о результатах выполнения этих программ;

сведения о предоставленных путевках на санаторно-курортное лечение в рамках оказания государственной социальной помощи в виде набора социальных услуг;

иные сведения, [перечень](#) которых определен [приказом](#) Минтруда от 12 октября 2016 г. N 569н

"Об утверждении перечня иных сведений о лице, признанном инвалидом, подлежащих включению в федеральный реестр инвалидов".

Среди прочего данным нормативным правовым актом предусмотрен оборот следующих сведений и документов, содержащих СКПД:

заключение о видах и степени выраженности ограничений категорий жизнедеятельности;

заключение о видах и степени выраженности стойких нарушений функций организма человека, обусловленных заболеваниями, последствиями травм или дефектами;

сведения о форме устройства ребенка-инвалида, оставшегося без попечения родителей, на воспитание в семью;

сведения об оказании высокотехнологичной медицинской помощи инвалиду (ребенку-инвалиду);

сведения о проведении операции кохлеарной имплантации;

сведения о лекарственном обеспечении лиц, больных гемофилией, муковисцидозом, гипопитарным нанизмом, болезнью Гоше, злокачественными новообразованиями лимфоидной, кроветворной и родственных им тканей, рассеянным склерозом, лиц после трансплантации органов и (или) тканей;

сведения об оказании санаторно-курортного лечения в санаторно-курортных организациях, находящихся в ведении Минздрава (за исключением санаторно-курортного лечения, осуществляемого в рамках предоставления набора социальных услуг);

сведения об оказании санаторно-курортного лечения в санаторно-курортных организациях, находящихся в ведении иных федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ (за исключением санаторно-курортного лечения, осуществляемого в рамках предоставления набора социальных услуг);

сведения об оказании паллиативной медицинской помощи;

сведения об обеспечении лекарственными препаратами и медицинскими изделиями, отпускаемыми по рецептам врачей при амбулаторном лечении бесплатно и со скидкой 50%.

Пенсионное законодательство также регламентирует порядок оборота отдельных разновидностей СКПД. Согласно [абз. 3 ч. 3 ст. 24](#) Федерального закона от 15 декабря 2001 г. N 166-ФЗ "О государственном пенсионном обеспечении в Российской Федерации" орган, осуществляющий пенсионное обеспечение, вправе проверять обоснованность выдачи и достоверность, в том числе, справки, подтверждающей факт установления инвалидности.

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.

По общему правилу гражданин самостоятельно принимает решение о разглашении сведений о состоянии своего здоровья, однако независимо от его желания они могут быть переданы в порядке и на основаниях, указанных в [ст. 13](#) Федерального закона от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в РФ", например:

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 (как правило, в условиях режимов чрезвычайного положения, чрезвычайной ситуации или повышенной готовности);

по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора;

в случае оказания медицинской помощи несовершеннолетнему;

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 проведения военно-врачебной экспертизы;

в целях расследования несчастного случая на производстве и профессионального заболевания, а также несчастного случая с обучающимся;

при обмене информацией медицинскими организациями;

в целях осуществления учета и контроля в системе обязательного социального страхования;

в целях осуществления контроля качества и безопасности медицинской деятельности.

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.

Базовые юридические термины, относящиеся к сфере медицинской деятельности, раскрываются в ст. 2 Федерального закона от 21 ноября 2011 г. N 323-ФЗ: здоровье, охрана здоровья граждан, медицинская помощь, медицинская услуга, медицинское вмешательство, профилактика, диагностика, лечение, медицинская организация, медицинский работник, лечащий врач, заболевание, качество медицинской помощи, телемедицинские технологии и др. Сама же медицинская деятельность согласно п. 10 названной статьи представляет собой профессиональную деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональную деятельность, связанную с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях.

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.

Согласно ст. 5 Федерального закона от 19 мая 1995 г. N 82-ФЗ "Об общественных объединениях" под общественным объединением понимается добровольное, самоуправляемое, некоммерческое формирование, созданное по инициативе граждан, объединившихся на основе общности интересов для реализации общих целей, указанных в уставе общественного объединения. Именно общие интересы, выступая основанием для объединения, обуславливают необходимость оборота СКПД.

Общественные объединения могут образовываться на основании национальной принадлежности (землячества, диаспоры), философских убеждений (казачьи общества), состояния здоровья (общественные организации инвалидов), интимных интересов и т.д. Для приема и инициации нового участника общественной организации необходимо оценить соответствие его взглядов и убеждений интересам сообщества, что предусматривает передачу претендентом своих персональных данных, в том числе перечисленных в ч. 1 комментируемой статьи.

Например, согласно п. 3 ч. 1 ст. 2 Федерального закона от 5 декабря 2005 г. N 154-ФЗ "О государственной службе российского казачества" казачье общество является формой самоорганизации граждан РФ, объединившихся на основе общности интересов в целях возрождения российского казачества, защиты его прав, сохранения традиционного образа жизни, хозяйствования и культуры российского казачества в соответствии с федеральным законодательством (некоммерческая организация).

В качестве примера приведем принятое в соответствии с указанным законом постановление мэрии г. Магадана от 2 февраля 2018 г. N 213, которое утверждает Устав Хуторского казачьего общества "Сокол", содержащий, среди прочего, следующие положения:

членами Казачьего общества могут быть граждане Российской Федерации, достигшие возраста 18 лет, относящие себя к казакам, разделяющие идеи казачества, признающие цели Казачьего общества и настоящий Устав, заинтересованные в осуществлении целей и задач Казачьего общества;

члены Казачьего общества обязаны: беречь честь и достоинство казака, укреплять единство российского казачества, хранить и развивать исторические, культурные и духовные обычаи и традиции российского казачества; активно участвовать в патриотическом воспитании молодых казаков, подготовке их к несению военной или иной службы; не совершать действий (бездействий), которые существенно затрудняют или делают невозможным достижение целей, ради которых создано Казачье общество;

член Казачьего общества может быть исключен из состава Казачьего общества в следующих случаях: если деятельность члена Казачьего общества противоречит целям и задачам Казачьего общества и (или) требованиям настоящего Устава; за неэтичное поведение, порочащее честь и достоинство казака; вступление в силу обвинительного приговора суда.

Общность политических взглядов является основанием для создания политических партий, среди основополагающих целей которых согласно ч. 4 ст. 3 Федерального закона от 11 июля 2001 г. N 95-ФЗ "О политических партиях" выделяются политическое образование и воспитание граждан, а также выражение мнений граждан по любым вопросам общественной жизни, доведение этих мнений до сведения широкой общественности и органов государственной власти. Следует обратить внимание, что в чч. 7 и 8 ст. 23 указанного закона содержатся нормы, дополнительно защищающие члена политической партии от дискриминации по мотивам политических взглядов. В частности, запрещается

требовать от граждан РФ, чтобы они при представлении официальных сведений о себе указывали членство в политической партии или отсутствие такового.

Религиозные убеждения являются базой для создания и участия в деятельности религиозных объединений и организаций. Согласно [ч. 1 ст. 6](#) Федерального закона от 26 сентября 1997 г. N 125-ФЗ "О свободе совести и о религиозных объединениях" религиозным объединением в РФ признается добровольное объединение граждан РФ, иных лиц, постоянно и на законных основаниях проживающих на территории РФ, 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. Определение религиозной организации дано в [ч. 1 ст. 8](#) указанного закона, а в [ч. 5 ст. 3](#) закреплено право каждого не сообщать о своем отношении к религии.

Следует особо отметить, что сбор и оборот СКПД общественными объединениями и организациями, равно как и членство в них, могут иметь место лишь в случае добровольного волеизъявления человека, оформленного в форме письменного согласия. Полученные общественным объединением или организацией персональные данные не могут быть использованы иначе, как в законодательно определенных целях их деятельности, не могут быть переданы третьим лицам, кроме случаев, прямо предусмотренных законом.

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

Комментируемый пункт содержит три относительно самостоятельных основания обработки СКПД. Установление прав субъекта персональных данных или третьих лиц необходимо в случае неочевидности правового статуса участника правоотношений, когда наличие специальных прав или обязанностей является необходимым или обязательным. Так, установление родственных связей необходимо для вступления в наследство или установления отцовства, а наличие или отсутствие психического расстройства, слабоумия либо иного болезненного состояния психики - для установления дееспособности.

Такое основание для обработки СКПД, как осуществление прав субъекта персональных данных или третьих лиц, представляется чрезмерно широким, так как формально может быть использовано в качестве повода к необоснованному вторжению в частную жизнь человека.

В теории права синонимом осуществления права является юридическая категория "реализация права", включающая в качестве самостоятельных форм: соблюдение, исполнение, использование и применение права. Учитывая контекст, в котором законодатель использует слово "осуществление", необходимо трактовать его содержание в узком смысле. Полагаем, речь в данном случае идет об осуществлении, в первую очередь, процедурно-процессуальных прав, которые прямо оговорены в соответствующих законодательных актах.

Третья составляющая рассматриваемого основания обработки СКПД - осуществление правосудия. Правосудие выступает одновременно правовой ценностью и формой разрешения юридических споров, вытекающих как из публично-правовых, так и из частноправовых отношений. Правосудие реализуется исключительно судом в рамках конституционного, гражданского, арбитражного, административного и уголовного судопроизводства. Его цель - справедливое восстановление нарушенных прав, обеспечение реализации права или достижение законного интереса. Например, религиозные взгляды и политические убеждения подозреваемого (обвиняемого) в совершении преступления экстремистской направленности имеют существенное значение для дела, так как могут раскрывать мотив его совершения.

10) Обработка персональных данных осуществляется в соответствии с законодательством РФ об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством.

Данный пункт аналогичен по своей правовой природе предыдущему, разница заключается лишь в том, что персональные данные используются на досудебных стадиях публично-правового производства, в рамках предупреждения и пресечения административных правонарушений или преступлений, в целях устранения угроз обороне и безопасности государства.

Основополагающими нормативными регуляторами в данной сфере, помимо [УК](#), [УПК](#) и [КоАП](#), выступают:

[Уголовно-исполнительный кодекс](#) РФ от 8 января 1997 г. N 1-ФЗ;

[Федеральный закон](#) от 7 февраля 2011 г. N 3-ФЗ "О полиции";

[Федеральный закон](#) от 3 июля 2016 г. N 226-ФЗ "О войсках национальной гвардии Российской Федерации";

[Федеральный закон](#) от 12 августа 1995 г. N 144-ФЗ "Об оперативно-розыскной деятельности";

[Федеральный закон](#) от 31 мая 1996 г. N 61-ФЗ "Об обороне";

[Федеральный закон](#) от 25 июля 2002 г. N 114-ФЗ "О противодействии экстремистской деятельности";

[Федеральный закон](#) от 6 марта 2006 г. N 35-ФЗ "О противодействии терроризму";

[Федеральный закон](#) от 25 декабря 2008 г. N 273-ФЗ "О противодействии коррупции";

[Федеральный закон](#) от 2 октября 2007 г. N 229-ФЗ "Об исполнительном производстве";

[Федеральный закон](#) от 9 февраля 2007 г. N 16-ФЗ "О транспортной безопасности" и др.

11) Обработка полученных в установленных законодательством РФ случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора.

Согласно [ч. 1 ст. 129](#) Основного закона прокуратура представляет собой единую федеральную централизованную систему органов, осуществляющих надзор за соблюдением Конституции и исполнением законов, надзор за соблюдением прав и свобод человека и гражданина, уголовное преследование в соответствии со своими полномочиями, а также выполняющих иные функции.

Прокуратура относится к органам с особым конституционным статусом. Она не может быть отнесена ни к одной ветви власти, в связи с чем не упоминалась в [пп. 6 и 7 ч. 2](#) комментируемой статьи.

Вопросам организации прокурорского надзора всецело посвящен раздел III Федерального закона от 17 января 1992 г. N 2202-1 "О прокуратуре Российской Федерации". В частности, согласно [абз. 3 ч. 1 ст. 22](#) данного закона прокурор при реализации надзорных полномочий вправе: требовать от руководителей и других должностных лиц представления необходимых документов и материалов или их копий, статистических и иных сведений; проводить проверки по поступившим в органы прокуратуры материалам и обращениям; проводить ревизии деятельности подконтрольных или подведомственных им организаций.

Согласно [п. 1.3](#) Инструкции о порядке обработки в органах прокуратуры персональных данных, полученных в связи с осуществлением прокурорского надзора, утв. [приказом](#) Генпрокуратуры от 22 ноября 2013 г. N 506, при осуществлении установленных законодательством полномочий прокуроры вправе получать следующую информацию о субъекте персональных данных:

анкетные и биографические данные, включая адрес места жительства и проживания;

сведения о гражданстве, паспортные данные или данные иного документа, удостоверяющего личность и гражданство (включая серию, номер, дату выдачи, наименование органа, выдавшего документ);

сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки;

сведения о трудовой деятельности, опыте работы, занимаемой должности, трудовом стаже, повышении квалификации и переподготовке;

сведения о составе семьи и наличии иждивенцев, о месте работы или учебы членов семьи;

сведения о состоянии здоровья и наличии заболеваний, о нахождении на различных медицинских учетах;

сведения об отношении к воинской обязанности;

сведения о доходах, расходах, налоговых обязательствах и иных обязательствах имущественного характера;

сведения об идентификационном номере налогоплательщика;

сведения о социальных льготах и о социальном статусе;

сведения о судимости, о привлечении к уголовной, административной или иного вида ответственности;

сведения об имуществе (недвижимости, транспортных средствах и др.);

сведения о предпринимательской деятельности субъекта персональных данных и членов его семьи;

сведения о доходах, расходах, об имуществе и обязательствах имущественного характера и иные персональные данные лиц, на которых распространяются обязанности, предусмотренные [ст. 8](#) Федерального закона от 25 декабря 2008 г. N 273-ФЗ "О противодействии коррупции" и иными правовыми актами Российской Федерации (в том числе сведения о доходах, расходах, об имуществе и обязательствах имущественного характера и иные персональные данные их супругов и несовершеннолетних детей);

персональные данные лиц, на которых распространяются установленные законодательством о противодействии коррупции запреты, ограничения и обязанности;

персональные данные иных лиц в целях выявления правонарушений (в том числе нарушений законодательства о противодействии коррупции);

иные персональные данные, необходимые для целей осуществления прокурорского надзора.

12) Обработка персональных данных осуществляется в соответствии с законодательством об

обязательных видах страхования, со страховым законодательством. Страховым правоотношениям посвящены [гл. 48](#) ГК и [Закон](#) РФ от 27 ноября 1992 г. N 4015-1 "Об организации страхового дела в Российской Федерации".

По общему правилу страхование жизни, здоровья и имущества является добровольным, а следовательно, передача страховой компании персональных данных требует письменного согласия субъекта.

Ряд нормативных правовых актов предъявляет к гражданам и организациям требования об обязательном страховании, это:

[Федеральный закон](#) от 16 июля 1999 г. N 165-ФЗ "Об основах обязательного социального страхования";

[Федеральный закон](#) от 24 июля 1998 г. N 125-ФЗ "Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний";

[Федеральный закон](#) от 29 декабря 2006 г. N 255-ФЗ "Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством";

[Федеральный закон](#) от 29 ноября 2010 г. N 326-ФЗ "Об обязательном медицинском страховании в Российской Федерации";

[Федеральный закон](#) от 25 апреля 2002 г. N 40-ФЗ "Об обязательном страховании гражданской ответственности владельцев транспортных средств".

Обязательное страхование, реализуемое в контексте социальной защиты населения или нивелирования возникающих при эксплуатации источников повышенной опасности рисков, предусматривает необходимость обработки отдельных СКПД.

Например, согласно [ч. 4 ст. 15](#) Федерального закона от 24 июля 1998 г. N 125-ФЗ "Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний" назначение обеспечения по страхованию осуществляется страховщиком на основании заявления, к которому прилагаются следующие документы:

акт о несчастном случае на производстве или профессиональном заболевании;

судебное решение об установлении юридического факта несчастного случая на производстве (профессионального заболевания);

свидетельство о смерти застрахованного, иные свидетельства о государственной регистрации актов гражданского состояния;

выданное в установленном порядке заключение о связи смерти застрахованного с несчастным случаем на производстве или профессиональным заболеванием;

заключение учреждения медико-социальной экспертизы о степени утраты профессиональной трудоспособности застрахованным;

заключение центра профессиональной патологии о наличии профессионального заболевания;

программа реабилитации пострадавшего;

документ, подтверждающий, что один из родителей, супруг (супруга) либо другой член семьи умершего застрахованного, занятый уходом за детьми, внуками, братьями и сестрами застрахованного, не достигшими возраста 14 лет либо достигшими указанного возраста, но по заключению учреждения медико-социальной экспертизы или медицинской организации признанными нуждающимися по состоянию здоровья в постороннем уходе, не работает;

заключение учреждения медико-социальной экспертизы или медицинской организации о признании детей, внуков, братьев и сестер застрахованного, достигших возраста 14 лет, нуждающимися по состоянию здоровья в постороннем уходе;

решение суда, подтверждающее факт нахождения на иждивении.

13) Обработка персональных данных осуществляется в случаях, предусмотренных законодательством РФ, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан.

Нормативную базу оборота СКПД по рассматриваемому основанию образуют СК, [Федеральный закон](#) от 24 апреля 2008 г. N 48-ФЗ "Об опеке и попечительстве" и [Федеральный закон](#) от 16 апреля 2001 г. N 44-ФЗ "О государственном банке данных о детях, оставшихся без попечения родителей", а также принимаемые на их основе подзаконные нормативные регуляторы.

Положения [ст. 127](#) СК обуславливают право органов опеки (попечительства) и суда устанавливать обстоятельства, исключающие возможность усыновления ребенка. Таковыми обстоятельствами, среди прочего, являются:

признание судом лица недееспособным или ограниченно дееспособным;

лишение по суду лица родительских прав или ограничение судом лица в родительских правах;

отстранение от обязанностей опекуна (попечителя) за ненадлежащее выполнение возложенных на него законом обязанностей;

отмена усыновления судом ранее по вине лица;

состояние здоровья, не позволяющее усыновить ребенка ([постановлением](#) Правительства от 14 февраля 2013 г. N 117 утвержден [Перечень](#) заболеваний, в который входят: туберкулез, инфекционные заболевания до прекращения диспансерного наблюдения в связи со стойкой ремиссией, злокачественные новообразования, психические расстройства и расстройства поведения до прекращения диспансерного наблюдения, наркомания, токсикомания, алкоголизм, а также заболевания и травмы, приведшие к инвалидности I группы);

отсутствие дохода, обеспечивающего усыновляемому ребенку прожиточный минимум;

отсутствие постоянного места жительства;

наличие судимости (в т.ч. снятой или погашенной) или уголовного преследования за совершение отдельных категорий преступлений;

наличие зарегистрированного за рубежом однополного брака или гражданства (подданства) государства, в котором такой брак разрешен.

Кроме того, [ст. 123](#) СК 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.

Обработка персональных данных в целях, определяемых рассматриваемым пунктом, регламентируется Федеральным законом от 16 апреля 2001 г. N 44-ФЗ "О государственном банке данных о детях, оставшихся без попечения родителей", согласно [ч. 2 ст. 6](#) которого в анкету ребенка включается в том числе следующая информация:

состояние здоровья ребенка, оставшегося без попечения родителей, его физическое и умственное развитие;

особенности характера ребенка, оставшегося без попечения родителей (общительный, замкнутый и другие особенности);

этническое происхождение ребенка, оставшегося без попечения родителей;

причины отсутствия родительского попечения над ребенком;

фамилии, имена, отчества, даты рождения, гражданство, принадлежность к определенной религии и культуре (при возможности указания такой информации), состояние здоровья (при наличии документального подтверждения такой информации), место жительства и (или) место пребывания родителей либо единственного родителя ребенка, оставшегося без попечения родителей.

14) Обработка персональных данных осуществляется в соответствии с законодательством о гражданстве Российской Федерации.

Процедурная составляющая производства по делам о гражданстве предусматривает необходимость оборота отдельных анкетных данных, относимых к СКПД. Например, [ч. 1 ст. 16](#) Федерального закона от 31 мая 2002 г. N 62-ФЗ "О гражданстве Российской Федерации", определяя причины отклонения заявлений о выдаче уведомления о возможности приема в гражданство РФ, о приеме в гражданство РФ и о восстановлении в гражданстве РФ, предусматривает сбор и обработку ГУ МВД по вопросам миграции и его территориальными органами СКПД, связанных с политическими и философскими взглядами, а также религиозными убеждениями кандидата на получение гражданства (например, приверженность экстремистской идеологии), а также иных СКПД, указывающих на нежелательность приема в гражданство РФ по соображениям безопасности.

Самим претендентом на получение гражданства РФ в соответствии с [Положением](#) о порядке рассмотрения вопросов гражданства РФ, утв. [Указом](#) Президента от 14 ноября 2002 г. N 1325, должны быть сообщены сведения о семейном положении и близких родственниках, а также могут быть сообщены сведения о национальности и вероисповедании.

3. [Часть 2.1](#) комментируемой статьи введена в настоящий федеральный закон [Федеральным законом](#) от 24 апреля 2020 г. N 123-ФЗ "О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных", вступила в силу 1 июля 2020 г. и легализует формально неопределенный перечень исключений из правил обработки СКПД на территории г. Москвы.

Комментируемая норма предусматривает, что обработка персональных данных, касающихся состояния здоровья, полученных в результате обезличивания персональных данных, допускается в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных [Федеральным законом](#) от 24 апреля 2020 г. N 123-ФЗ.

При этом следует учитывать закрепленное в [ч. 4 ст. 1](#) Федерального закона от 24 апреля 2020 г. N 123-ФЗ правило, согласно которому положения нормативных правовых актов субъекта РФ,

устанавливающие условия экспериментального правового режима, не могут исключать, изменять или вступать в противоречие с положениями федеральных законов и иных нормативных правовых актов РФ, относящихся в соответствии с [Конституцией](#) к ведению РФ или совместному ведению РФ и субъектов РФ.

Иными словами, [ч. 2.1](#) комментируемой статьи предусматривает возможность обработки специальных категорий медицинских персональных данных, которая в целом должна соответствовать основаниям и требованиям, закрепленным в [ч. 2](#) комментируемой статьи. Подобная формулировка существенно девальвирует возможности развертывания на территории г. Москва так называемой регуляторной песочницы - зоны особого правового регулирования, обеспечивающего создание, развитие и апробацию инновационных технологий, внедрение которых не урегулировано федеральным законодательством или противоречит ему.

В пояснительной записке к проекту [Федерального закона](#) от 24 апреля 2020 г. N 123-ФЗ отмечалось, что он разработан во исполнение послания Президента Федеральному Собранию РФ от 15 января 2020 г. для обеспечения создания собственных стандартов и развития технологий, которые определяют будущее, в частности, технологий искусственного интеллекта.

Согласно [п. 1 ч. 1 ст. 2](#) ФЗ N 123 экспериментальным правовым режимом является проведение в течение предусмотренного данным законом срока (5 лет) эксперимента в отношении участников экспериментального правового режима специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте РФ - городе федерального значения Москве, а также последующего возможного использования результатов применения искусственного интеллекта.

На сегодняшний день при отсутствии постановлений Правительства г. Москвы, развивающих положения [Федерального закона](#) от 24 апреля 2020 г. N 123-ФЗ, трудно предположить возможные формы использования искусственного интеллекта при обработке обезличенных персональных данных, однако перспективные цели подобного использования возможно определить при изучении положений [Федерального закона](#) от 31 июля 2020 г. N 258-ФЗ "Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации", который вступает в силу 28 января 2021 года.

В соответствии с [ч. 1 ст. 3](#) указанного закона целями установления экспериментального правового режима являются:

- обеспечение повышения качества жизни населения;
- повышение эффективности государственного или муниципального управления;
- повышение эффективности деятельности хозяйствующих субъектов в ходе внедрения технологий искусственного интеллекта;
- формирование комплексной системы регулирования общественных отношений, возникающих в связи с развитием и использованием технологий искусственного интеллекта, по результатам установления экспериментального правового режима.

Следует исходить из норм, закрепленных в [ст. 4](#) Федерального закона от 24 апреля 2020 г. N 123-ФЗ:

Правительство г. Москвы по согласованию с Минцифры определяет порядок и условия обработки участниками экспериментального правового режима персональных данных, полученных в результате обезличивания, на основании соглашений с уполномоченным органом, а также требования к таким соглашениям ([ч. 1](#));

персональные данные, полученные в результате обезличивания и обрабатываемые на основании соглашения с уполномоченным органом, не могут быть переданы лицам, не являющимся участниками экспериментального правового режима, при этом в случае утраты статуса участника экспериментального правового режима или прекращения эксперимента в связи с истечением срока его проведения лицо, являвшееся участником экспериментального правового режима, утрачивает право на получение персональных данных, полученных в результате обезличивания, а хранящиеся у такого лица персональные данные, полученные в результате обезличивания, подлежат уничтожению;

при проведении эксперимента не допускается хранение персональных данных, полученных в результате обезличивания и обрабатываемых на основании соглашения с уполномоченным органом, за пределами г. Москвы.

[4. Частью 3](#) комментируемой статьи урегулирован оборот особой разновидности персональных данных - сведений о судимости. Установлено правило, согласно которому обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством РФ, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами. Согласно [ст. 86](#) УК 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 и [УПК](#). Судимость является обстоятельством, исключающим выполнение гражданами определенных трудовых или служебных функций (например, прохождение государственной службы в правоохранительных органах), а равно реализацию отдельных гражданских прав (членство в некоторых общественных организациях, внештатное сотрудничество с полицией и т.д.). Кроме того, совершение умышленного преступления лицом, имеющим не снятую и не погашенную судимость за ранее совершенное умышленное преступление, признается рецидивом и является обстоятельством, отягчающим тяжесть наказания.

В соответствии с [постановлением](#) Правительства РФ от 30 мая 2016 г. N 479 проставление апостиля на справках о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования, архивных документах и справках о реабилитации отнесено к полномочиям МВД России. Предоставление органам публичной власти сведений о судимости производится на основании [п. 39 ч. 1 ст. 12](#) Федерального закона от 7 февраля 2011 г. N 3-ФЗ "О полиции" на безвозмездной основе.

Граждане Российской Федерации, иностранные граждане, лица без гражданства либо их уполномоченные представители могут получить сведения о судимости в порядке, предусмотренном [Административным регламентом](#) МВД России по предоставлению государственной услуги по выдаче справок о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования, утв. [приказом](#) МВД России от 27 сентября 2019 г. N 660. Непосредственное предоставление государственной услуги осуществляется ФКУ "ГИАЦ МВД России" и информационными центрами территориальных органов МВД России по субъектам РФ на основании письменного заявления субъекта персональных данных.

5. Согласно [ч. 4](#) комментируемой статьи обработка СКПД, осуществлявшаяся в случаях, предусмотренных [чч. 2 и 3](#) настоящей статьи, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, и если иное не установлено федеральным законом. Основаниями для прекращения обработки данных могут быть:

- отзыв субъектом СКПД письменного согласия на обработку своих персональных данных;
- окончание Всероссийской переписи населения и подведение ее итогов;
- отмена режима чрезвычайного положения, чрезвычайной ситуации или повышенной готовности, введенных при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- прекращении членства субъекта СКПД в общественном объединении или организации (в том числе религиозной или политической);
- увольнение гражданина с государственной службы;
- достижение совершеннолетия лицом, состоящим на профилактическом учете в полиции, на учете в органах опеки и попечительства;
- отказ от получения государственной услуги;
- смерть субъекта СКПД и другие.

Статья 10.1. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения

1. Настоящая [статья](#) введена в комментируемый закон [Федеральным законом](#) от 30 декабря 2020 г. N 519-ФЗ "О внесении изменений в Федеральный закон "О персональных данных" и вступает в силу 1 марта 2021 года. Федеральный закон N 519-ФЗ внес принципиальные изменения в свободное распространение персональных данных.

Отменяется понятие "персональные данные, сделанные общедоступными субъектом персональных данных", которое использовалось в [п. 10 ч. 1 ст. 6](#) комментируемого закона. Вместо данного понятия принята новая дефиниция "персональные данные, разрешенные субъектом персональных данных для распространения" - это персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном комментируемым законом ([п. 1.1 ч. 1 ст. 3](#)).

Ранее общедоступность персональных данных означала, что все сведения, которые человек распространил о себе в открытых источниках в сети Интернет, могут без ограничений использоваться любыми лицами. Это означало, что информация, размещенная субъектом персональных данных, например в социальных сетях, с указанием фамилии, имени, отчества, даты рождения, места учебы и работы, с добавлением фотографий себя и родственников и т.п., могла быть перепечатана любыми ресурсами в сети Интернет. Некоторые ограничения были возможны только при закрытии своей страницы ее обладателем, однако если информация с нее становилась объектом гласности и начинала бесконтрольно распространяться по сети, то удалить ее законным способом было невозможно.

Аналогичная ситуация возникала при размещении персональных данных о своих сотрудниках на

сайтах организаций или самими субъектами персональных данных на сайтах профессиональных сообществ (например, педагогических или медицинских).

При этом отмена дефиниции "персональные данные, сделанные общедоступными субъектом персональных данных" не означает отмены понятия "общедоступные источники персональных данных". Представляется, что теперь формирование таких общедоступных источников будет возможно только при оформлении согласия в соответствии с комментируемой статьей.

2. **Часть 1** комментируемой статьи предусматривает, что необходимо оформление отдельного согласия на обработку персональных данных, разрешенных субъектом для распространения. При этом оператор должен обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных. Соответственно, всем операторам потребуется заключение новых соглашений с субъектами персональных данных. В соглашении должно быть четко указано - какие именно категории персональных данных субъект предоставляет для распространения.

Например, заполняя анкету регистрации в интернет-магазине, субъект персональных данных разрешит использовать только свое имя и возраст при комментировании качества товаров. А соглашение, подписанное им с социальной сетью "Одноклассники", будет предусматривать возможность размещения для распространения фамилии, имени, отчества, даты рождения и одной фотографии. При этом остальные сведения должны быть скрыты для всех, кроме друзей субъекта. Несмотря на то, что многие операторы уже работают по указанной схеме, потребуется получение специального согласия на распространение персональных данных неопределенному кругу лиц.

В соответствии с **ч. 9 ст. 9** комментируемого закона, также введенной **Федеральным законом** от 30 декабря 2020 г. N 519-ФЗ, требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, устанавливаются Роскомнадзором.

3. **Часть 2** комментируемой статьи предусматривает, что законность подтверждения распространения или иной обработки персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку. Таким образом, любое лицо, использующее персональные данные, раскрытые неопределенному кругу лиц самим субъектом персональных данных, должно получать отдельное согласие субъекта на это использование.

Положения **ч. 2** комментируемой статьи должны закрыть возможность безнаказанного распространения персонифицированной рекламы товаров и финансовых услуг. Также данные нормы призваны препятствовать перепечатыванию из одного издания в другое журналистами, блогерами и интернет-ресурсами сведений о каком-либо лице под предлогом, что данные сведения уже опубликованы другим ресурсом и являются общедоступными. Подобный подход существенно затруднит работу новостных агрегаторов и "мусорных" интернет-порталов и упростит отслеживание источника информации.

4. **Часть 3** комментируемой статьи предусматривает, что если персональные данные были раскрыты неопределенному кругу лиц в результате нарушения закона или случайно, дальнейшее их распространение или обработка возможны только в случае получения оператором у субъекта согласия. Часть 3 настоящей статьи является продолжением **ч. 2** и определяет, что для открытого опубликования (раскрытия неопределенному кругу лиц) в любом случае необходимо получение разрешения субъекта персональных данных.

Кроме того, запрещается дальнейшее раскрытие неопределенному кругу лиц информации, которая была размещена в открытом доступе без согласия субъекта персональных данных. В результате ответственность за перепечатку незаконно раскрытой информации возлагается не только на первое разгласившее информацию лицо, а на всех лиц, участвовавших в ее дальнейшем распространении. Представляется, что положения **чч. 2 и 3** распространяются также на блогеров и социальные сети в целом.

5. **Часть 4** комментируемой статьи установила, что согласие субъекта персональных данных на их распространение должно быть выражено явно - простого согласия субъекта на обработку его персональных данных в этом случае уже недостаточно. Оператор должен обратить внимание субъекта именно на то, что его персональные данные будут распространяться, и получить согласие конкретно на распространение для неопределенного круга лиц.

Представляется, что до подписания субъектом персональных данных согласия на распространение сведений все его аккаунты в социальных сетях и мессенджерах должны быть заблокированы для просмотра.

6. **Часть 5** комментируемой статьи предусматривает, что в согласии субъекта персональных данных на их распространение должны быть указаны запреты и условия на обработку персональных данных, предусмотренные **ч. 9** данной статьи. В случае их отсутствия указанные персональные данные не могут распространяться (предоставляться) для неограниченного круга лиц.

7. **Частью 6** комментируемой статьи определено, что согласие на обработку персональных данных, разрешенных для распространения, может быть подписано субъектом непосредственно, то есть в бумажной форме или в электронном виде на сайте оператора.

С 1 июля 2021 г. согласие можно будет предоставить, используя информационную систему уполномоченного органа по защите прав субъектов персональных данных.

8. **Часть 7** комментируемой статьи предусматривает, что указанная часть информационной системы должна быть создана Роскомнадзором. Кроме того, Роскомнадзор должен утвердить порядок взаимодействия субъекта персональных данных с оператором.

9. **Часть 8** настоящей статьи закрепила обязательность именно явного выражения согласия субъекта на распространение его персональных данных для неопределенного круга лиц. Установлено, что в данном случае молчание или бездействие лица, персональные данные которого желает распространить оператор, не является знаком согласия. Таким образом, страницы в социальных сетях лиц, которые не подписали указанное согласие, должны быть скрыты до получения оператором такого согласия.

10. **Часть 9** комментируемой статьи обязывает операторов предлагать субъекту персональных данных выбор на установление запретов или дополнительных условий при распространении персональных данных неопределенному кругу лиц. Например, человек согласен, чтобы были опубликованы его фамилия и имя, но выступает против публикации даты рождения, сведений об образовании и т. д.

Отсутствие возможности установить запрет или условия делает согласие недействительным в соответствии с **ч. 5** данной статьи.

11. **Часть 10** рассматриваемой статьи предусматривает, что оператор обязан в течение 3 рабочих дней опубликовать условия согласия, подписанного субъектом персональных данных. Из текста статьи не совсем понятно, где именно оператор должен опубликовать данные условия или запреты. Скорее всего, законодатель имел в виду, что, размещая персональные данные, разрешенные субъектом для распространения, оператор должен указать, что другие данные субъект запретил размещать для неопределенного круга лиц.

12. В **ч. 11** комментируемой статьи установлено, что на обработку и последующее распространение персональных данных не распространяются никакие запреты или условия, если эта деятельность осуществляется в государственных, общественных и иных публичных интересах. Указанные интересы должны быть закреплены в законодательстве Российской Федерации.

Например, размещение персональных данных государственных служащих на сайтах государственных органов предусмотрено федеральными законами и не требует дополнительного согласия. А вот дальнейшее их использование и распространение другими операторами будет являться незаконным без получения согласия у государственного служащего, чьи персональные данные будут распространяться.

13. В соответствии с **ч. 12** комментируемой статьи субъект персональных данных может запретить их распространение в любой момент. Для этого он должен направить оператору требование, в котором должны быть указаны:

фамилия, имя, отчество;
контактная информация (номер телефона, почтовый адрес или электронная почта);
перечень персональных данных, обработка которых подлежит прекращению.

Перечисленные персональные данные могут обрабатываться исключительно оператором, которому было направлено требование.

Распространение персональных данных должно быть прекращено оператором в момент получения им указанного требования.

14. **Часть 14** комментируемой статьи установила, что отзыв разрешения на распространение оператором персональных данных субъекта может осуществляться без ограничений. Таким образом, субъект может потребовать прекратить распространение своих персональных данных от любого лица, которому он ранее подписал согласие на данное распространение.

Кроме того, предусмотрена возможность обращения в суд в случае невыполнения оператором требований субъекта персональных данных. Оператор или любое другое лицо, осуществляющее распространение персональных данных субъекта, обязан в течение 3 дней после получения требования прекратить передачу (распространение, предоставление, доступ) его персональных данных.

15. **Часть 15** комментируемой статьи является продолжением **ч. 11** и исключает государственные органы и органы местного самоуправления из операторов, которые должны получать согласие субъектов на распространение их персональных данных. В результате, если распространение персональных данных осуществляется в соответствии с функциями, полномочиями или обязанностями органов власти, а также в государственных, общественных и иных публичных интересах, то оно не

требует получения согласия субъекта персональных данных на данное распространение.

16. Положения настоящей **статьи** предусматривают необходимость принятия подзаконных актов Роскомнадзора, в которых будут установлены:

форма согласия субъекта на распространение его персональных данных для неопределенного круга лиц, включающая запреты и условия на обработку персональных данных, установленные субъектом;

порядок взаимодействия оператора и субъекта персональных данных при подписании согласия на распространение персональных данных, в том числе особенности подписания данного согласия в электронном виде;

порядок функционирования части информационной системы уполномоченного органа по защите прав субъектов персональных данных, которая будет обеспечивать взаимодействие между операторами и субъектами персональных данных и позволит субъекту подписать согласие на распространение своих персональных данных, указав необходимые условия и запреты, не взаимодействуя с оператором;

правила и порядок публикации оператором условий подписанного субъектом персональных данных согласия на распространение персональных данных неограниченному кругу лиц;

форма требования субъекта по прекращению оператором или иным лицом распространения персональных данных.

Таким образом, внесение указанных изменений закрывает один из основных пробелов настоящего федерального закона, запрещая перепечатывать персональные данные с одного ресурса в другой без разрешения субъекта персональных данных. Теперь любая публикация данных о человеке может осуществляться исключительно с его согласия.

Любое распространение персональных данных, если оно прямо не предусмотрено федеральными законами, требует обязательного согласия субъекта. Это согласие обязательно должно содержать условия распространения и возможность установления запретов для распространения отдельных категорий персональных данных. Субъекту дано право установить запрет на передачу данных неограниченному кругу лиц и обработку ими этих сведений.

Например, субъект может установить в социальной сети запрет на распространение своих изображений для всеобщего пользования и запрет на скачивание его изображений. При этом он имеет право отозвать свое согласие или внести в него дополнительные условия и ограничения в любой момент.

Важнейшим положением комментируемой статьи является запрет получения согласия автоматически - при молчании или бездействии субъекта персональных данных. При этом субъект персональных данных, требуя прекратить распространение своих персональных данных, не должен доказывать незаконность их распространения.

В результате любой сайт обязан получать согласие своих пользователей о том, какие сведения о них можно публиковать, а также можно ли передавать эти сведения третьим лицам (разрешить распространение для неограниченного круга лиц).

Ответственность за нарушение положений комментируемой статьи должна наступать в соответствии со **ст. 13.11** КоАП "Нарушение законодательства Российской Федерации в области персональных данных". Представляется, что в отдельных случаях распространение персональных данных субъекта без получения его согласия на это может быть классифицировано как уголовно-наказуемое деяние в соответствии со **ст. 137** "Нарушение неприкосновенности частной жизни" УК.

Статья 11. Биометрические персональные данные

1. **Часть 1** комментируемой статьи закрепляет общее понятие биометрических персональных данных, однако не конкретизирует их состав.

Дефиниция "биометрические персональные данные" определяет, что они характеризуют биологические или физиологические признаки лица, которые по общему правилу являются неизменными на протяжении всей жизни человека или достаточно длительного периода жизни.

Все биометрические персональные данные можно условно подразделить на две группы: изначально собираемые с целью идентификации физических лиц и собираемые с другими целями. Те виды биометрических персональных данных, которые используются для идентификации, накапливаются в массовом порядке в информационных системах, базах и банках данных. Те виды биометрических персональных данных, которые собираются с другими целями (преимущественно медицинскими), потенциально могут впоследствии использоваться в целях идентификации и поэтому также относятся к биометрическим персональным данным.

Так, является доказанным фактом, что дактилоскопические данные (отпечатки пальцев и ладоней рук, а также ног) являются неизменными на протяжении всей жизни. Генетические данные

человека также являются неизменными на протяжении всей его жизни. Фотографическое и видеоизображения, а также данные голоса человека (фоноскопические данные) меняются с возрастом и, соответственно, требуют корректировки при использовании их для целей идентификации. Кроме того, является доказанным фактом уникальность сетчатки и радужной оболочки глаза человека.

В качестве биометрических персональных данных могут также использоваться другие данные о человеке, например, его рост, вес, сведения о здоровье и другие физиологические признаки. Однако на практике для идентификации физических лиц эти виды биометрических персональных данных в России не применяются и накапливаются в основном в медицинских целях.

Таким образом, биометрическими персональными данными, используемыми в Российской Федерации для идентификации физических лиц, являются:

- дактилоскопические данные;
- данные о сетчатке и радужной оболочке глаза;
- геномная информация;
- фотографии, видео и данные голоса человека.

Для осуществления идентификации лица по его биометрическим данным требуется применение специального оборудования и программного обеспечения. Указанное оборудование используется как на этапе сбора биометрических персональных данных, так и на этапе идентификации человека, то есть при сравнении его биометрических персональных данных с данными, содержащимися в базе данных.

Также в ч. 1 комментируемой статьи указано, что биометрические персональные данные могут обрабатываться оператором только при наличии согласия в письменной форме субъекта персональных данных.

Соответственно, обработкой биометрических персональных данных является их обработка именно оператором. При этом использование лицом своих биометрических данных для осуществления доступа к электронному устройству, например, отпечатка пальца для доступа к смартфону, не является их обработкой. Это обусловлено тем, что в указанном примере биометрические персональные данные хранятся и обрабатываются самим пользователем, а не оператором.

В разъяснениях Роскомнадзора от 2 сентября 2013 г. "О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки"*(47) указано, что не относятся к биометрическим персональным данным:

- фотографии и видео, использование которых осуществляется в государственных, общественных или иных публичных интересах;
- фотографии и видео гражданина, которые получены при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях;
- фотографии и видео, когда гражданин позировал за плату;
- сканирование или ксерокопирование паспорта, а также другого документа, удостоверяющего личность;
- фотография, содержащаяся в личном деле работника;
- рентгеновские или флюорографические снимки, характеризующие физиологические и биологические особенности человека и находящиеся в истории болезни (медицинской карте) пациента (не имеет значения, бумажной или электронной), поскольку они не используются оператором (медицинским учреждением) для установления личности пациента.

При этом являются биометрическими персональными данными фотографии сотрудников, посетителей государственных и муниципальных органов, предприятий (организаций), содержащиеся в системе контроля управления доступа (СКУД). Эти фотографии характеризуют физиологические и биологические особенности человека и позволяют установить, принадлежит ли данному лицу предъявляемый СКУД пропуск. На их основе можно установить личность человека путем сравнения фото с лицом предъявителя пропуска и указываемых владельцем пропуска фамилии, имени и отчества с указанными в СКУД, и эти данные используются оператором для установления личности субъекта персональных данных в случае сомнения в том, что пропуск предъявляется его действительным владельцем.

Таким образом, фотографическое изображение и иные сведения, используемые для обеспечения однократного и (или) многократного прохода на охраняемую территорию и установления личности гражданина, также относятся к биометрическим персональным данным. Соответственно, организация должна получать письменное согласие своих сотрудников и посетителей на использование их изображений в СКУД.

2. **Часть 2** комментируемой статьи предусматривает возможность обработки биометрических персональных данных без согласия лица в различных правоохранительных и государственных целях. К ним относятся:

реализация международных договоров России о реадмиссии;
 осуществление правосудия и исполнение судебных актов;
 проведение обязательной государственной дактилоскопической регистрации;
 случаи, предусмотренные законодательством РФ об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством, законодательством о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.

Для реализации всех вышеперечисленных целей в Российской Федерации создано 3 системы обработки биометрических персональных данных, которые функционируют в масштабах всей страны:

дактилоскопическая идентификационная система;
 система генетической идентификации;
 единая биометрическая система.

Для сбора дактилоскопических сведений используются дактилоскопические сканеры. Для автоматизации обработки дактилоскопической информации и последующей идентификации лиц применяются автоматизированные дактилоскопические идентификационные системы (АДИС), преимущественно АДИС "Папилон" ("Системы Папилон": <https://www.papillon.ru/>).

Для сбора данных ДНК биологических объектов (ДНК-профилей) используются биологические следы человека - кровь, сперма, слюна, волосы, фрагменты тканей тела и иной биологический материал. После проведения анализов данные ДНК накапливаются в Федеральной системе генетической идентификации, которая также используется для автоматизации обработки указанных данных.

Для сбора фотографий и записей голоса человека в Единой биометрической системе используются сертифицированные камеры. Для обработки сведений в Единой биометрической системе применяется специальное программное обеспечение.

Сведения о сетчатке и радужной оболочке глаза человека во всероссийских системах обработки биометрических персональных данных в настоящий момент не применяются.

Формирование дактилоскопических информационных ресурсов осуществляется всеми правоохранительными органами Российской Федерации, но ведется преимущественно органами внутренних дел. Основой для формирования дактилоскопических информационных ресурсов являются [п. 27 ч. 1 ст. 12, пп. 19 и 32 ч. 1 ст. 13](#) Федерального закона от 7 февраля 2011 г. N 3-ФЗ "О полиции". Данный закон установил полномочия полиции осуществлять государственную дактилоскопическую регистрацию, дактилоскопировать всех задержанных лиц, формировать дактилоскопические информационные ресурсы.

Банк данных дактилоскопической информации состоит из следов рук неустановленных лиц, изъятых с места преступления, и информации, получаемой при государственной дактилоскопической регистрации.

Государственная дактилоскопическая регистрация подразделяется на добровольную и обязательную и осуществляется в соответствии с Федеральным законом от 25 июля 1998 г. N 128-ФЗ "О государственной дактилоскопической регистрации в Российской Федерации". [Статьей 1](#) названного закона определено, что дактилоскопической информацией называются биометрические персональные данные об особенностях строения папиллярных узоров пальцев и (или) ладоней рук человека, позволяющие установить его личность. Таким образом, в дактилоскопические информационные ресурсы включаются отпечатки пальцев и ладоней рук человека.

Целью государственной дактилоскопической регистрации в соответствии со [ст. 2](#) Федерального закона от 25 июля 1998 г. N 128-ФЗ является идентификация личности человека. В [ст. 6](#) дополнительно закреплено, что дактилоскопическая идентификация имеет следующие цели:

розыск без вести пропавшего лица;
 идентификация неопознанного трупа;

подтверждение личности лица или установление личности лица в случае, если это лицо из-за возраста или состояния здоровья не может само сообщить данные о себе, а также не имеет при себе никаких документов.

Кроме того, целью идентификации человека по дактилоскопическим информационным ресурсам является предупреждение, раскрытие и расследование преступлений, а также предупреждение и выявление административных правонарушений.

В соответствии со [ст. 7](#) Федерального закона от 25 июля 1998 г. N 128-ФЗ добровольность дактилоскопической регистрации предусматривает письменное подтверждение лицом его желания осуществить данную регистрацию. Форма заявления утверждена в [Приложении N 1](#) Административного регламента МВД по предоставлению государственной услуги по проведению добровольной государственной дактилоскопической регистрации в Российской Федерации, утв.

[приказом](#) МВД от 28 сентября 2018 г. N 640.

Перечень лиц, которые подлежат обязательной дактилоскопической регистрации, закреплён в [ст. 9](#) Федерального закона от 25 июля 1998 г. N 128-ФЗ и может быть подразделен на четыре группы:

- 1) военнослужащие, сотрудники и работники правоохранительных органов, государственные служащие отдельных ведомств;
- 2) лица, которые работают в определенной сфере деятельности: спасатели, члены летных экипажей, частные детективы и охранники, работники ведомственной охраны, моряки и др.;
- 3) мигранты, которые приезжают на длительный срок с целями проживания или трудовой деятельности на территории России;
- 4) лица, совершившие или подозреваемые в совершении преступления, находящиеся под административным арестом, личность которых невозможно или сложно установить.

Полный [перечень](#) должностей лиц, которые подлежат обязательной государственной дактилоскопической регистрации и включаются в первую группу, закреплён [постановлением](#) Правительства от 6 апреля 1999 г. N 386.

Порядок прохождения обязательной дактилоскопической регистрации некоторых категорий лиц устанавливается приказом соответствующего министерства или ведомства. В качестве примера можно привести [приказ](#) МЧС от 5 мая 2012 г. N 255 "Об организации в МЧС России работы по проведению обязательной государственной дактилоскопической регистрации".

Дактилоскопирование моряков осуществляется в процессе выдачи паспорта моряка на основании Административного регламента Федерального агентства морского и речного транспорта предоставления государственной услуги по оформлению и выдаче удостоверений личности моряка членам экипажей морских судов, судов смешанного (река-море) плавания и судов рыбопромыслового флота, утв. приказом Минтранса от 12 декабря 2013 г. N 460.

Дактилоскопирование частных охранников осуществляется перед выдачей им удостоверения на основании [Административного регламента](#), утв. [приказом](#) Росгвардии от 28 июня 2019 г. N 228.

Дактилоскопирование частных детективов осуществляется перед лицензированием их деятельности на основании [Административного регламента](#), утв. [приказом](#) Росгвардии от 28 июня 2019 г. N 227. Подразделения Росгвардии не осуществляют и не организывают дактилоскопическую регистрацию. Частные детективы и охранники обязаны самостоятельно пройти дактилоскопическую регистрацию в полиции и указать в заявлении, когда и где она была пройдена.

Сотрудники ведомственной охраны также обязаны самостоятельно пройти дактилоскопическую регистрацию или предоставить сведения о том, где и когда они проходили ее раньше. [Пункт 13](#) Административного регламента государственного контроля за деятельностью подразделений ведомственной охраны, утв. [приказом](#) Росгвардии от 21 декабря 2018 г. N 651, предусматривает только проверку документов, которые подтверждают прохождение сотрудниками ведомственной охраны дактилоскопической регистрации.

Осуществляется обязательное дактилоскопирование всех иностранных граждан и лиц без гражданства, которые собираются находиться на территории России длительное время. К ним относятся лица, которые приехали в нашу страну на работу и получают разрешение на работу или патент, а также лица, которые собираются проживать в России и получают вид на жительство, разрешение на временное проживание или удостоверение беженца.

В [Федеральном законе](#) от 25 июля 2002 г. N 115-ФЗ "О правовом положении иностранных граждан в Российской Федерации" определено место прохождения обязательной дактилоскопической регистрации иностранными гражданами:

для лиц, обратившихся за получением разрешения на временное проживание, - место подачи заявления или будущее место жительства ([ч. 4 ст. 6](#));

для лиц, незаконно находящихся в России, подлежащих депортации или реадмиссии, - месте содержания ([ст. 33](#)).

Дактилоскопическая регистрация трудовых мигрантов проводится в месте получения патента или разрешения на работу в соответствии с [Порядком](#), утв. [приказом](#) МВД от 13 августа 2018 г. N 514 "Об утверждении Порядка проведения территориальными органами Министерства внутренних дел Российской Федерации обязательной государственной дактилоскопической регистрации и фотографирования иностранных граждан и лиц без гражданства, в отношении которых принято решение о выдаче разрешительных документов, предоставляющих право на осуществление трудовой деятельности в Российской Федерации".

Формирование дактилоскопического массива осуществляется преимущественно МВД России на основании Положения, утв. совместным [приказом](#) 12 министерств и ведомств, а также Главного управления специальных программ Президента от 23 сентября 2020 г.*[\(48\)](#) Указанный совместный приказ разграничивает ведение дактилоскопического массива информации по ведомствам.

подавляющее большинство массивов дактилоскопической информации формируется и ведется МВД. Однако ряд ведомств осуществляет ведение массивов дактилоскопической информации по своим сотрудникам самостоятельно. К таким ведомствам относятся ФСБ, СВР и Минобороны в отношении сотрудников внешней разведки, ФСО, ФНС, СК. Это осуществляется в целях обеспечения безопасности государства в целом, и этих сотрудников, в частности, поскольку существует возможность утечки информации из общего массива дактилоскопической регистрации.

Система генетической идентификации функционирует в Российской Федерации на основании Федерального закона от 3 декабря 2008 г. N 242-ФЗ "О государственной геномной регистрации в Российской Федерации". В соответствии с данным законом в Российской Федерации государственная геномная регистрация проводится в целях идентификации личности человека. [Статьей 6](#) указанного федерального закона определено, что проводятся добровольная и обязательная государственная геномная регистрация.

В соответствии со [ст. 7](#) того же закона обязательной государственной геномной регистрации подлежат:

лица, осужденные и отбывающие наказание в виде лишения свободы за совершение тяжких или особо тяжких преступлений, а также всех категорий преступлений против половой неприкосновенности и половой свободы личности;

неустановленные лица, биологический материал которых изъят в ходе производства следственных действий.

неопознанные трупы.

[Порядок](#) проведения обязательной государственной геномной регистрации лиц, осужденных и отбывающих наказание в виде лишения свободы, установлен [постановлением](#) Правительства от 11 октября 2011 г. N 828.

В соответствии со [ст. 8](#) Федерального закона от 3 декабря 2008 г. N 242-ФЗ добровольная государственная геномная регистрация граждан Российской Федерации, а также иностранных граждан и лиц без гражданства, проживающих или временно пребывающих на территории Российской Федерации, проводится на основании их письменного заявления и на платной основе.

[Статья 14](#) закрепила цели использования геномной информации, полученной в результате проведения государственной геномной регистрации. К ним относятся:

предупреждение, раскрытие и расследование преступлений, а также выявление и установление лиц, их совершивших;

розыск пропавших без вести граждан Российской Федерации, а также иностранных граждан и лиц без гражданства, проживающих или временно пребывающих на территории Российской Федерации;

установление личности человека, чей труп не опознан иными способами;

установление родственных отношений разыскиваемых (устанавливаемых) лиц.

Учет геномной информации, полученной при проведении государственной геномной регистрации, ведется МВД. Для автоматизации ведения учета информационных карт геномной информации создана Федеральная система генетической идентификации (Ксенон-2)*[\(49\)](#).

Функционирование Единой биометрической системы осуществляется на основании [ст. 14.1](#) ФЗ "Об информации, информационных технологиях и о защите информации". В настоящий момент единая информационная система персональных данных (Единая биометрическая система, ЕБС) находится на стадии формирования и позволяет гражданину проходить удаленную идентификацию по биометрическим образцам для получения некоторых финансовых услуг. Размещение сведений в ЕБС осуществляется банками. В перспективе планируется размещение сведений в системе государственными и муниципальными органами и организациями, преимущественно многофункциональными центрами. После полномасштабного внедрения Единая биометрическая система должна стать национальной платформой, обеспечивающей доступ граждан к государственным и муниципальным информационным ресурсам. В качестве перспективных направлений использования Единой биометрической системы выделяют:

применение биометрической идентификации вместо электронной подписи при оказании государственных услуг и выполнении функций;

применение биометрической идентификации при осуществлении коммерческих сделок и нотариальном их заверении;

биометрическую идентификацию личности для участия граждан в дистанционном голосовании в ходе избирательных компаний.

В состав сведений, помещаемых в Единую биометрическую систему, включены данные изображения лица человека, полученные с помощью фото- видео устройств, и данные голоса человека, полученные с помощью звукозаписывающих устройств. [Состав](#) сведений и особенности их формирования, обработки, хранения и использования установлены в [постановлении](#) Правительства от

30 июня 2018 г. N 772.

Изображения лица человека и его голос были выбраны как самые распространенные и доступные для массового использования биометрические модальности. Они не требуют специального оборудования для считывания, могут быть сняты и переданы любым смартфоном. Отпечатки пальцев не используются из-за низкой чувствительности сканеров смартфонов и закрытого программно-аппаратного обеспечения вендора. Поскольку программное обеспечение для снятия отпечатков пальцев произведено за пределами Российской Федерации, то оно не может обеспечить должный уровень безопасности обработки биометрических персональных данных^{*(50)}.

Распоряжением Правительства от 22 февраля 2018 г. N 293-р функции оператора системы возложены на публичное акционерное общество междугородной и международной электрической связи "Ростелеком".

Доступ в единую биометрическую систему осуществляется или на портале Госуслуг (gosuslugi.ru) или на портале Единой биометрической системы (bio.rt.ru). Процедура удаленной идентификации гражданина с помощью Единой биометрической системы также осуществляется через мобильное приложение. Удаленный доступ осуществляется через встроенные криптографические средства защиты информации.

Передача биометрических данных для их актуализации предусмотрена внепланово при критических травмах или планово с периодичностью один раз в 3 года.

Также к биометрическим персональным данным относятся фотографии граждан, которые накапливаются в различных информационных системах в процессе оформления документов. Наиболее крупными такими системами являются:

Государственная система изготовления, оформления и контроля паспортно-визовых документов нового поколения (ГС ПВДНП) - учет выданных паспортов граждан Российской Федерации, удостоверяющих личность граждан Российской Федерации на территории России, и учет выданных паспортов, удостоверяющих личность граждан Российской Федерации за пределами территории России, в том числе содержащих электронный носитель информации;

Государственная информационная система миграционного учета (ГИСМУ) - банк данных по учету иностранных граждан и лиц без гражданства;

Федеральная информационная система Госавтоинспекции МВД (ФИС ГИБДД-М) - подсистема "Водительские удостоверения" о выданных водительских удостоверениях и других сведениях для допуска водителя к участию в дорожном движении.

3. В **ст. 4** Регламента ЕС о защите персональных данных даны несколько определений биометрических персональных данных:

генетические данные - персональные данные, касающиеся унаследованных или приобретенных генетических характеристик физического лица, которые предоставляют уникальную информацию о физиологии или здоровье указанного физического лица и которые являются результатом, в частности, анализа биологического образца соответствующего физического лица;

биометрические данные - персональные данные, возникающие в результате особой технической обработки, касающиеся физических, физиологических или поведенческих характеристик физического лица, которые предусматривают или подтверждают уникальную идентификацию указанного физического лица, например, изображение лица человека или дактилоскопические данные;

данные в отношении здоровья - персональные данные, касающиеся физического или психического здоровья физического лица, в том числе предоставление медицинских услуг, которые раскрывают информацию о состоянии его или ее здоровья.

Таким образом, Регламент подразделил биометрические персональные данные на генетические, биометрические, используемые для идентификации физического лица, и данные о здоровье. Как мы отмечали выше, российское законодательство не выделяет отдельно виды биометрических данных. Однако фактически они подразделяются на используемые для идентификации, в том числе генетические, и не используемые для идентификации, то есть данные в отношении здоровья. Соответственно, российский подход менее конкретизирован и существенно шире.

Директива ЕС о защите физических лиц при обработке персональных данных компетентными органами в **ст. 3** содержит аналогичные определения генетических данных, биометрических данных и данных в отношении здоровья.

Регламент ЕС о защите персональных данных отнес все виды биометрических персональных данных к особым категориям персональных данных и установил для них специальный порядок их сбора и дальнейшего исследования.

В комментируемом законе особые категории персональных данных подразделены на две разных группы: специальные категории персональных данных (**ст. 10**) и биометрические персональные данные (**ст. 11**). Соответственно, основания для обработки особых категорий персональных данных, указанные

в [ст. 9](#) Регламента ЕС, в российском законе также указаны в двух разных статьях.

Важнейшим основанием в обоих правовых актах указано согласие субъекта биометрических персональных данных на их обработку.

Однако в Регламенте ЕС полностью отсутствуют основания для обработки персональных данных в целях безопасности, обороны, противодействия терроризму и т.д., закрепленные в [ч. 2 ст. 11](#) настоящего федерального закона. Прямой анализ оснований обработки биометрических персональных данных, указанных в [ст. 9](#) Регламента ЕС, показывает, что в правоохранных целях допускается их обработка только для предъявления, исполнения или защиты судебных исков или в случаях, когда суды действуют в пределах своей судебной компетенции. При этом допускается обработка специальных категорий персональных данных:

в целях исполнения обязательств и особых прав контролера или субъекта данных в сфере трудового законодательства, права социального обеспечения и социальной защиты;

фондом, объединением или некоммерческой организацией в рамках их законной деятельности с соответствующими гарантиями в политических, философских, религиозных или профсоюзных целях;

по причинам особого общественного интереса на основании законодательства Союза или государства-члена ЕС;

в целях превентивной или профессиональной медицины;

по причинам общественного интереса в области народного здравоохранения;

для целей архивизации информации в интересах государства, для научных, исторических или статистических целей.

Директива ЕС о защите физических лиц при обработке персональных данных компетентными органами в [ст. 10](#) предусматривает только 3 основания для обработки специальных категорий персональных данных:

если это разрешено законодательством Европейского Союза или государства-члена ЕС;

если это необходимо для защиты жизненных интересов субъекта данных или другого физического лица;

если такая обработка относится к персональным данным, которые субъект данных явно сделал общедоступными.

При этом в [п. 19 преамбулы](#) рассматриваемого Регламента ЕС сделана оговорка, что возможно введение ограничений для защиты специфических важных интересов, включая общественную безопасность и предупреждение, расследование, выявление уголовных преступлений или привлечение к ответственности или приведение в исполнение уголовных наказаний, в том числе защиту и предотвращение угроз общественной безопасности. Однако введение ограничений допускается на уровне государств-членов ЕС.

Директива вообще вывела из-под своего правового регулирования вопросы обработки биометрических персональных данных в правоохранных целях, закрепив в [п. 5 преамбулы](#), что она не применяется в деятельности в области судебного сотрудничества по уголовным делам и полицейского сотрудничества. Также в [п. 11 преамбулы](#) Директива указывает на необходимость разработки отдельной директивы, которая установила бы специальные правила о защите физических лиц при обработке персональных данных компетентными органами в целях предотвращения, расследования, выявления или уголовного преследования преступлений или исполнения уголовных наказаний, включая защиту от угроз общественной безопасности и предотвращение таких угроз, с учетом специфического характера указанных видов деятельности.

Можно констатировать, что подход к обработке биометрических персональных данных в России и ЕС принципиально отличается. В России допускается их сбор, накопление, хранение и использование преимущественно в общественных целях, причем в основном без согласия субъекта персональных данных. В ЕС в таких целях обработка биометрических персональных данных запрещена, зато осуществляется во многих целях негосударственными организациями. Кроме того, можно сделать вывод, что существенная часть вопросов обработки биометрических персональных данных делегирована правовыми документами ЕС на уровень государств-членов ЕС.

Статья 12. Трансграничная передача персональных данных

1. [Часть 1](#) комментируемой статьи ограничивает состав государств, на территорию которых могут передаваться персональные данные. К ним относятся или конкретные страны, которые являются сторонами [Конвенции](#) о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. (далее - Конвенция), или государства, обеспечивающие адекватную защиту прав субъектов персональных данных.

Сторонами [Конвенции](#) являются 47 государств - членов Совета Европы, которые подписали и ратифицировали данный международный правовой акт. Кроме того, к Конвенции присоединились 8

государств, не являющихся членами Совета Европы, которые ратифицировали ее, не подписывая. Таким образом, в настоящий момент в Конвенции участвует 55 государств.

Российская Федерация подписала [Конвенцию](#) 7 ноября 2001 года и ратифицировала ее [Федеральным законом](#) от 19 декабря 2005 г. N 160-ФЗ. В указанном законе сделано исключение для двух видов персональных данных, которые не попадают под действие правил о трансграничной передаче данных. Это персональные данные, обрабатываемые физическими лицами исключительно для личных и семейных нужд, а также персональные данные, относящиеся к государственной тайне в соответствии с [Законом](#) РФ от 21 июля 1993 г. N 5485-1 "О государственной тайне".

[Конвенция](#) действует на территории России с 1 сентября 2013 года. Для обеспечения действия Конвенции был принят [Федеральный закон](#) от 7 мая 2013 г. N 99-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных" и Федерального закона "О персональных данных".

Также в [части 1](#) комментируемой статьи установлено право государства на запрет или ограничение трансграничной передачи персональных данных в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства. С одной стороны, указанные запреты или ограничения не противоречат международным обязательствам Российской Федерации. Однако, с другой стороны, сама [Конвенция](#) не допускает никаких запретов и ограничений, а [Федеральный закон](#) от 19 декабря 2005 г. N 160-ФЗ, которым осуществлялась ратификация Конвенции, не установил возможность таких запретов и ограничений. В этой связи данная норма представляется бланкетной, а реальные запреты и ограничения могут быть введены только в отношении информации, являющейся государственной тайной.

2. [Часть 2](#) комментируемой статьи определила, что 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, утверждается Роскомнадзором. По состоянию на 1 октября 2020 года в него входят 22 государства^{*(51)}.

Для того чтобы государство было признано обеспечивающим адекватную защиту прав субъектов персональных данных, необходимо, чтобы нормы права в отношении персональных данных и применяемые меры безопасности соответствовали положениям [Конвенции](#). Такие государства, как Мексика, Кабо-Верде, Швейцария и Сенегал сначала выполнили требования Конвенции и были включены в список Роскомнадзора, а впоследствии присоединились к Конвенции.

Необходимо обратить внимание на тот факт, что такие крупные государства, как США, Китай и Индия, не обеспечивают, по мнению Роскомнадзора, адекватную защиту прав субъектов персональных данных, соответственно, трансграничная передача персональных данных в указанные страны невозможна. Это обусловлено, в первую очередь, тем, что указанные государства не пожелали подстраиваться под европейские нормы в целом и положения [Конвенции](#) в частности.

Из всех государств бывшего СССР [Конвенцию](#) подписали Азербайджан, Армения, Грузия, Молдова и Украина. В список Роскомнадзора был включен только Казахстан. Таким образом, формально в соответствии с положениями комментируемой [статьи](#) трансграничная передача персональных данных не допускается с Белоруссией, Узбекистаном, Туркменией, Таджикистаном и Киргизией. Но реально между государствами СНГ заключены соглашения по разным направлениям деятельности, в которых отдельно установлена возможность и порядок трансграничной передачи персональных данных.

К таким соглашениям относятся, например, [Соглашение](#) о сотрудничестве в создании государственных информационных систем паспортно-визовых документов нового поколения и дальнейшем их развитии и использовании в государствах-участниках СНГ (заключено в г. Кишиневе 14 ноября 2008 г.) и [Соглашение](#) о сотрудничестве государств-участников СНГ в создании совместимых национальных телемедицинских систем и дальнейшем их развитии и использовании (заключено в г. Санкт-Петербурге 19 ноября 2010 г.).

Однако большая часть обмена информацией, относящейся к персональным данным, между государствами СНГ осуществляется в соответствии с соглашениями в экономической и правоохранительной сферах, которые даже не упоминают такое понятие, как "трансграничная передача". Можно упомянуть, например:

[Протокол](#) об обмене информацией в электронном виде между государствами - участниками СНГ для осуществления налогового администрирования (подписан в г. Астане 2 ноября 2018 г.);

[Соглашение](#) об обмене информацией в рамках Содружества Независимых Государств в сфере борьбы с терроризмом и иными насильственными проявлениями экстремизма, а также их

финансированием (заключено в г. Ташкенте 3 ноября 2017 г.);

[Соглашение](#) об обмене информацией в сфере борьбы с преступностью (заключено в г. Астане 22 мая 2009 г.) и др.

Указанные международные правовые акты предусматривают обмен информацией, которая относится, в том числе и к персональным данным.

3. [Часть 3](#) комментируемой статьи установила, что оператор до начала трансграничной передачи персональных данных обязан убедиться, что тот оператор в иностранном государстве, которому осуществляется передача персональных данных, обеспечивает их адекватную защиту.

Критериев, определяющих адекватность защиты прав субъектов персональных данных на территории иностранного государства, действующим законодательством Российской Федерации не предусмотрено. Помимо наличия государства в одном из двух списков: участвующих в [Конвенции](#) (55 стран) и перечисленных в перечне Роскомнадзора (22 страны), легального порядка определения адекватности не существует.

Для обеспечения контроля за деятельностью операторов приняты [Правила](#) организации и осуществления государственного контроля и надзора за обработкой персональных данных, утв. [постановлением](#) Правительства от 13 февраля 2019 г. N 146, и [Административный регламент](#) исполнения Роскомнадзором государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, утв. [приказом](#) Минкомсвязи от 14 ноября 2011 г. N 312.

Необходимо согласиться с учеными в том, что наличие такой нормы и отсутствие критериев адекватности приводит к тому, что операторы вынуждены самостоятельно осуществлять сравнительно-правовые исследования в целях определения наличия у той или иной страны адекватной защиты прав субъектов персональных данных*(52). Но легитимной трансграничная передача персональных данных может считаться только или в вышеуказанные 77 государств, или при соблюдении требований [ч. 4](#) комментируемой статьи. Во всех остальных случаях определение адекватности оператором самостоятельно может привести к принятию Роскомнадзором решения о том, что данные действия являются нарушением.

4. В [ч. 4](#) комментируемой статьи перечислены 5 случаев, которые допускают возможность трансграничной передачи персональных данных в любое государство без определения адекватности.

Эти случаи опираются на основания для обработки персональных данных, закрепленные в [ст. 6, 10 и 11](#) настоящего федерального закона. К ним относятся:

1) согласие субъекта в письменной форме. Основой для обработки указанных персональных данных являются [п. 1 ч. 1 ст. 6](#) и [п. 1 ч. 2 ст. 10](#) настоящего федерального закона. Такое согласие должно быть конкретным, сознательным, информированным и оформлено в соответствии со [ст. 9](#) комментируемого закона. Согласие может быть оформлено в письменной форме или в форме электронного документа, подписанного электронной подписью, в соответствии с [Федеральным законом](#) от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи";

2) случаи, предусмотренные международными договорами. Основой для обработки указанных персональных данных являются [п. 2 ч. 1 ст. 6](#) и [п. 2.1 ч. 2 ст. 10](#) комментируемого закона. Международные договоры и соглашения, в том числе двусторонние или многосторонние межправительственные и межведомственные договоры, предусматривающие обмен информацией, позволяют осуществлять трансграничную передачу персональных данных без дополнительных условий. Как мы отметили выше, само словосочетание "трансграничная передача", как правило, не используется, также может отсутствовать в тексте договора словосочетание "персональные данные". Вместо указанных дефиниций применяются словосочетания "сведения о лицах", "информация о лицах", "обмен информацией" и др.;

3) случаи, предусмотренные федеральными законами, в следующих государственных целях:
защита основ конституционного строя России;
обеспечение обороны и безопасности страны;
обеспечение транспортной безопасности.

Основой для обработки указанных персональных данных являются [п. 7 ч. 2 ст. 10](#) и [ч. 2 ст. 11](#) настоящего федерального закона;

4) исполнение договора, стороной которого является субъект персональных данных. Основой для обработки указанных персональных данных являются [п. 5 ч. 1 ст. 6](#) и [п. 6 ч. 2 ст. 10](#) настоящего федерального закона. При этом в самом договоре должна быть установлена необходимость трансграничной передачи персональных данных. В качестве примеров можно привести трансграничную передачу данных о клиенте туристическим агентством в зарубежный отель для целей бронирования или трансграничную передачу данных о пассажире авиаперевозчику и т. п.

Кроме того, трансграничная передача информации, в том числе персональных данных,

осуществляется при работе пользователя с современными телекоммуникационными устройствами и облачными сервисами. Подавляющее большинство хранилищ данных IT-компаний находится за пределами Российской Федерации, в том числе серверы мессенджеров (Viber, WhatsApp, Telegram), социальных сетей (Twitter, Instagram, Facebook) и облачных хранилищ (Google). Кроме того, сведения о клиентах собирают компании - производители программного обеспечения в целом и операционных систем в частности, как для персональных компьютеров (Windows), так и для мобильных устройств (Android, iOS). Договоры с вышеперечисленными и другими аналогичными компаниями, подписываемые пользователями в электронном виде при подключении, предусматривают трансграничную передачу персональных данных этих пользователей без их дополнительного согласия, в том числе биометрических и специальных категорий персональных данных.

Попытки российского государства обеспечить обработку персональных данных наших граждан на территории России, в том числе требование о локализации, содержащееся в [ч. 5 ст. 18](#) настоящего федерального закона, пока не увенчались успехом. Большую часть производителей перенести серверы из Европы или США в Россию заставить не удалось;

5) защита жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия субъекта персональных данных в письменной форме. Основой для обработки указанных персональных данных являются [п. 6 ч. 1 ст. 6](#) и [п. 3 ч. 2 ст. 10](#) настоящего федерального закона.

Персональные данные после их трансграничной передачи обрабатываются в иностранном государстве в соответствии с его законодательством о персональных данных и действие комментируемого закона на переданные персональные данные не распространяется.

Необходимо отметить, что в соответствии с [ч. 2 ст. 5](#) настоящего федерального закона не допускается обработка персональных данных, не соответствующая цели сбора этих персональных данных. В этой связи трансграничная передача персональных данных должна проверяться не только на соответствие государства установленным требованиям, но и на соответствие цели сбора данных. Так, например, сбор персональных данных клиентов магазинов при оформлении дисконтных карт не должен допускать их последующую трансграничную передачу, даже если производители товаров находятся за пределами России.

Кроме того, в настоящий момент трансграничная передача персональных данных осуществляется оператором, как правило, в электронном виде. Соответственно, при правовой оценке правомерности действий оператора должны учитываться положения [ст. 16](#) комментируемого закона, определяющие порядок автоматизированной обработки персональных данных.

5. Анализируя подход государств - членов Европейского Союза к трансграничной передаче персональных данных, можно сделать вывод, что они руководствуются не [Конвенцией](#) 1981 г., а [Регламентом](#) ЕС о защите персональных данных и [Директивой](#) ЕС о защите физических лиц при обработке персональных данных компетентными органами.

Вопросы трансграничной передачи персональных данных регулируются [гл. V](#) Регламента "Передача персональных данных третьим странам или международным организациям". В Директиве вопросы трансграничной передачи персональных данных также регулируются [гл. V](#) с аналогичным названием. При этом передача персональных данных из одного государства ЕС в другое не признается трансграничной передачей и не попадает под регулирование данной главы. Российская Федерация в данном случае признается законодательством ЕС в качестве третьей страны.

Если положения [ст. 12](#) комментируемого закона прямо предусматривают возможность передачи персональных данных на территорию иностранного государства, являющегося стороной [Конвенции](#), то документы Европейского Союза Конвенцию даже не упоминают.

Положения [Регламента](#) и [Директивы](#) дублируют друг друга и предусматривают почти идентичный порядок принятия решения о передаче персональных данных в третью страну или международную организацию.

Первым вариантом принятия решения является передача персональных данных на основании решения о соответствии, которое принимается Европейской Комиссией. Решение о соответствии предполагает, что третья страна, территория, один или несколько специфических секторов в указанной третьей стране, или соответствующая международная организация гарантируют надлежащий уровень защиты. Подобный подход аналогичен российскому подходу о признании государства обеспечивающим адекватную защиту прав субъектов персональных данных. Однако, в отличие от России, где решение принимается Роскомнадзором, в ЕС решение принимается наднациональным органом - Европейской Комиссией.

Учитывая уровень отношений между Россией и Европейской Комиссией, который в настоящее время является наихудшим за все годы существования Российской Федерации и Европейского Союза, возможно предположить, что получение решения о соответствии не будет принято еще длительное

время, если вообще когда-то будет принято. Отдельные авторы утверждают, что виной этому несовершенство российского законодательства, особенности правоприменительной практики, недостаточность самостоятельности Роскомнадзора, плохая работа судебной системы*(53). Однако представляется, что даже при полном исправлении всех вышеуказанных недостатков положительное решение на уровне Еврокомиссии не будет принято в обозримой исторической перспективе по политическим причинам.

Вторым вариантом принятия решения является передача персональных данных при условии соблюдения соответствующих гарантий. Контролер или обрабатывающее данные лицо могут передать персональные данные третьей стране или международной организации в случае, если контролер или обрабатывающее данные лицо предусмотрели соответствующие гарантии и если субъекты данных обладают юридически защищенными правами и эффективными средствами правовой защиты. В Регламенте ЕС о защите персональных данных предусмотрено 6 способов предоставления гарантий. Директива ЕС о защите физических лиц при обработке персональных данных установила всего 2 способа:

надлежащие гарантии в отношении защиты персональных данных предоставлены в форме имеющего обязательную юридическую силу документа;

контролер оценил все обстоятельства, сопровождающие передачу персональных данных, и пришел к выводу о наличии надлежащих гарантий в отношении защиты персональных данных.

Представляется, что данный путь для получения персональных данных российскими компаниями и организациями, в том числе государственными, является самым оптимальным. Для его практической реализации необходимо заключение юридически обязывающего соглашения об обеспечении защиты персональных данных между российской организацией и контролером в иностранном государстве.

Третьим вариантом принятия решения является утверждение компетентным надзорным органом юридически обязывающих корпоративных правил. Данный вариант закреплен только в Регламенте и действует для компаний или группы компаний, которые частично находятся в ЕС, а частично за его пределами. В процессе своей деятельности они осуществляют трансграничную передачу персональных данных. Соответственно, если надзорный орган утвердит указанные юридически обязывающие правила, то для данной компании снимаются все ограничения на передачу персональных данных, что является аналогом решения Европейской Комиссии для государства.

Четвертым вариантом принятия решения является частичное отступление для определенных случаев (отступления для особых ситуаций).

Статья 49 Регламента в ч. 1 установила следующий перечень случаев:

(а) субъект данных дал прямое согласие на соответствующую передачу данных после того, как он был проинформирован о возможных рисках указанной передачи данных вследствие отсутствия решения о соответствии и надлежащих гарантий;

(b) передача необходима для выполнения договора между субъектом данных и контролером или для имплементации преддоговорных мер, принятых по запросу субъекта данных;

(с) передача необходима для заключения договора или для исполнения договора, заключенного в интересах субъекта данных между контролером и другим физическим или юридическим лицом;

(d) передача необходима по причинам общественного интереса;

(е) передача необходима для обоснования, осуществления или оспаривания судебного иска;

(f) передача необходима для защиты жизненно важных интересов субъекта данных или других лиц, если субъект данных физически или юридически не может дать свое согласие;

(g) передача осуществляется из реестра, целью которого согласно законодательству Союза или государства-члена ЕС является предоставление информации общественности и который открыт для ознакомления широкой общественности или любому лицу, которое может доказать наличие законного интереса, но только в той мере, в какой соблюдаются условия, установленные законодательством Союза или государства-члена ЕС, для ознакомления в отдельном случае.

Причем в ч. 3 определено, что пп. (а), (b) и (с) не должны применяться в отношении деятельности, осуществляемой органами государственной власти при выполнении ими своих полномочий. Часть 4 установила, что общественный интерес в значении п. (d) должен быть признан в законодательстве Союза или в законодательстве государства-члена ЕС, под действие которого подпадает контролер.

Директива в ч. 1 ст. 38 установила пять отступлений:

(а) для защиты жизненно важных интересов субъекта данных или других лиц;

(b) для защиты законных интересов субъекта данных, если это предусмотрено законодательством государства-члена ЕС, передающего персональные данные;

(с) для предотвращения непосредственной и серьезной угрозы общественной безопасности

государства-члена ЕС или третьей страны;

(d) в отдельных случаях для целей, указанных в [ст. 1\(1\)](#) Директивы; или

(e) в отдельных случаях для установления, реализации правовых требований или для защиты по правовым требованиям в связи с целями, указанными в [ст. 1\(1\)](#) Директивы.

При этом в [ч. 2](#) определено, что персональные данные не передаются, если передающий компетентный орган установит, что основные права и свободы заинтересованного субъекта данных превосходят общественный интерес в передаче, как указано в [пп. \(d\) и \(e\) параграфа 1 ст. 38](#).

Таким образом, и [Регламент](#) и [Директива](#) установили максимально возможные преграды на передачу персональных данных государственным органам.

Поскольку и [Регламент](#) и [Директива](#) предусматривают возможность выдачи разрешений на трансграничную передачу персональных данных отдельным организациям, то разрешение получается каждой компанией или государственным органом отдельно, в том числе посредством выдачи соответствующих гарантий. Представляется, что для получения персональных данных из стран ЕС государственными органами и организациями самым целесообразным является заключение отдельных договоров по обмену информацией.

Резюмируя вышесказанное, можно констатировать, что Российская Федерация занимает неравновесное положение в сфере трансграничной передачи персональных данных с государствами - членами ЕС. Россия на основании [Конвенции](#) предоставляет персональные данные в государства ЕС фактически без ограничений. В ответ ЕС создал такой механизм получения разрешения на передачу персональных данных в третьи страны, который максимально затруднил получение данного разрешения.

[Статья 13](#). Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных

1. [Часть 1](#) комментируемой статьи делегирует государственным и муниципальным органам и организациям право на создание информационных систем персональных данных. Необходимо отметить, что большая часть государственных (муниципальных) информационных систем собирает, обрабатывает и хранит персональные данные граждан. Каждое министерство и ведомство на всех уровнях власти работает с населением, накапливает о нем информацию и использует ее в своей деятельности.

Информационные системы персональных данных являются разновидностью государственных и муниципальных информационных систем, определение которых закреплено в [ст. 13](#) ФЗ "Об информации, информационных технологиях и о защите информации".

В [ч. 3 ст. 14](#) названного закона установлено, что государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления. В [ч. 4](#) статьи установлено, что перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия ее предоставления - Правительством или соответствующими государственными органами.

Таким образом, состав персональных данных, вносимых в государственные информационные системы, должен быть установлен федеральным законом. Например, в [ст. 17](#) Федерального закона от 7 февраля 2011 г. N 3-ФЗ "О полиции" перечислены 42 категории сведений о гражданах, которые имеют право собирать органы внутренних дел и помещать в банки данных. Существенная часть этих сведений является биометрическими персональными данными или относится к специальным категориям персональных данных.

Самой известной государственной информационной системой, накапливающей персональные данные, является Единый портал государственных услуг (функций) Российской Федерации (<https://www.gosuslugi.ru>).

2. В [ч. 2](#) комментируемой статьи закреплена возможность кодирования персональных данных граждан в соответствии с особенностями учета, установленными федеральными законами. Главным условием такой кодировки с технической точки зрения является наличие у каждого субъекта не повторяющегося индивидуального номера.

В подавляющем большинстве случаев для кодировки используется Страховой номер индивидуального лицевого счета (СНИЛС) - уникальный номер индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования. Кроме того, широко применяются для обозначения принадлежности персональных данных конкретному субъекту персональных данных данные паспорта гражданина России, документа идентифицирующего личность иностранного гражданина (например, вида на жительство). В отдельных системах применяется ИНН - цифровой код, упорядочивающий учет налогоплательщиков в Российской Федерации, или номер полиса обязательного медицинского страхования.

Возможно применение других идентификаторов субъектов персональных граждан для их учета в государственных информационных системах, например, сочетания фамилии, имени, отчества (Ф. И. О.) и даты рождения, или Ф. И. О. и места регистрации, Ф. И. О. и номера мобильного телефона. Однако эти идентификаторы не обладают полной уникальностью и содержат слишком большое количество символов для корректной автоматизированной обработки.

Планировалось использовать для идентификации граждан универсальную электронную карту, которая должна была стать обязательной в соответствии с [гл. 6](#) Федерального закона от 27 июля 2010 г. N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг". Однако после возражений верующих и Русской православной церкви [Федеральным законом](#) от 28 декабря 2016 г. N 471-ФЗ обязательное внедрение универсальных электронных карт было отменено, а [гл. 6](#) Федерального закона от 27 июля 2010 г. N 210-ФЗ утратила силу.

Из опыта создания персонального идентификатора в виде отдельной электронной карты можно выделить только карту москвича - это именная пластиковая карта, которая выдается жителям г. Москвы и служит персональным электронным ключом к городской инфраструктуре*(54). Карта москвича является одновременно электронным ключом, банковской картой и дисконтной картой.

3. [Часть 3](#) комментируемой статьи устанавливает, что учет персональных данных и их кодировка не должны нарушать права и свободы граждан, оскорблять их чувства или унижать их человеческое достоинство.

Использование цифровой кодировки представляется оптимальным вариантом как с технической стороны, так и для того, чтобы не затрагивать права и чувства граждан. Однако оно может вызывать неприятие отдельных лиц. Основные возражения вызывает использование штрих-кодов, которые воспринимаются верующими как "число дьявола". Однако и другие цифровые кодировки (например, ИНН) вызывают неприятие верующих христиан. Для разъяснения позиции государства по отдельным видам кодов, присваиваемых гражданам, принимались решения судов и нормативные правовые акты.

В 2003 году Конституционный Суд РФ в [определении](#) от 10 июля 2003 г. N 287-О указал, что наличие в идентификационном номере некоего числа, могущего затрагивать религиозные чувства налогоплательщика, носит случайный характер; идентификационный номер не заменяет имя человека и подлежит использованию наряду с другими сведениями о налогоплательщике исключительно в целях налогового учета*(55). Аналогичный вывод содержится и в [определении](#) Верховного Суда РФ от 1 марта 2006 г. N 13-В05-13*(56).

В 2012 году Минздравсоцразвития в письме от 4 апреля 2012 г. N 20-1/7000775 "По вопросу несогласия граждан с введением новой системы электронного учета персональных данных при оказании медицинских услуг" разъяснил, что страховой номер (СНИЛС) присваивается индивидуальному лицовому счету, а не человеку и используется наряду с анкетными данными гражданина в целях учета его пенсионных прав, не заменяя собой его имени.

Анализ приведенных и других определений позволяет отметить устойчивую позицию государства, которая заключается в том, что любой номер не заменяет имя человека и используется только наряду с анкетными данными гражданина в целях учета. Однако, несмотря на все разъяснения, протесты граждан в связи с присвоением им цифровых кодов продолжаются.

4. В [ч. 4](#) комментируемой статьи установлена возможность создания государственного регистра населения.

В 2005 году была сделана попытка создания всеобщего государственного регистра населения - принята [Концепция](#) создания системы персонального учета населения Российской Федерации*(57). Концепция предусматривала для создания регистра введение единого идентификатора персональных данных, обеспечивающего возможность однозначного установления соответствия персональных данных, размещаемых в различных автоматизированных системах учета, конкретному физическому лицу. В последующем должна была быть осуществлена интеграция различных ведомственных автоматизированных систем учета персональных данных граждан с обеспечением к ним доступа в электронном виде государственных и муниципальных органов и организаций.

Однако из-за приведенных выше возражений религиозного характера развитие государственных информационных систем пошло по пути создания "электронного правительства", объединившего в своем составе Единый портал государственных и муниципальных услуг (функций) и Единую систему межведомственного электронного взаимодействия.

Функционирование этих и других информационных систем осуществляется в соответствии с положениями:

- [Федерального закона](#) от 27 июля 2010 г. N 210-ФЗ;

- [постановления](#) Правительства от 8 июня 2011 г. N 451 "Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и

муниципальных функций в электронной форме";

- [постановления](#) Правительства от 8 сентября 2010 г. N 697 "О единой системе межведомственного электронного взаимодействия".

Упомянутый выше портал Госуслуг и всю систему электронного правительства можно считать прообразом государственного регистра населения, но внесение в него персональных данных осуществляется гражданином добровольно и самостоятельно. Мнения, что система электронного правительства не является государственным регистром населения, придерживается и Верховный Суд РФ, который в [решении](#) от 29 мая 2012 г. N АКПИ12-645 указал, что использование в регистрах единой системы идентификации и аутентификации идентификаторов не нарушает свободу совести и вероисповедания граждан, поскольку в системе используются идентификаторы, установленные федеральными законами, и только с согласия заявителей*(58).

5. Вопросы создания государственными и муниципальными органами информационных систем персональных данных в [Регламенте](#) ЕС о защите персональных данных и [Директиве](#) ЕС о защите физических лиц при обработке персональных данных компетентными органами не рассматриваются. В указанных документах употребляется устойчивое словосочетание "обработка осуществляется органом государственной власти или правительственным учреждением", но не уточняется - создаются ли для обработки персональных данных специализированные государственные информационные системы.

Глава 3. Права субъекта персональных данных

[Статья 14.](#) Право субъекта персональных данных на доступ к его персональным данным

1. Комментируемая [статья](#) обеспечивает защиту законных интересов субъектов, чьи персональные данные находятся в распоряжении оператора. Она является первой в главе 3 настоящего федерального закона, нормы которой определяют наиболее общие, присущие всем без исключения субъектам персональных данных права.

Специальные правомочия субъектов персональных данных, возникающие при наличии определенных условий, нашли свое отражение в последующих статьях данной главы:

[ст. 15](#) - права при обработке персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации;

[ст. 16](#) - права при принятии решений на основании исключительно автоматизированной обработки персональных данных;

[ст. 17](#) - право на обжалование действий или бездействия оператора персональных данных.

Соотнося положения [ст. 14](#), [18](#) и [23](#) комментируемого закона, нельзя не отметить оригинальное распределение правомочий: находящиеся по отношению к оператору персональных данных в "слабом" организационно-финансовом положении, субъекты персональных данных обеспечиваются доступной и эффективной системой прав, позволяющих предупредить или пресечь противоправное посягательство на конфиденциальность персональных данных; недостаточная же информированность субъекта персональных данных о нарушении соответствующих прав компенсируется наращиванием контрольно-надзорного и пресекающего потенциала полномочий органов государственной власти в рассматриваемой сфере.

Подобное положение вещей полностью соответствует мировым тенденциям в формировании баланса прав, интересов и обязанностей трех указанных участников информационных правоотношений. В Директиве ЕС о защите физических лиц при обработке персональных данных компетентными органами отмечается, что эффективная защита персональных данных на территории Европейского Союза требует усиления прав субъектов данных и обязанностей лиц, осуществляющих обработку персональных данных, а также эквивалентных полномочий по контролю и обеспечению соблюдения положений для защиты персональных данных в государствах-членах ЕС ([п. 7](#)).

2. [Части 1](#) и [7](#) комментируемой статьи нормативно закрепляют три базовых и взаимосвязанных друг с другом права субъекта персональных данных, которые возникают в связи с их оборотом.

2.1. Право субъекта персональных данных на получение информации, касающейся обработки его персональных данных, является частным проявлением права на доступ к информации, чья реализация обеспечивается нормами [ст. 24](#), [29](#) и [42](#) Конституции, [ст. 10](#) Конвенции о защите прав человека и основных свобод от 4 ноября 1950 г. и [ст. 3](#), [8](#) и [16](#) ФЗ "Об информации, информационных технологиях и о защите информации".

Ознакомление субъекта персональных данных (его представителя) с информацией должно осуществляться на безвозмездной основе (см. [комментарий](#) к ч. 2 ст. 20).

Исчерпывающего перечня информации, доступ к которой субъекту персональных данных обеспечивается нормами комментируемой [статьи](#), не приведено. Это обусловлено возможностью

появления новых категорий идентифицирующих лицо сведений, а также способов и средств их обработки и использования.

При этом в [ч. 7](#) комментируемой статьи прямо указано на возможность доступа к информации, содержащей:

подтверждение факта обработки персональных данных оператором. Оператор обязан сообщить, обрабатывает ли он персональные данные субъекта, а также когда и кем они были ему переданы;

правовые основания и цели обработки персональных данных. Оператор обязан сообщить правовые основания обработки персональных данных с указанием нормы конкретного федерального закона (см. комментарий к [ч. 2 ст. 5](#) и [ч. 1 ст. 6](#));

цели и применяемые оператором способы обработки персональных данных (сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование). Оператор обязан обосновать соответствие применяемых способов цели, определенной в федеральном законе;

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;

обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом. Оператор обязан указать непосредственные категории обрабатываемых персональных данных, в том числе специальные категории персональных данных, а также субъекта или оператора, которые предоставили персональные данные для обработки;

сроки обработки персональных данных, в том числе сроки их хранения. Данные сроки должны быть обусловлены договором, требованиями федерального закона и целями обработки;

порядок осуществления субъектом персональных данных прав, предусмотренных комментируемым законом (см. [комментарии](#) к ст. 15-17);

информацию об осуществленной или о предполагаемой трансграничной передаче данных (см. [комментарий](#) к ст. 12);

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу (см. [комментарии](#) к чч. 3-5 ст. 6);

иные сведения, предусмотренные настоящим федеральным законом или другими федеральными законами.

Аналогичное понимание содержания права субъекта персональных данных на доступ к ним прослеживается в законодательстве Евросоюза. Согласно [ст. 15](#) Регламента ЕС о защите персональных данных субъект данных имеет право запрашивать у контролера подтверждение относительно того, обрабатываются ли относящиеся к нему персональные данные, и если дело обстоит именно так, он имеет право на доступ к персональным данным и связанной информации. К ней относятся:

- (a) цели обработки;
- (b) категории обрабатываемых персональных данных;
- (c) получатели или категории получателей, которым были или будут раскрыты персональные данные, в частности, получатели в третьих странах или международные организации;
- (d) по мере возможности, предусмотренный срок, в течение которого будут храниться персональные данные, или, при отсутствии соответствующей возможности, критерии, используемые для определения указанного периода;
- (e) существование права требования от контролера исправления или удаления соответствующих персональных данных, или ограничения их обработки, или возражения против указанной обработки;
- (f) право подачи жалобы в надзорный орган;
- (g) в случае если персональные данные получены не от субъекта данных, любая доступная информация об их источнике;
- (h) наличие автоматизированного процесса принятия решения, в том числе формирование профиля согласно [ст. 22\(1\)](#) и [\(4\)](#) и, как минимум в указанных случаях, достоверная информация о соответствующей логической схеме, а также о значимости и предполагаемых последствиях указанной обработки для субъекта данных.

Вместе с тем, в отличие от российского законодательства о персональных данных, нормативные акты Евросоюза предусматривают прямую, а не пассивную обязанность операторов персональных данных хранить и предоставлять по требованию субъектов персональных данных и уполномоченных должностных лиц сведения, характеризующие техническую и содержательную стороны оборота персональных данных.

Например, согласно [ст. 24](#) Директивы ЕС о защите физических лиц при обработке

персональных данных компетентными органами государства-члены ЕС должны нормативно закрепить:

1) обязанность контролеров вести учет всей деятельности, связанной с обработкой данных и подпадающей под их ответственностью.

Учетные сведения должны содержать следующую информацию:

(а) имя, фамилию и контактные сведения о контролере и, в соответствующих случаях, о контролере, осуществляющем обработку совместно с ним, и об инспекторе по защите персональных данных;

(b) цели обработки;

(с) категории получателей, которым были или будут раскрыты персональные данные, включая получателей в третьих странах или международных организации;

(d) описание категорий субъектов данных и категорий персональных данных;

(е) если применимо, использование метода формирования профиля;

(f) если применимо, категории передачи персональных данных третьей стране или международной организации;

(g) указание на правовое основание операций по обработке, включая передачу, для которых предназначены персональные данные;

(h) по возможности, предусмотренные сроки для удаления различных категорий данных;

(i) по возможности, общее описание технических и организационных мер безопасности, указанных в [ст. 29\(1\)](#) Директивы.

2) обязанность лиц, обрабатывающих данные, вести учет всех категорий операций по обработке, осуществляемых от имени контролера, с указанием:

(а) имени, фамилии и контактных сведений о лице или лицах, обрабатывающих данные, о каждом контролере, от имени которого действует обрабатывающее данные лицо, и, если применимо, об инспекторе по защите персональных данных;

(b) категорий обработки, осуществляемых от имени контролера;

(с) если применимо, передачи персональных данных третьей стране или международной организации, если на это получены прямые инструкции контролера, включая идентификационную информацию о такой третьей стране или международной организации;

(d) по возможности, общее описание технических и организационных мер безопасности, указанных в [ст. 29\(1\)](#) Директивы.

При достаточно детальной проработке категорий сведений следует обратить внимание на превалирование диспозитивных формулировок, таких как "если применимо" и "по возможности". Применение подобной юридической техники может быть оправдано разнообразием форм и условий обработки персональных данных, однако в конечном итоге требует разъяснений законодателя, суда или надзирающего органа исполнительной власти.

2.2. Право субъекта персональных данных требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, полученными незаконно или избыточными (не необходимыми) для заявленной цели обработки, включает следующие правомочия:

2.2.1. Право требовать уточнения обрабатываемых оператором персональных данных в случае их искажения, неполноты или неактуальности. Замена подобных персональных данных на актуальные, полные и точные данные должна быть произведена оператором в течение 7 дней со дня получения обращения (запроса) субъекта персональных данных. В этот же срок субъект персональных данных должен быть письменно уведомлен о корректировке обрабатываемых персональных данных (см. [комментарий](#) к ч. 3 ст. 20).

2.2.2. Право требовать блокирования неправомерно обрабатываемых, неточных или подлежащих уничтожению персональных данных (см. [комментарий](#) к [чч. 1, 2 и 6 ст. 21](#)).

2.2.3. Право требовать уничтожения персональных данных предусматривает "страховочный" механизм обеспечения законности оборота персональных данных - по общему правилу оператор при обнаружении неправомерно обрабатываемых персональных данных в течение 10 дней, а при достижении целей обработки персональных данных или отзыва субъектом персональных данных согласия на их обработку в 30-дневный срок обязан самостоятельно уничтожить их. Общий срок уничтожения персональных данных составляет 7 дней со дня получения обращения или запроса (см. [комментарий](#) к ч. 3 ст. 20). Согласно [п. 8 ст. 3](#) комментируемого закона уничтожение персональных данных - это действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Примечательно, что правовой институт уничтожения персональных данных субъекта обладает признаками административной процедуры, при которой субъект вынужден доказывать возможность и

законность ее производства, в то время как в европейском праве используется, пожалуй, более гуманный, механизм, состоящий из обязанности оператора всеми доступными способами проверять актуальность и достоверность персональных данных и безоговорочного права субъекта персональных данных "на забвение". Последний, в частности, предусмотрен ст. 17 Регламента ЕС о защите персональных данных, в [ч. 1](#) которой закрепляется право субъекта персональных данных требовать от контролера незамедлительного удаления относящихся к нему персональных данных, а также обязанность контролера (оператора) незамедлительно удалить персональные данные, если применяется одно из следующих оснований:

(a) персональные данные больше не требуются для целей, для которых они были получены или обрабатывались в иных случаях;

(b) субъект данных отзывает свое согласие, на основании которого согласно [п. \(a\) ст. 6 \(1\)](#) или [п. \(a\) ст. 9 \(2\)](#) проводилась обработка, и если отсутствует иное юридическое основание для обработки;

(c) субъект данных возражает против обработки согласно [ст. 21 \(1\)](#), и отсутствуют имеющую преимущественную юридическую силу законные основания для обработки, или субъект данных возражает против обработки согласно [ст. 21\(2\)](#);

(d) персональные данные обрабатывались незаконно;

(e) персональные данные должны быть уничтожены в целях соблюдения юридической обязанности согласно законодательству Союза или государства-члена ЕС, под действие которого подпадает контролер;

(f) персональные данные собирались в отношении предоставления услуг информационного общества согласно [ст. 8\(1\)](#).

Более того, согласно [ч. 2 ст. 17](#) указанного Регламента, если контролер обнаружил персональные данные и он согласно [параграфу 1](#) этой статьи обязан удалить персональные данные, он с учетом имеющихся технологических возможностей и расходов на имплементацию должен принять необходимые меры, в том числе технические меры, чтобы проинформировать контролеров, которые обрабатывают персональные данные, о том, что субъект данных затребовал от них удаление любых ссылок, копий или точных повторений указанных персональных данных.

Обратными по вектору регулирования в части удаления персональных данных являются нормы [ч. 3 ст. 16](#) Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами, которыми предусмотрена замена запрашиваемого субъектом удаления персональных данных на временное ограничение доступа к ним (блокирование). Основаниями принятия такого решения могут быть случаи, когда:

(a) точность персональных данных оспаривается субъектом данных, и невозможно установить их точность или неточность;

(b) персональные данные должны быть сохранены в целях предоставления доказательств.

2.3. Право субъекта персональных данных принимать предусмотренные законом меры по защите своих прав. Защита прав субъекта персональных данных может иметь восстановительный (гражданско-правовой) или охранительный (публично-правовой) характер.

В первом случае речь идет об обжаловании неправомерных действий оператора персональных данных в компетентный орган государственной власти (Роскомнадзор) или в суд (см. [комментарий](#) к ст. 17). Во втором - о привлечении оператора персональных данных к юридической ответственности (см. [комментарий](#) к ст. 24).

Вариативным результатом реализации восстановительной процедуры в контексте защиты прав субъекта персональных данных является ограничение доступа к информации, обрабатываемой с нарушением законодательства РФ в области персональных данных, которое предусмотрено [ст. 15.5](#) ФЗ "Об информации, информационных технологиях и о защите информации".

3. [Часть 8](#) комментируемой статьи предусматривает возможность ограничения права субъекта персональных данных на получение информации, касающейся обработки его персональных данных. Подобное ограничение возможно только на основании [Конституции](#) и федерального законодательства, при этом в самой комментируемой норме в качестве примеров приведены следующие условия:

1) Обработка персональных данных осуществляется в целях обороны страны, безопасности государства и охраны правопорядка. Данная формулировка имеет прямую отсылку к положениям [ч. 3 ст. 55](#) Конституции, определяющей основные цели ограничения прав человека и гражданина на территории России, в том числе права на доступ к информации.

Подобное ограничение может осуществиться в штатном и особом режиме. В первом случае речь идет о правовом режиме государственной и служебной тайны, во втором - о введении дополнительных ограничений в условиях особых правовых режимов военного или чрезвычайного положения, режима контртеррористической операции, а также ограничении доступа к информации о режимных объектах.

2) Обработка персональных данных осуществляется органами дознания и предварительного

следствия в контексте задержания субъекта персональных данных по подозрению в совершении преступления (гл. 12 УПК), предъявления ему обвинения по уголовному делу (гл. 23 УПК) или избрания ему меры пресечения (гл. 13 УПК), за исключением прямо предусмотренных УПК случаев, допускающих ознакомление подозреваемого или обвиняемого с такими персональными данными.

3) Обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Основу нормативного регулирования в данной сфере образуют нормы [Федерального закона](#) от 7 августа 2001 г. N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" и утвержденной Президентом 30 мая 2018 г. [Концепции](#) развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

4) Доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц. Формулировка данного пункта несколько противоречива, так как ознакомление субъекта с его же персональными данными априори не может нарушать тем самым права третьих лиц. Следует полагать, что речь в данном пункте идет о персональных данных субъекта, которые содержательно неотделимы от иной информации, разглашение которой влечет нарушение прав и законных интересов третьих лиц.

5) Обработка персональных данных осуществляется в случаях, предусмотренных законодательством о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства. Основу нормативного регулирования в данной сфере образуют положения [Федерального закона](#) от 9 февраля 2007 г. N 16-ФЗ "О транспортной безопасности" и [приказа](#) Минтранса от 19 июля 2012 г. N 243 "Об утверждении Порядка формирования и ведения автоматизированных централизованных баз персональных данных о пассажирах и персонале (экипаже) транспортных средств, а также предоставления содержащихся в них данных".

4. [Части 2-6](#) комментируемой статьи определяют условия и порядок реализации субъектом персональных данных права на получение сведений, указанных в [ч. 7](#) комментируемой статьи. Условиями реализации права выступают следующие обстоятельства:

1) Субъект персональных данных может быть идентифицирован на основании данных, указанных в обращении (запросе). Этот документ должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя (для граждан РФ - паспорт), сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан [электронной подписью](#) в соответствии с законодательством РФ.

Следует понимать, что в случае использования оператором персональных данных расширенного перечня критериев идентификации личности (например, корпоративные пароли или реквизиты служебных документов), эти данные также могут быть истребованы. В [ч. 5 ст. 12](#) Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами это право оператора отражено, в отличие от отечественного законодательства, достаточно конкретно: "Если контролер имеет достаточные основания для сомнения относительно личности физического лица, подающего запрос согласно [ст. 14](#) или [16](#) Директивы, он может потребовать предоставления дополнительной информации, необходимой для подтверждения личности субъекта данных".

2) Субъектом персональных данных (его представителем) должны быть соблюдены сроки и форма подачи обращения или запроса оператору персональных данных.

3) В запрашиваемых сведениях не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных, то есть при наличии согласия. При отсутствии специальных разъяснений относительно указанного исключения, следует полагать, что персональные данные третьих лиц возможно передать субъекту, чьи персональные данные неотделимы от них, при наличии согласия третьих лиц или при наличии оснований на обработку персональных данных без согласия субъекта.

Согласно [ст. 4](#) [Федерального закона](#) от 2 мая 2006 г. N 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации" обращением гражданина является направленное в государственный орган, орган местного самоуправления или должностному лицу в письменной форме или в форме электронного документа предложение, заявление или жалоба, а также устное обращение гражданина в государственный орган, орган местного самоуправления.

Аналогичное понимание обращения характерно и при обращении в негосударственные, в том числе коммерческие, организации. Требование субъекта персональных данных о получении сведений может содержаться в заявлении (просьба гражданина о содействии в реализации его конституционных прав и свобод или конституционных прав и свобод других лиц, либо сообщение о нарушении законов и иных нормативных правовых актов, недостатках в работе государственных органов, органов местного самоуправления и должностных лиц, либо критика деятельности указанных органов и должностных лиц) или жалобе (просьба гражданина о восстановлении или защите его нарушенных прав, свобод или законных интересов либо прав, свобод или законных интересов других лиц). Требования к письменному обращению субъекта персональных данных в органы публичной власти нормативно закреплены в [ст. 7](#) Федерального закона от 2 мая 2006 г. N 59-ФЗ.

Предусмотренный [ч. 3 ст. 12](#) Регламента ЕС о защите персональных данных порядок предоставления оператором субъекту персональных данных информации устанавливает схожие, а отчасти и более продолжительные сроки для ответа на запрос: контролер должен незамедлительно предоставить субъекту данных информацию о мерах, принятых в рамках запроса согласно [ст. 15-22](#), и в любом случае в течение одного месяца после получения запроса. Указанный срок может быть продлен еще на два месяца, при необходимости, с учетом сложности и количества запросов. Контролер должен проинформировать субъекта данных о любом таком продлении в течение одного месяца после получения запроса, с указанием причин превышения срока. Если субъект данных подает запрос посредством электронной формы, информация должна быть предоставлена по возможности электронным способом, если субъект данных не запрашивает иной способ передачи информации.

4.1. Порядок реализации субъектом персональных данных права на получение информации, касающейся обработки его персональных данных:

1) Направление оператору обращения или запроса субъектом персональных данных или его представителем. Подробнее о правовом статусе представителя субъекта персональных данных см. [комментарий](#) к [ч. 6 ст. 10](#).

2) Направление субъекту персональных данных оператором в 30-дневный срок со дня получения обращения или запроса запрашиваемых сведений или уведомления об отказе в предоставлении таковых при наличии соответствующих обстоятельств.

Основаниями для отказа могут быть как обстоятельства, указанные в [п. 3](#) комментария к настоящей статье, так и нарушение порядка подачи обращения (запроса); они должны быть обоснованы оператором персональных данных с указанием нормы комментируемого закона (см. [пп. 3 и 4](#) комментария к настоящей статье). Срок рассмотрения обращения (запроса) включает день его получения и рассчитывается календарными днями, включая выходные и праздничные дни.

Запрашиваемые сведения должны быть представлены субъекту персональных данных (его представителю) в доступной форме. Данное требование при отсутствии официальных разъяснений свободно для интерпретации. По общему правилу, согласно [ч. 4 ст. 10](#) ФЗ "О порядке рассмотрения обращений граждан Российской Федерации", сведения представляются в той же форме (на бумажном носителе или в электронном сообщении) и формате (расширение и структура файла электронного документа).

Полагаем, на направляемый субъекту персональных данных ответ распространяются и положения [ч. 5 ст. 15](#) Закона РФ от 25 октября 1991 г. N 1807-1 "О языках народов Российской Федерации", согласно которым ответы на предложения, заявления и жалобы граждан Российской Федерации даются на языке обращения, а в случае невозможности дать ответ на языке обращения используется государственный язык Российской Федерации.

3) Повторное обращение (запрос) субъекта персональных данных (его представителя) к оператору персональных данных, который по первичному его обращению (запросу) представил истребуемые сведения, может быть осуществлено не ранее, чем через 30 дней после первичного обращения (запроса).

4) Повторное обращение (запрос) субъекта персональных данных (его представителя) к оператору персональных данных, который по первичному его обращению (запросу) не представил истребуемые сведения в полном объеме, может быть осуществлено в любой момент после получения ответа на первичное обращение (запрос). В подобном обращении (запросе) должно содержаться обоснование его повторного направления.

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 состоит из трех фундаментальных положений:

необходимость получения согласия субъекта персональных данных на их использование в целях

коммерческой рекламы при прямом с ним контакте с помощью средств связи;

необходимость получения согласия субъекта персональных данных на их использование в целях политической агитации при прямом с ним контакте с помощью средств связи;

закрепление презумпции вины оператора, состоящей в возложении на него бремени доказывания получения вышеуказанного согласия от субъекта персональных данных.

Как отмечает ряд исследователей, данная правовая норма в значительной степени была сформулирована с учетом положений европейского законодательства по аналогичным вопросам. В качестве примеров приводятся: [Директива](#) Европейского Парламента и Совета Европейского Союза N 95/46/ЕС от 24 октября 1995 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, [Директива](#) Европейского Парламента и Совета Европейского Союза N 2002/58/ЕС от 12 июля 2002 г. в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи)*⁽⁵⁹⁾.

По нашему мнению, комментируемую статью можно считать примером удачного заимствования положений европейского права с целью совершенствования российского законодательства.

В рамках исследования зарубежного законодательства по заявленной тематике большой интерес представляют положения Директивы ЕС о защите физических лиц при обработке персональных данных. В [пп. 35, 37](#) преамбулы указанного документа определены случаи, когда обработка персональных данных со стороны государственных органов допускается без согласия субъекта персональных данных. Согласие не требуется при соблюдении определенных условий, связанных с целью обработки персональных данных:

обработка персональных данных необходима в целях предотвращения, расследования, выявления преступлений или исполнения уголовных наказаний, включая защиту от угроз общественной безопасности и предотвращение таких угроз;

указанные выше виды деятельности должны охватывать защиту жизненно важных интересов субъекта персональных данных.

Также введена категория особо конфиденциальных персональных данных, под которыми понимаются персональные данные, в силу своей специфики представляющие собой информацию, имеющую особое значение для защиты прав и свобод субъекта персональных данных.

Полный перечень таких данных в рассматриваемом документе отсутствует, но в качестве примера приведены персональные данные, касающиеся расовой и этнической принадлежности. Для их обработки введены дополнительные ограничения. Даже в случае получения согласия на обработку таких данных от лица, которого они касаются, это не должно являться самостоятельным основанием для подобных действий со стороны государственных органов, подразумевающим безусловное оправдание их совершения. Отмечается необходимость определения на уровне национального законодательства правовых гарантий законности обработки упомянутых персональных данных. Перечень таких гарантий является открытым, но некоторые из них фигурируют в рассматриваемом документе:

законодательное закрепление возможности сбора указанных данных исключительно в контексте определенной информации;

более строгие правила доступа к таким данным;

прямой запрет на передачу подобных данных третьим лицам.

При отсутствии законодательного урегулирования рассматриваемого вопроса на национальном уровне допускается обработка персональных данных, обладающих особой конфиденциальностью, если:

обработка касается персональных данных, публично раскрытых субъектом персональных данных;

обработка персональных данных необходима для защиты жизненно важных интересов физического лица.

Значительной актуальностью в европейском законодательстве также обладает [Регламент](#) ЕС о защите персональных данных. В данном документе изложены основные положения, касающиеся порядка получения согласия на обработку персональных данных. Отмечено, что согласие должно быть дано в виде четкого утвердительного действия. Не является таковым молчание, заранее проставленный знак, иное бездействие субъекта персональных данных. Запрещается ставить оказание услуг, либо выполнение работ, либо обеспечение доступа к иным подобным благам в зависимость исключительно от факта предоставления согласия на обработку персональных данных, если это возможно и без такого согласия. Бремя доказывания получения указанного согласия, равно как и доказывания факта его добровольности, возлагается на оператора. Отмечается, что согласие не требуется в случае защиты общественного интереса.

2. Российские суды, определяя информацию, подлежащую защите как относящуюся к персональным данным, нередко проявляют в своей практике большую жесткость, нежели Роскомнадзор.

Последний занял позицию, что номера телефонов, безотносительно к иной информации о субъекте персональных данных, не могут считаться персональными данными, поэтому допустимо их использование в рекламных и социологических целях без согласия владельцев, что следует из разъяснений ведомства, опубликованных на его сайте^{*(60)}. Однако некоторые суды исходят из диаметрально противоположной точки зрения.

Пример: апелляционным определением Нижегородского областного суда от 11 октября 2016 г. по делу N 33-12355/2016 отказано в удовлетворении апелляционной жалобы АО "ФОРУС Банк" на решение Арзамасского городского суда Нижегородской области от 14 июня 2016 г. по делу N 33-12355/2016, которым было удовлетворено исковое заявление А. к АО "ФОРУС Банк", содержащее требование обязать ответчика удалить персональные данные истца и компенсировать моральный вред в связи с их неправомерным использованием.

Истец, будучи адвокатом и представителем одного из должников ответчика, позвонил последнему со своего номера телефона, после чего на этот номер стали поступать регулярные звонки от банка с требованием погасить задолженность. Суды посчитали, что использование одного лишь телефонного номера истца, без какой-либо иной информации о нем, можно считать обработкой персональных данных, которая возможна только с его согласия. Кроме того, суды отметили, что факт расположения данного номера в сети Интернет на рекламном сайте истца не означает, что номер телефона относится к общедоступным персональным данным, которые можно обрабатывать без согласия их субъекта, поскольку они были размещены для конкретной цели и, как следствие, могли использоваться свободным образом только в соответствии с ней - обращение за юридическими услугами к истцу.

Полагаем, что в указанном вопросе позицию судов следует считать более последовательной, нежели мнение ведомства. Примечательно, что Роскомнадзор в схожем случае, когда о субъекте персональных данных был известен не номер его телефона, а только лишь имя, занял точку зрения, в соответствии с которой подобная информация относится к персональным данным, использование которых возможно только с согласия их субъекта, что находило поддержку в судах.

Пример: постановлением Тамбовского областного суда от 4 октября 2016 г. по делу N 4А-288/2016 отказано в удовлетворении жалобы ООО "ТГЮК" об отмене постановления мирового судьи судебного участка N 1 Октябрьского района г. Тамбова от 15 июня 2016 г. и решения судьи Октябрьского районного суда г. Тамбова от 22 августа 2016 г. по делу о привлечении к административной ответственности ООО "ТГЮК" по [ст. 13.11 КоАП](#) за нарушение законодательства в области персональных данных.

Суды согласились с позицией прокурора, сформированной на основании докладной записки из Управления Роскомнадзора Тамбовской области, о том, что использование ООО "ТГЮК" на своем сайте типовой формы для обратной связи, содержащей графы "Ваше имя", "Тема сообщения", "Сообщение", предполагает, что последний является оператором, поэтому имеет право производить их обработку только с согласия субъектов персональных данных и при условии размещения на своем сайте документа, определяющего политику в отношении обработки персональных данных и сведения о реализуемых требованиях к их защите, что не было сделано в рассматриваемом случае.

Необходимо отметить, что многие суды исходят из того, что согласие субъекта персональных данных на их использование в рекламных и агитационных целях не требуется, когда данные являются общедоступными в силу их размещения в свободном виде владельцами аккаунтов или сайтов в сети Интернет, выступающих в качестве субъектов персональных данных. Указанная позиция подтверждается рядом судебных актов^{*(61)} и в значительной степени тождественна вышеприведенным положениям законодательства ЕС. При этом, как было указано выше, может иметь значение цель публичного размещения персональных данных.

3. Важно обеспечить правильную форму выражения согласия субъекта персональных данных на их обработку. Это актуально в том числе для случаев, когда подобные действия осуществляются через сеть Интернет. Роскомнадзор 8 ноября 2017 г. опубликовал на своем официальном сайте разъяснения, в соответствии с которыми допускается получение согласия посредством проставления соответствующего "клика" на сайте. Исключения, предполагающие получение обязательного письменного согласия, составляют:

биометрические персональные данные;

специальные персональные данные;

персональные данные, передаваемые на территорию государства, которое не обеспечивает их надлежащую защиту.

Роскомнадзор также указал на необходимость размещения на подобных сайтах политики обработки персональных данных и локализацию персональных данных российских пользователей на территории РФ^{*(62)}.

Судебная практика зачастую также исходит из возможности упрощенного получения согласия субъекта персональных данных на их обработку посредством проставления отметки в соответствующей графе. При этом в типовых договорах это обязательно должен быть отдельный раздел (см. [апелляционное определение](#) Самарского областного суда от 17 мая 2016 г. по делу N 33-5757/2016).

4. **Часть 2** комментируемой статьи закрепляет обязанность оператора немедленно прекращать по требованию субъекта персональных данных их обработку. По нашему мнению, термин "немедленно" является слишком неточным и допускает произвольное толкование. Гипотетически его использование в рассматриваемом случае способно привести к нарушению разумного и справедливого баланса интересов участников правоотношений. В этой связи нельзя исключать, что более верным решением представляется закрепление на законодательном уровне точного срока прекращения обработки персональных данных со стороны оператора (например, в течение 12 часов с момента получения подобного запроса).

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

1. Комментируемая **статья** посвящена правам субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных в случаях, предусмотренных законом.

Здесь следует сказать, что обработка персональных данных в принципе может быть автоматизированной и неавтоматизированной. Неавтоматизированная осуществляется в соответствии с [постановлением](#) Правительства от 15 сентября 2008 г. N 687 г. "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

Обработка данных считается 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. При этом 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.

Как отмечается в специализированной литературе, оператор также может совершить ошибку, неправильно трактуя данные пункты. Дело в том, что почти во всех операциях по обработке персональных данных участвует человек, но это не значит, что обработка неавтоматизированная. Сохранение информации на компьютере в виде файла уже делает обработку информации автоматизированной. Примером неавтоматизированной обработки может стать выдача бумажного одноразового пропуска на территорию организации*(63).

Таким образом, исключительно автоматизированной обработка персональных данных будет считаться, если не предполагает непосредственного участия человека.

Некоторые специалисты обращают внимание на особенность толкования комментируемой нормы в аспекте ее буквального восприятия. В частности, отмечается, что зачастую при рассмотрении фразы "принятие решений на основании исключительно автоматизированной обработки" правоприменители неверно переставляют акцент. В процитированной фразе внимание переключается с "исключительно" автоматизированной обработки на исключительно "автоматизированную" обработку. Юридическая конструкция, которая предполагает ограничение исключительности, но не запрет, ориентирует нас на обдуманное принятие решения, порождающего юридические последствия, на основе автоматизированной обработки, то есть без участия человека. При смещении акцента в сторону автоматизированной обработки все дальнейшие вопросы рассматриваются в контексте, что есть автоматизированная и что есть ручная обработка*(64).

В рамках **ч. 1** рассматриваемой статьи предусмотрено общее правило, а именно запрет на принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

Проблема применения исключительно автоматизированной обработки персональных данных является достаточно острой.

Пример: как следует из материалов дела о признании незаконными действий, обязании предоставить сведения, возмещении убытков, компенсации морального вреда, судебных расходов, истица ссылаясь на то, что на ее личный телефон было получено SMS-сообщение рекламного характера. Она не является клиентом банка, не предоставляла согласие на обработку своих персональных данных, и считает, что банк навязывает услуги по кредитованию против ее воли. Поскольку истец не давала согласие на получение рекламы по телефону, следовательно, направление

SMS-сообщения является незаконным, ущемляющим права истца, в связи с чем исковые требования являются законными и обоснованными.

Вместе с тем суд первой инстанции посчитал, что номер SIM-карты истца не является персональными данными и истцом не доказан факт незаконной обработки персональных данных. Однако, по мнению суда апелляционной инстанции, данная позиция не согласуется с [ч. 1](#) комментируемой статьи. Таким образом, судом апелляционной инстанции требование было удовлетворено частично, поскольку установлен факт распространения ненадлежащей рекламы (см. [апелляционное определение](#) Новосибирского областного суда от 7 апреля 2015 г. по делу N 33-2831/2015).

2. Исключениям из правила, установленного [ч. 1](#) комментируемой статьи, посвящена ее [ч. 2](#). В частности, решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных:

при наличии согласия в письменной форме субъекта персональных данных (о согласии субъекта персональных данных на обработку его персональных данных см. [комментарий](#) к ст. 9).

А.И. Савельевым сделано справедливое замечание, что согласие субъекта должно сопровождаться разъяснениями оператора относительно порядка принятия соответствующего решения и возможных юридических последствий такого решения. Очевидно, что данное требование не предполагает предоставления субъекту детальных сведений об алгоритме принятия решения и используемых программных средствах, поскольку они представляют собой интеллектуальную собственность оператора (правовой статус такой собственности может зависеть от политики оператора, например, она может охраняться как программа для ЭВМ и (или) ноу-хау). Однако субъекту должны быть предоставлены для ознакомления персональные данные, которые обрабатываются при принятии им решения, и их источник, например, использование сведений о субъекте, доступных в социальных сетях. Без указанных сведений вряд ли можно говорить о возможности принятия информированного решения*(65);

в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

Вопросам автоматизированного процесса принятия решения в конкретном случае посвящены отдельные положения Регламента ЕС о защите физических лиц при обработке персональных данных, согласно [ст. 22](#) которого субъект данных должен иметь право не подпадать под действие решения, основанного исключительно на автоматической обработке, которое порождает юридические последствия в отношении него или нее или существенно воздействует на него или на нее.

Вместе с тем данное правило не должно применяться, если:

решение необходимо для заключения или исполнения договора между субъектом данных и контролером данных;

решение допускается законодательством Союза или государства-члена ЕС, под действие которого подпадает контролер и которое также устанавливает приемлемые меры защиты прав, свобод и законных интересов субъекта данных;

решение основывается на прямом согласии субъекта данных.

3. [Часть 3](#) комментируемой статьи представляется логически верным завершением положений [ч. 2](#), предусматривая следующие обязанности оператора:

разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения;

предоставить возможность заявить возражение против такого решения;

разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

Обращаем внимание на то, что законодателем не установлены требования к согласию субъекта персональных данных, предусматривающему возможность принятия в результате автоматической обработки данных решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающего его права и законные интересы, а также к порядку разъяснения прав субъектов персональных данных. На наш взгляд, данные требования должны быть разработаны Роскомнадзором. В настоящее время форма данного согласия и требования к порядку разъяснения устанавливаются оператором самостоятельно в рамках локальных актов.

Как правило, в положениях об обработке персональных данных, разрабатываемых операторами, предусматривается, что оператор обязан устно, а по письменному требованию субъекта персональных данных - письменно разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против

такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

При этом текст устного разъяснения оператор составляет в письменном виде до начала автоматизированной обработки персональных данных, а в случаях автоматизированной обработки различными способами разъяснение подготавливается отдельно для каждого способа.

Возражение субъекта персональных данных на принятое на основании исключительно автоматизированной обработки персональных данных решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, должно содержать указание на принятое оператором решение, а также указание на нарушение прав и законных интересов субъекта персональных данных. В связи с этим к возражению должны быть приложены подтверждающие это документы.

4. **Часть 4** рассматриваемой статьи обязывает оператора рассмотреть возражение субъекта персональных данных на принятое на основании исключительно автоматизированной обработки персональных данных решение в течение 30 дней со дня его получения, и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

Вместе с тем форма уведомления законодателем не уточнена. Уведомление может быть как в устной, так и в письменной форме. Как правило, операторы письменно уведомляют субъектов персональных данных.

Статья 17. Право на обжалование действий или бездействия оператора

1. В настоящее время - в эпоху повсеместной цифровизации - положение **п. 6 преамбулы** Регламента ЕС о защите персональных данных, обращающее внимание на появление новых проблем, связанных с защитой персональных данных ввиду увеличения масштаба сбора персональных данных и обмена ими, выражает остроту проблематики применения инструментов по защите персональных данных.

В **Директиве** ЕС о защите физических лиц при обработке персональных данных компетентными органами предусматривается необходимость установления ответственности и обязательств контролера в отношении любой обработки персональных данных, осуществляемой контролером или от его имени. Риски для прав и свобод физических лиц, разной степени вероятности и серьезности, могут возникать в результате обработки персональных данных, которая может привести к физическому, материальному или нематериальному ущербу.

Комментируемой **статьей** российским законодательством декларируется право субъекта персональных данных обжаловать действия или бездействие оператора как в уполномоченный орган по защите прав субъектов персональных данных, так и в судебном порядке.

В нашей стране уполномоченным надзорным органом выступает Роскомнадзор, так как именно он является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

Тем самым комментируемое положение соответствует требованиям **ст. 33, 46** Конституции, провозгласившим гарантии права на обращения в государственные органы и судебной защиты прав и свобод каждого.

Также оно соотносится с нормами европейского права, закрепившими правило о том, что каждый человек имеет право на защиту относящихся к нему персональных данных (**ст. 8** Хартии ЕС об основных правах от 12 декабря 2007 г. и **ст. 16** Договора о функционировании Европейского Союза от 25 марта 1957 г.). Реализация данного права человека осуществляется в том числе в рамках **Регламента** ЕС о защите персональных данных и **Директивы** ЕС о защите физических лиц при обработке персональных данных.

Защита субъективных прав в рамках российского законодательства может осуществляться посредством самозащиты, административной защиты, а также судебной (процессуальной) защиты.

Право на защиту является сопутствующим любому субъективному праву человека. **Конституция** провозглашает право каждого человека защищать принадлежащие ему субъективные гражданские права. В данном случае верными представляются выводы А.И. Базилевича о том, что право на защиту является самостоятельным субъективным гражданским правом, установленным Конституцией, **ГК**, иными федеральными законами и международно-правовыми актами, и существует объективно, то есть независимо от того, нуждается в нем носитель этого права в данный конкретный момент или нет, а защита субъективных гражданских прав и охраняемых законом интересов осуществляется посредством применения всей совокупности элементов защиты в установленном законом порядке, то есть посредством применения надлежащей формы, средств и способов защиты***(66)**

В.М. Жуйков в своем диссертационном исследовании дал характеристику права на судебную защиту как не подлежащего ограничениям конституционного права каждого заинтересованного лица на беспрепятственное обращение за защитой своих прав, свобод или охраняемых законом интересов на рассмотрение его дела в разумный срок беспристрастным и независимым судом, а также и на исполнение судебного акта^{*(67)}.

Между тем заслуживающая внимания оговорка содержится в [п. 4 преамбулы](#) Регламента ЕС о защите персональных данных, она предусматривает необходимость соотнесения права на судебную защиту с иными субъективными гражданскими правами. Так, право на защиту персональных данных не является абсолютным правом; его необходимо рассматривать относительно его функции в обществе, оно должно быть уравнено с другими основными правами в соответствии с принципом пропорциональности. Регламент соблюдает все основные права, свободы и принципы, признанные в ЕС, в частности уважение частной и семейной жизни, жилища и переписки, защиту персональных данных, свободу мысли, совести и вероисповедания, свободу выражения мнения и распространения информации, право ведения хозяйственной деятельности, право на эффективное средство правовой защиты и на справедливое судебное разбирательство, культурное, религиозное и языковое разнообразие.

В соответствии со [ст. 51](#) Регламента ЕС о защите персональных данных каждое государство-член ЕС должно предусмотреть один или несколько независимых органов государственной власти, ответственных за мониторинг применения Регламента, для защиты основных прав и свобод физических лиц при обработке данных и для содействия свободному движению персональных данных в ЕС ("надзорный орган").

В России, как уже отмечалось, уполномоченным органом по защите прав субъектов персональных данных является Роскомнадзор.

Важно учитывать, что сбор, обработка, передача, распространение персональных данных возможны только с согласия субъекта персональных данных, при этом согласие должно быть конкретным. Под персональными данными понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу.

Субъект персональных данных должен воспользоваться правом, декларируемым настоящей статьей, только в случае, если обработка персональных данных действительно нарушает его права.

В [п. 142 преамбулы](#) Регламента ЕС о защите персональных данных также уточняется, что в случае, если субъект данных считает, что его права согласно указанному Регламенту нарушены, он вправе передать некоммерческому органу, организации или объединению, которые были основаны в соответствии с законодательством государства-члена ЕС, имеют уставные задачи в сфере общественного интереса, а также осуществляют деятельность в области защиты персональных данных, право подавать в надзорный орган жалобу от его имени, осуществлять права на судебную защиту от имени субъектов данных или в случаях, предусмотренных законодательством государства-члена ЕС, осуществлять право на получение компенсации от его имени субъектов данных.

Отметим, что на практике реализация декларируемого настоящей статьей права обжалования действий или бездействия оператора нередко приводит к безосновательному заявлению субъектом персональных данных требований. Зачастую такие споры возникают в рамках трудовых правоотношений.

Пример 1: в ходе рассмотрения требования о признании незаконными действий по распространению персональных данных суд, отказывая в удовлетворении исковых требований, подчеркнул, что обработка данных истца, содержащихся в ее заявлениях на отпуск, осуществлялась ответчиком и его представителем в соответствии с положениями [пп. 3, 7 ч. 1 ст. 6](#) комментируемого закона, а именно в связи с участием А. в гражданском судопроизводстве, а также для осуществления оператором - работодателем АО "Мерседес-Бенц РУС" судебной защиты, поскольку согласие субъекта персональных данных на обработку его персональных данных в данном случае не требовалось; хранение работодателем копий заявлений истца на отпуск за период с 2012-2014 гг. не является нарушением норм действующего законодательства, а также в связи с продолжением трудовых отношений сторон. Доказательств, свидетельствующих о наличии в действиях работодателя нарушений действующего законодательства, ущемляющих законные права истца, в материалы дела не представлено (см. [определение](#) Первого кассационного суда общей юрисдикции от 13 июля 2020 г. по делу N 88-16257/2020).

Пример 2: из материалов дела о защите прав субъекта персональных данных, возмещении морального вреда следует, что истцы указали на то, что состояли в трудовых отношениях с ответчиком. Позже им стало известно, что их персональные данные без их согласия содержатся в проектах производства геодезических работ, при этом персональные данные были предоставлены руководству с коммерческой целью.

В удовлетворении требования судом было отказано, поскольку судом было установлено, что в соответствии с трудовыми договорами, заключенными между ответчиком и истцами, последние выразили свое согласие на осуществление работодателем обработки, сбора, систематизации, накопления, хранения, уточнения, использования, распространения (в том числе передачи), обезличивания, блокировки, уничтожения, а также передачи работодателем по своему усмотрению персональных данных и соответствующих документов, содержащих персональные данные, третьим лицам (см. [апелляционное определение](#) Московского городского суда от 26 августа 2019 г. по делу N 33-38193/2019).

Субъект персональных данных в соответствии с комментируемой [статьей](#) определяет, в каком порядке будет требовать защиты своего нарушенного права - в административном или же судебном.

По нашему мнению, целесообразно использовать административный ресурс, поскольку Роскомнадзор является специализирующимся на данных делах органом.

Справка: согласно Отчету об итогах работы с обращениями граждан в Роскомнадзоре в I квартале 2020 года в I квартале 2020 года в Центральный аппарат Роскомнадзора поступило 1838 обращений, касающихся вопросов защиты персональных данных*(68).

По мнению некоторых специалистов, право подачи жалобы в судебном порядке следует вообще рассматривать как дополнительное (если не работает основное право - обращение в Роскомнадзор)*(69). Действительно, инструментарий, которым обладает Роскомнадзор, позволяет ему всесторонне рассматривать жалобы в области защиты персональных данных.

В соответствии с [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](#) Минкомсвязи от 14 ноября 2011 г. N 312, должностные лица Роскомнадзора ее территориального органа при проведении проверок в рамках рассмотрения обращений граждан вправе в пределах своей компетенции:

выдавать обязательные для выполнения предписания об устранении выявленных нарушений в области персональных данных;

составлять протоколы об административном правонарушении или направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении дел об административных правонарушениях, а также о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных;

использовать технику и оборудование, принадлежащие Роскомнадзору или его территориальному органу;

запрашивать и получать необходимые документы (сведения) для достижения целей проведения проверки;

получать доступ к информационным системам персональных данных в режиме просмотра и выборки необходимой информации;

направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном порядке, если условием лицензии на осуществление такой деятельности предусмотрен запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушениями требований законодательства Российской Федерации в области персональных данных;

требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

привлекать экспертов и экспертные организации при проведении контрольно-надзорных мероприятий, а также для анализа полученных материалов.

Справка: согласно итогам работы Роскомнадзора за 2019 год, наблюдается резкий рост активности граждан в части реализации ими законодательно закрепленных прав в сфере защиты персональных данных.

В 2019 году доля поступивших обращений граждан, содержащих жалобы в сфере защиты персональных данных, в общем объеме обращений занимает первое место (52 375 шт. или 35%), однако впервые с момента реализации Роскомнадзором функций регулятора в сфере защиты персональных данных, годовое количество поданных жалоб в сфере защиты персональных данных превысило

количество поданных жалоб в сфере связи (24%).

Подавляющее количество жалоб, поступивших от граждан, традиционно касалось защиты персональных данных в связи с их размещением в сети Интернет, организацией деятельности банков и передачей персональных данных граждан коллекторским агентствам.

В частности, в отношении кредитных организаций распространены жалобы на передачу персональных данных без согласия граждан, а в отношении коллекторских агентств - на обработку персональных данных граждан без их согласия. Предмет жалоб на действия владельцев интернет-сайтов, как правило, связан с предоставлением доступа неограниченного числа лиц к персональным данным гражданина^{*(70)}.

По мнению Роскомнадзора, в целом увеличение количества обращений по данной тематике обусловлено, прежде всего, повышением уровня правовой культуры граждан и предоставлением государственными органами дополнительных возможностей для защиты своих прав. В части обеспечения информационной безопасности личности вопросы защиты персональных данных являются неотъемлемым элементом системы работы Роскомнадзора по контролю за деятельностью в сети. Со вступлением в 2019 году в силу новых законодательных норм активизирована судебная претензионная деятельность, расширены формы и методы профилактической работы.

Обращаем внимание на то, что при подаче жалобы (искового заявления в суд) на осуществление оператором обработки персональных данных с нарушением установленных требований заявитель (истец) должен приложить документы, подтверждающие нарушение установленных требований, а также документы, подтверждающие нарушение его прав и законных интересов. При непредставлении указанных документов заявителю (истцу) в удовлетворении его требований будет отказано.

Пример: согласно материалам дела о признании незаконными действий по обработке персональных данных и передаче их третьим лицам истица указала, что заключила договор о техническом обслуживании и ремонте внутридомового (внутриквартирного) газового оборудования. Условиями договора было предусмотрено ее согласие на автоматизированную обработку персональных данных и передачу их третьим лицам, на что она согласна не была, договор подписала вынужденно, на других условиях ответчик отказался поставлять газовое отопление. В удовлетворении требования было отказано, поскольку доказательств того, что стороне истца было отказано ответчиком в отзыве согласия на обработку персональных данных, в материалы дела не представлено. Таким образом, истцом в нарушение требований [ст. 56](#) ГПК не было представлено доказательств нарушения своих прав (см. [определение](#) Второго кассационного суда общей юрисдикции от 19 мая 2020 г. по делу N 88-10275/2020).

2. В соответствии с [ч. 2](#) рассматриваемой статьи субъект персональных данных имеет право на защиту своих прав и законных интересов. Кроме того, комментируемая статья предусматривает возможность субъекта персональных данных требовать возмещения убытков и (или) компенсации морального вреда в судебном порядке.

Пример: в рамках рассмотрения дела о признании договоров недействительными, применении последствий недействительности, признании незаконными действий, обязанности прекратить передачу персональных данных, обязанности внести исправления в кредитную историю, взыскании компенсации морального вреда истец ссылался на то, что он получил уведомление, что является должником по договорам займа, однако данные договоры он не заключал.

Удовлетворяя искивые требования частично, суд исходил из того, что ответчиками не представлены доказательства, подтверждающие факт обращения истца за получением займа (кредита), заключения с ним договора потребительского займа и выдаче истцу денежных средств в качестве займа. В связи с этим суд пришел к выводу о признании договоров займа недействительными. Кроме того, с учетом того, что истец организациям не давал разрешение на обработку своих персональных данных, суд удовлетворил искивые требования в части признания незаконными персональных данных истца, при этом обязал ответчиков прекратить передачу персональных данных истца третьим лицам, прекратить обработку персональных данных и уничтожить персональные данные (см. [определение](#) Второго кассационного суда общей юрисдикции от 11 февраля 2020 г. по делу N 88-2320/2020).

Согласно [ст. 24](#) настоящего федерального закона лица, виновные в нарушении требований комментируемого закона, несут предусмотренную законодательством Российской Федерации ответственность. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, установленных в соответствии с настоящим федеральным законом, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Таким образом, по правилам [ст. 151](#) ГК, если гражданину причинен моральный вред

(физические или нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину нематериальные блага, а также в других случаях, предусмотренных законом, суд может возложить на оператора обязанность денежной компенсации указанного вреда.

Вместе с тем при определении размеров компенсации морального вреда суд принимает во внимание степень вины нарушителя и иные заслуживающие внимания обстоятельства. Суд должен также учитывать степень физических и нравственных страданий, связанных с индивидуальными особенностями гражданина, которому причинен вред.

На субъекта персональных данных при подаче искового заявления в суд возлагается обязанность представить допустимые доказательства причинения ему действиями ответчика нравственных и физических страданий и наличия причинно-следственной связи между действиями ответчика и последствиями нарушения личных неимущественных прав истца. В противном случае ему будет отказано в компенсации морального вреда.

Пример: при заявлении требований в суд Х. указал, что на его телефон стали поступать автозвонки. В данных звонках утверждалось, что он является должником и обязан погасить долг. Вместе с тем, по заявлению истца, с ответчиком договоры займа он не заключал, его клиентом не является. Принимая во внимание, что в судебном заседании нашел подтверждение факт нарушения ответчиком прав гражданина Х. как субъекта персональных данных, учитывая все заслуживающие внимания обстоятельства, а именно характер и степень нравственных страданий, причиненных истцу нарушением его прав, требования разумности и справедливости, судебная коллегия посчитала правомерным взыскать с ответчика в пользу истца компенсацию морального вреда (см. апелляционное определение Московского городского суда от 16 октября 2018 г.).

Следует учитывать, что ответственность за причинение морального вреда возлагается на лицо, причинившее такой вред. Вместе с тем, важно помнить, что доказать отсутствие вины в причинении вреда обязан причинитель вреда (п. 4 Обзора судебной практики Верховного Суда РФ N 4 (2016), утв. президиумом Верховного Суда РФ 20 декабря 2016 г.), хотя и на субъекте персональных данных лежит обязанность представить доказательства причинения ему морального вреда.

Глава 4. Обязанности оператора

Статья 18. Обязанности оператора при сборе персональных данных

1. Комментируемая статья определяет базовые обязанности оператора персональных данных перед субъектом персональных данных: уведомить о сборе персональных данных и разъяснить последствия отказа в предоставлении персональных данных. Помимо того, в ч. 5 комментируемой статьи закреплена публично-правовая обязанность оператора персональных данных обеспечить территориальную локализацию обрабатываемых персональных данных. Дополнительные обязательства операторов персональных данных и обеспечивающие выполнение обязанностей меры закреплены в последующих статьях главы 4 "Обязанности оператора" комментируемого закона. Следует отметить, что, хотя обязанности операторов персональных данных и корреспондируют с правами субъектов персональных данных (см. комментарий к ст. 14), их объем не идентичен.

Например, согласно ч. 1 комментируемой статьи при сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную ч. 7 ст. 14 комментируемого закона. Под сбором персональных данных следует понимать целенаправленный процесс получения персональных данных оператором непосредственно от субъекта персональных данных либо через специально привлеченных для этого третьих лиц.

Не являются сбором персональных данных:

случаи, когда персональные данные получены оператором в результате случайного (незапрошенного) попадания к нему персональных данных, например, вследствие получения писем по электронной или иной почте, в которых содержатся персональные данные;

случаи, когда одна организация-оператор получает от другой персональные данные, которые представляют собой контактную информацию работников или представителей такой организации, переданную в ходе осуществления ими своей законной деятельности.

Согласно ч. 7 ст. 14 комментируемого закона оператор не обязан априорно предоставлять субъекту персональных данных информацию о возможности и способах обжалования решения об обработке его персональных данных. Полагаем, в данном случае следует учитывать положения ч. 1 ст. 13 Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами, согласно которым оператор обязан ознакомить субъекта персональных данных, в том числе с контактными данными инспектора (работника или сотрудника оператора) по защите персональных

данных, а также разъяснить ему право на подачу жалобы в надзорный орган и контактные данные надзорного органа. Инкорпорация подобной нормы в отечественное законодательство, как нам представляется, повысит степень защищенности субъекта персональных данных от произвольного и необоснованного оборота его персональных данных.

Использованная законодателем формулировка "по его просьбе" вряд ли может быть признана удачной. С лексической точки зрения подобная лексема характеризует субъекта персональных данных, как находящегося в слабой позиции "просителя", а с юридической не позволяет однозначно соотнести между собой право субъекта персональных данных "на получение сведений" в результате обращения либо запроса и обязанность оператора предоставить сведения "по просьбе". Например, учитывая определенные в [ч. 3 ст. 14](#) условия и процедуру удовлетворения обращения (запроса) субъекта персональных данных оператором персональных данных, неясно, должна ли "просьба" иметь письменный вид и содержать перечисленные в указанной норме реквизиты. Отсутствие нормативных разъяснений приводит к выводу о допустимости любой формы "просьбы" субъекта персональных данных и ответа оператора персональных данных - она может быть как устной, так и письменной, оформленной на бумажном носителе или в электронном сообщении.

Вместе с тем применительно к устному ответу оператора на обращение, запрос или "просьбу" субъекта персональных данных целесообразно установить условия, аналогичные тем, что закреплены в [ч. 1 ст. 12](#) Регламента ЕС о защите персональных данных: "По просьбе субъекта данных информация может быть предоставлена в устной форме, при условии, что личность субъекта данных установлена иным способом". Подобная формулировка обеспечивает защиту субъекта персональных данных от манипулирования оператором возможностью устного информирования.

Также следует обратить внимание, что оператор персональных данных обязан удовлетворить просьбу субъекта на первичной стадии - стадии сбора его персональных данных. В этом контексте, например, излишним представляется предоставление сведений, указанных в [п. 1](#) (подтверждение факта обработки персональных данных оператором) и [п. 5](#) (обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения) [ч. 7 ст. 14](#) комментируемого закона. Полагаем, удовлетворение просьбы субъекта о предоставлении указанных сведений на стадии сбора персональных данных является отдельной обязанностью, которая не ограничивает субъекта персональных данных в реализации права на обращение или запрос сведений.

Концептуально схожую позицию в определении объема обязанностей оператора персональных данных демонстрирует европейский законодатель. Так, согласно [п. 56 преамбулы](#) Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами контролер или обрабатывающее данные лицо должны вести учет всех категорий операций по обработке персональных данных в сфере их ответственности. Каждый контролер и обрабатывающее данные лицо должны сотрудничать с надзорными органами и представлять им указанные документы по запросу, чтобы они могли использоваться для мониторинга таких операций по обработке. Контролер или обрабатывающее данные лицо, которые обрабатывают персональные данные в неавтоматизированных системах обработки, должны иметь в наличии эффективные методы подтверждения законности обработки, обеспечения самоконтроля, а также целостности и защиты данных, в частности, журналы регистрации и иные формы ведения учета.

2. [Часть 2](#) комментируемой статьи определяет, что если предоставление персональных данных является обязательным в соответствии с федеральным законом, то оператор обязан разъяснить субъекту юридические последствия отказа предоставить его персональные данные. Использованная формулировка "юридические последствия отказа" также имеет неоднозначную интерпретацию. Одни специалисты в области оборота персональных данных связывают ее с применением к отказавшемуся предоставить персональные данные субъекту мер уголовной и административной ответственности*[\(71\)](#), другие же связывают последствия отказа с невозможностью субъекта воспользоваться отдельными специальными правами*[\(72\)](#). Полагаем, оба подхода справедливы и приемлемы. С одной стороны, идентификация личности обязательна для реализации, например, большинства видов деятельности, за которыми установлен государственный (муниципальный) надзор (управление транспортным средством, выезд за пределы РФ, приобретение большим наркотических средств и т.д.), с другой же стороны отказ в предоставлении сведений образует состав ряда административных правонарушений и преступлений, таких как [ст. 6.29](#) "Невыполнение обязанностей о представлении информации о конфликте интересов при осуществлении медицинской деятельности и фармацевтической деятельности" и [ст. 19.7](#) "Непредставление сведений (информации)" КоАП или [ст. 308](#) "Отказ свидетеля или потерпевшего от дачи показаний" УК.

Полагаем, есть и третья разновидность юридических последствий отказа субъекта от представления персональных данных - это обработка указанных в [п. 10 ч. 1 ст. 6](#) и [п. 2 ч. 2 ст. 10](#) комментируемого закона данных вопреки воле субъекта персональных данных.

3. **Части 3 и 4** комментируемой статьи регламентируют порядок действий оператора, которым получены персональные данные не от субъекта этих данных. По общему правилу (ч. 3) оператору в таком случае предписывается до начала обработки персональных данных уведомить о ней субъекта персональных данных, сообщив при этом:

- наименование либо фамилию, имя, отчество и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемых пользователей персональных данных;
- установленные комментируемым законом права субъекта персональных данных;
- источник получения персональных данных.

Исключения из этого общего правила предусмотрены **ч. 4** комментируемой статьи. Оператор освобождается от обязанности предоставить субъекту персональных данных указанные выше сведения в случаях, если:

1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором (см. **комментарий** к ст. 22).

2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных (см. **комментарий** к ст. 6).

3) обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных **ст. 10.1** настоящего федерального закона (см. **комментарий** к ст. 10.1).

4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных (см. **комментарий** к ст. 6).

Законодательным пробелом следует признать отсутствие среди оснований освобождения оператора персональных данных от обязанности предоставить субъекту персональных данных сведения иных критериев, которые перечислены в **п. 1.2** комментария к ст. 6 настоящего федерального закона, при условии, что уведомление субъекта о факте обработки его персональных данных дезорганизует государственно-властную деятельность или создаст угрозу для иного общественного интереса. Примечательно, что подобное положение содержится в **ч. 3 ст. 13** Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами, согласно которой государства-члены ЕС могут принимать законодательные меры, задерживающие, ограничивающие или исключающие предоставление информации субъекту данных в таком объеме и в течение такого срока, пока указанные меры являются необходимыми и соразмерными в демократическом обществе с должным учетом основных прав и законных интересов соответствующего физического лица:

(а) во избежание препятствования направлению официальных или правовых запросов, проведению расследований или процедур;

(б) во избежание ущерба предотвращению, выявлению, расследованию или уголовному преследованию преступлений либо исполнению уголовных наказаний;

(с) в целях защиты общественной безопасности;

(д) в целях защиты национальной безопасности;

(е) в целях защиты прав и свобод иных лиц.

Следует обратить внимание, что в рассмотренной норме Директивы речь идет не об отказе в доступе к сведениям, когда сам факт обработки персональных данных признается секретным (ограниченным в доступе), а об ограничении объема или продлении срока обязательного уведомления. Подобный вывод можно сделать однозначно, так как полное или частичное ограничение права субъекта персональных данных на доступ к данным по тем же основаниям предусмотрено в другой норме - **ч. 1 ст. 15** той же Директивы. **Частью 3** той же статьи предусматривается право оператора не уведомлять субъекта об отказе в доступе к данным.

5) предоставление субъекту персональных данных сведений, предусмотренных **ч. 3** комментируемой статьи, нарушает права и законные интересы третьих лиц (см. **комментарий** к ст. 6).

4. В соответствии с **ч. 5** комментируемой статьи при сборе персональных данных, в том числе посредством Интернет, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ, за исключением случаев, указанных **пп. 2, 3, 4, 8 ч. 1 статьи 6** комментируемого закона.

Во-первых, системообразующим элементом рассматриваемой нормы является гражданство субъекта персональных данных. Согласно **ст. 3** Федерального закона от 31 мая 2002 г. N 62-ФЗ "О гражданстве Российской Федерации" таковым является устойчивая правовая связь лица с РФ,

выражающаяся в совокупности их взаимных прав и обязанностей. Примечательно, что обязанность оператора персональных данных устанавливать гражданство субъекта персональных данных установлена лишь косвенно через рассматриваемую норму. Например, письменное согласие субъекта на обработку персональных данных не должно включать отдельного реквизита "гражданство", о нем можно судить лишь по тому документу, который субъект персональных данных указал в качестве удостоверяющего его личность. В сложившейся ситуации действующим на территории России операторам рекомендуется либо исходить из предположения, что все обрабатываемые ими персональные данные относятся к гражданам РФ, либо предусмотреть механизм установления гражданства субъекта РФ посредством заполнения соответствующего реквизита с последующей верификацией полученных данных (что более трудоемко и дорогостояще).

Во-вторых, заслуживающим особого внимания элементом комментируемой нормы является перечень способов обработки персональных данных граждан России, которые могут осуществляться исключительно на территории РФ. К ним относятся:

1) Запись. Согласно [ГОСТ 13699-91](#) (Межгосударственный стандарт "Запись и воспроизведение информации. Термины и определения", утв. постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 29 марта 1991 г. N 342), под записью (регистрацией, фиксацией) информации следует понимать процесс преобразования сигналов информации в пространственное изменение физических характеристик или формы носителя записи с целью сохранения и последующего воспроизведения записанной информации. При этом носителем информации признается физическое тело, используемое при записи для сохранения в нем или на его поверхности сигналов информации. Данный ГОСТ также содержит примечания, согласно которым носители информации классифицируются в зависимости от системы записи, от формы носителя и в соответствии с системой записи.

2) Систематизация. Согласно ГОСТ 7.74-96 (Межгосударственный стандарт "Система стандартов по информации, библиотечному и издательскому делу. Информационно-поисковые языки. Термины и определения", принятый Межгосударственным Советом по стандартизации, метрологии и сертификации, протокол N 9 от 12 апреля 1996 г.) систематизация представляет собой присвоение данным или документам классификационных индексов в соответствии с правилами какого-либо классификационного информационно-поискового языка. Выделяются документальный (предназначен для индексирования документов (частей документов) с целью последующего хранения и поиска); классификационный (предназначен для индексирования документов (частей документов) и информационных запросов посредством понятий и кодов какой-либо классификационной системы), дескрипторный (предназначен для координатного индексирования документов и информационных запросов посредством дескрипторов и (или) ключевых слов), фактографический (предназначен для индексирования описаний фактов и информационного поиска в фактографических информационных массивах), объектно-признаковый (предназначен для индексирования описаний фактов в виде перечня объектов (предметов) с указанием относящихся к ним признаков (свойств) и соответствующих значений признаков) и вербальный (использует для представления своих лексических единиц слова и выражения естественного языка в их орфографической форме) информационно-поисковые языки, а также язык предметных рубрик (предназначен для индексирования документов (частей документов) и информационных запросов посредством предметных рубрик) и язык ключевых слов (предназначен для индексирования документов и информационных запросов посредством ключевых слов). Систематизация персональных данных, таким образом, представляет собой структурирование этих данных по заранее определенным классификационным признакам с возможностью осуществления поиска и выборки информации на основании поискового запроса посредством использования информационно-поисковых языков.

3) Хранение. Согласно [ГОСТ Р 52292-2004](#) (Национальный стандарт РФ "Информационная технология (ИТ). Электронный обмен информацией. Термины и определения", утв. [приказом](#) Федерального агентства по техническому регулированию и метрологии от 29 декабря 2004 г. N 135-ст) хранение представляет собой процесс поддержания данных в неизменном состоянии после их сохранения, обеспечивающий возможность их последующего считывания в произвольный момент времени.

4) Накопление. Как юридический термин хранение данных нормативно не закреплено. Накопление представляет собой комплексный процесс, включающий сбор и хранение информации в упорядоченном (систематизированном) виде. С определенной степенью допущения можно сказать, что накопление - это состояние информационной системы, при котором объем актуальной систематизированной информации постоянно увеличивается.

5) Уточнение (обновление, изменение). Такие действия представляют собой видоизменение уже накопленных данных в случае, если содержательно они перестали соответствовать объективной

действительности. При невозможности уточнить (обновить, актуализировать) персональные данные доступ к ним подлежит блокированию в соответствии со [ст. 21](#) комментируемого закона.

б) Извлечение. Данное понятие наиболее близко к термину "экспорт", который закреплен в [ГОСТ Р ИСО/МЭК ТО 10032-2007](#) (Национальный стандарт РФ "Эталонная модель управления данными", утв. [приказом](#) Федерального агентства по техническому регулированию и метрологии от 27 декабря 2007 г. N 573-ст). Экспорт данных понимается как услуга по управлению данными, заключающаяся в извлечении данных из базы данных и создании копии этих данных, организованных в соответствии с форматом обмена данными. Иными словами, извлечение представляет собой перенос данных из базы на сторонний носитель, в том числе выборочный, без утраты их оператором базы данных.

В-третьих, следует обратить внимание на исключения из общего правила, обязывающего оператора осуществлять обработку персональных данных граждан РФ в указанных выше формах только на территории страны (см. пп. 1.2.1, 1.2.2, 1.2.4 и 1.2.8 [комментария](#) к ст. 6).

В-четвертых, следует обратить внимание на ст. 15.5 ФЗ "Об информации, информационных технологиях и о защите информации", в которой определен порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства РФ в области персональных данных. Ее положения непосредственно коррелируют с нормами комментируемой статьи. В соответствии с [ч. 1-3](#) данной статьи в целях ограничения неправомерного оборота персональных данных в сети Интернет создается автоматизированная информационная система "Реестр нарушителей прав субъектов персональных данных" (далее - Реестр, <https://pd.rkn.gov.ru>), которая формируется и ведется федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи (Роскомнадзор) в порядке, установленном Правительством РФ.

Согласно [ч. 5](#) данной статьи основанием для включения в Реестр информации является вступивший в законную силу судебный акт. При этом инициатором судебного разбирательства могут быть как государственный орган, выявивший нарушение законодательства о персональных данных в ходе реализации контрольных мероприятий, в том числе мониторинга сети Интернет, так и сами граждане - субъекты персональных данных. Так, [ч. 6](#) данной статьи субъекту персональных данных делегируется право обратиться в Роскомнадзор с заявлением о принятии мер по ограничению доступа к персональным данным, обрабатываемым с нарушением законодательства РФ, на основании вступившего в законную силу судебного акта. В Реестр включаются:

- 1) доменные имена и (или) указатели страниц сайтов в сети Интернет, содержащих информацию, обрабатываемую с нарушением законодательства РФ в области персональных данных;
- 2) сетевые адреса, позволяющие идентифицировать сайты в сети Интернет, содержащие информацию, обрабатываемую с нарушением законодательства РФ в области персональных данных;
- 3) указания на вступившие в законную силу судебные акты;
- 4) информация об устранении нарушения законодательства РФ в области персональных данных;
- 5) дата направления операторам связи данных об информационном ресурсе для ограничения доступа к этому ресурсу.

Надзор за исполнением операторами персональных данных возложенных на них обязанностей осуществляется Роскомнадзором в порядке, определенном [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](#) Минкомсвязи России от 14 ноября 2011 г. N 312. Нарушение же правил оборота персональных данных граждан России влечет административную ответственность по [ч. 8 ст. 13.11](#) КоАП.

Пример: на основании [постановления](#) Второго кассационного суда общей юрисдикции от 7 июля 2020 г. N 16-3770/2020 решение судьи Таганского районного суда г. Москвы от 16 марта 2020 г., вынесенное в отношении Твиттер, Инк. (Twitter, Inc.) по делу об административном правонарушении, предусмотренном [ч. 8 ст. 13.11](#) КоАП, было оставлено без изменения, а жалоба защитника - без удовлетворения. Суд посчитал доказанным тот факт, что 9 января 2020 г. в 09 часов 01 минуту по московскому времени по адресу: 1355 Маркет Стрит, номер 900, Сан Франциско. Калифорния, 94103, (1355 Market Street, suite 900, San Francisco California 94103) Компания Твиттер, Инк. (Twitter, Inc.) осуществляла сбор персональных данных граждан Российской Федерации, на сайте сети Интернет с доменным именем <https://twitter.com>, не обеспечив запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) или извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, чем нарушило [ч. 5 ст. 18](#) комментируемого закона.

Доказательствами по делу выступили: протокол об административном правонарушении; акт изготовления скриншотов; скриншоты страниц сайта <https://twitter.com>, из которых усматривается, что в обязательном порядке для регистрации на указанном интернет-ресурсе необходимо создать учетную запись и указать личную информацию: имя пользователя, адрес электронной почты или номер телефона, изображение, описать биографию; сведения, полученные в результате проверки, проведенной с помощью общедоступного whois-сервиса, о том, что данные российских пользователей социальной сети Twitter обрабатываются с использованием баз данных, находящихся на территории США и ЕС.

Доводы жалобы о том, что Компания не осуществляет свою деятельность на территории РФ, в связи с чем местом совершения инкриминируемого ему административного правонарушения не может быть территория РФ, были проверены судом и признаны не убедительными.

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

1. Комментируемая **статья** предусматривает систему правовых и организационных мер, обеспечивающих исполнение оператором персональных данных установленных законодательством обязанностей.

Согласно **ч. 1** комментируемой статьи оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, оператор персональных данных определяет самостоятельно с учетом норм комментируемого закона и принимаемых на его основе подзаконных нормативных актов, при этом в рассматриваемой норме содержится перечень рекомендуемых мер, которые могут применяться вариативно:

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

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 РФ, устранение последствий таких нарушений. Исследователи законодательства о персональных данных к таковым относят **(73)**:

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;

должностную инструкцию 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;

типовую форму 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 (см. [комментарий](#) к ст. 19);

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. Внутренний контроль и аудит осуществляется на плановой основе локальными нормативными актами оператора и реализуется уполномоченными сотрудниками организации;

5) оценку 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 настоящим федеральным законом;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства 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.

Примечательно, что, предусматривая в [ст. 3](#) комментируемого закона возможность совместной обработки персональных данных несколькими операторами, законодатель не обеспечил подобное взаимодействие действенным механизмом реализации. Как следствие, обозначенные вопросы регулируются на подзаконном уровне. Примером подобного нормативного акта является [приказ](#) Генпрокуратуры N 39, МВД N 1070, МЧС N 1021, Минюста N 253, ФСБ N 780, Минэкономразвития N 353, ФСКН N 399 от 29 декабря 2005 г. "О едином учете преступлений", которым определен в том числе единый для указанных правоохранительных органов порядок организации приема, регистрации и проверки сообщений о преступлениях, порядок регистрации уголовных дел и учета преступлений.

В европейском законодательстве данная сфера урегулирована значительно подробнее. Так, организации совместной обработки персональных данных несколькими операторами посвящена [ст. 21](#) Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами. В соответствии с содержащимися в данной статье нормами контролеры (операторы), осуществляющие совместную обработку персональных данных, должны с соблюдением принципов прозрачности и посредством соглашения определять свои обязанности по выполнению Директивы, в частности в отношении осуществления прав субъекта данных, а также свои соответствующие обязательства по предоставлению информации, за исключением случаев, когда и поскольку соответствующие обязанности контролера определены законодательством ЕС или государства-члена ЕС. В соглашении должен быть указан контактный пункт для субъектов данных. Государства-члены ЕС вправе определить, кто из контролеров, осуществляющих совместную обработку, может действовать в качестве единого контактного пункта для субъектов данных в целях осуществления прав субъектов данных. Независимо от условий соглашения "совместных операторов", государства-члены ЕС вправе предусмотреть, что субъект персональных данных может осуществлять свои законодательно закрепленные права в отношении каждого из таких операторов.

2. [Часть 2](#) комментируемой статьи вопреки наименованию содержащей ее статьи фактически легализует обязанность оператора персональных данных опубликовать или иным образом обеспечить неограниченный доступ к:

документу, определяющему политику оператора персональных данных в отношении обработки персональных данных;

сведениям о реализуемых требованиях к защите персональных данных.

Способами обеспечения неограниченного доступа к указанным сведениям могут стать их публикация в печатных средствах массовой информации, размещение ее на информационных стендах, на сайте в сети Интернет и т.д. В отношении оператора, который осуществляет сбор персональных данных с использованием информационно-телекоммуникационных сетей, установлена императивная обязанность публикации указанных выше документов и сведений в соответствующей информационно-телекоммуникационной сети с предоставлением возможности неограниченного доступа к ним.

Например, политика конфиденциальности ООО "Яндекс" (<https://yandex.ru/legal/confidential/index.html>) действует в отношении всей информации, которую ООО "Яндекс" или его аффилированные лица могут получить в процессе использования субъектом любых сайтов, программ, продуктов или сервисов, включая персональные данные.

Политика конфиденциальности имеет форму "вопрос-ответ" и состоит из следующих подразделов:

- 1) Что регулирует настоящая политика конфиденциальности?
- 2) Кто обрабатывает информацию?
- 3) Какова цель данной политики?
- 4) Какую персональную информацию о вас собирает Яндекс?
- 5) Какова правовая основа и цели обработки вашей персональной информации?
- 6) Как Яндекс защищает вашу персональную информацию?
- 7) Кто еще имеет доступ к вашей персональной информации и кому она может быть передана?
- 8) Где хранится и обрабатывается ваша персональная информация?
- 9) Как долго мы храним вашу персональную информацию?
- 10) Ваши права.

11) Как мы используем файлы cookie и другие подобные технологии на сайтах или при использовании вами сервисов?

12) Обновление настоящей политики.

13) Вопросы и предложения.

В четвертом разделе перечислены виды данных, обрабатываемых ООО "Яндекс":

персональная информация, предоставленная при регистрации (создании учетной записи), такая как имя, номер телефона, адрес и возраст;

электронные данные (HTTP-заголовки, IP-адрес, файлы cookie, веб-маяки/пиксельные теги, данные об идентификаторе браузера, информация об аппаратном и программном обеспечении, данные сети wi-fi);

дата и время осуществления доступа к сайтам или сервисам;

информация об активности во время использования сайтов или сервисов (например, история поисковых запросов, данные о покупках в сервисах, данные о посещенных организациях, лайки и предпочтения, адреса электронной почты тех, с кем ведете переписку, данные телефонной книги, информация о взаимодействии с другими пользователями, а также файлы и контент, хранящиеся в системах Яндекса);

информация о геолокации;

иная информация, необходимая для обработки в соответствии с условиями, регулирующими использование конкретных сайтов или сервисов Яндекса.

В том же разделе особо подчеркивается, что Яндекс не собирает целенаправленно такую персональную информацию, как расовое происхождение, политические взгляды, информация о здоровье и биометрические данные, за исключением случаев, предусмотренных пользовательскими соглашениями отдельных сервисов.

3. **Часть 3** комментируемой статьи предусматривает возможность установления Правительством РФ специальных обязанностей для операторов персональных данных, являющихся органами публичной власти. В Российской Федерации, исторически имеющей жесткую субординационную систему государственного управления, доля подобных операторов от общего их числа достаточно высока. В соответствии с **постановлением** Правительства РФ от 21 марта 2012 г. 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" в перечень подобных мер входят:

1) назначение ответственного за организацию обработки персональных данных в государственном или муниципальном органе из числа государственных или муниципальных служащих и (или) работников указанного органа, замещающих должности, не являющиеся должностями государственной гражданской службы РФ или муниципальной службы, на основании трудового договора (далее - служащие).

2) утверждение актом руководителя государственного или муниципального органа следующих документов:

правил обработки персональных данных, устанавливающих процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере персональных данных, а также определяющих 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;

правил рассмотрения запросов субъектов персональных данных или их представителей;

правил 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;

правил работы с обезличенными данными в случае обезличивания персональных данных;

перечня информационных систем персональных данных;

перечня персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций;

перечня должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных;

перечня должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

должностного регламента (должностных обязанностей) или должностной инструкции ответственного за организацию обработки персональных данных в государственном или муниципальном органе;

типового обязательства служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;

типовой формы согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных, а также типовой формы разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

порядка доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка персональных данных.

3) принятие правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке, предусмотренных соответствующими нормативными правовыми актами, для выполнения установленных Правительством РФ требований к защите персональных данных при их обработке, исполнение которых обеспечивает установленные уровни защищенности персональных данных.

4) выполнение установленных [постановлением](#) Правительства РФ от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" требований:

обеспечение возможности определения места хранения каждой категории персональных данных (материальных носителей) и установления перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

обеспечение сохранности персональных данных и исключение возможности несанкционированного доступа к ним, в том числе, через принятие мер, устанавливаются самим оператором;

обеспечение раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

Европейское законодательство содержит аналогичные нормативные установления. Так, [ч. 2 ст. 20](#) Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами предписывает операторам персональных данных имплементировать технические и организационные меры, гарантирующие обработку только тех персональных данных, которые необходимы для каждой конкретной цели обработки. Указанное обязательство применяется в отношении количества собранных персональных данных, объема их обработки, срока их хранения и их доступности. В частности, указанные меры должны гарантировать, что по умолчанию доступ к персональным данным не будет предоставлен неопределенному числу физических лиц без участия отдельного лица.

5) проведение периодических проверок условий обработки персональных данных в государственном или муниципальном органе в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям. Проверки осуществляются лицом, 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.

б) ознакомление служащих государственного или муниципального органа, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ 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.

7) уведомление уполномоченного органа по защите прав субъектов персональных данных об обработке (намерении осуществлять обработку) персональных данных, за исключением случаев, установленных комментируемым законом.

8) обезличивание персональных данных в установленных законом случаях и в соответствии с установленными Роскомнадзором требованиями и методами.

Помимо перечисленных мер, отдельные обязанности оператора вытекают из положений [постановления](#) Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", [приказа](#) ФСТЭК России от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", [приказа](#) ФСБ России от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)", а также иных подзаконных нормативных актов.

4. Согласно [ч. 4](#) комментируемой статьи оператор обязан представить документы и локальные акты, указанные в [ч. 1](#) комментируемой статьи, и (или) иным образом подтвердить принятие мер, указанных в ч. 1 комментируемой статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных. Срок предоставления сведений определяется в запросе, однако по общему правилу он не должен превышать 30 дней.

[Статья 19.](#) Меры по обеспечению безопасности персональных данных при их обработке

1. Комментируемая [статья](#) посвящена обязанностям оператора персональных данных принимать меры по обеспечению безопасности персональных данных при их обработке.

В силу [ч. 1](#) рассматриваемой статьи оператор должен принять необходимые меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Меры разделяются на:

1) правовые.

К числу правовых мер относится, в частности, создание оператором определенного пакета документов в рамках реализации защиты персональных данных. Обращаем внимание, что перечень таких документов законом прямо не предусмотрен, также отсутствуют точные рекомендации Роскомнадзора на этот счет. К таким документам, как правило, относятся:

утвержденная политика в отношении обработки персональных данных;

приказ о назначении лица, ответственного за организацию обработки персональных данных физических лиц;

приказ об утверждении перечня работников, имеющих доступ к персональным данным физических лиц;

соглашение о конфиденциальности с работниками, имеющими доступ к персональным данным.

журналы учета и движения персональных данных;

регламенты по работе с персональными данными.

Существуют [рекомендации](#) Роскомнадзора от 31 июля 2017 г. по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном [Федеральным законом](#) от 27 июля 2006 года N 152-ФЗ "О персональных данных";

2) организационные и технические.

К организационным и техническим мерам следует относить совершаемые действия оператором в рамках обеспечения безопасности данных. Обращаем внимание, что [постановление](#) Правительства от 21 марта 2012 г. N 211 утвержден [Перечень](#) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

Принятие мер оператором персональных данных по обеспечению их безопасности ставится во главу угла и в рамках Регламента ЕС о защите персональных данных. Согласно [ст. 24](#) Регламента контролер должен имплементировать соответствующие технические и организационные меры, гарантирующие и подтверждающие, что обработка осуществляется в соответствии с Регламентом.

Указанные меры должны своевременно пересматриваться и при необходимости уточняться.

Кроме того, государства-члены ЕС, надзорные органы, Совет ЕС и Европейская Комиссия должны содействовать разработке норм поведения, предназначенных для надлежащего применения [Регламента](#), с учетом специфических особенностей различных секторов обработки и специфических потребностей микропредприятий, малых и средних предприятий.

Объединения и другие организации, представляющие категории контролеров или обрабатывающих данные лиц, могут разработать нормы поведения, внести в них изменения или расширить их в целях определения применения Регламента, с учетом следующего:

- справедливой и прозрачной обработки;
- законных интересов контролеров в определенных контекстах;
- сбора персональных данных;
- псевдонимизации персональных данных;
- информации, предоставляемой общественности и субъектам данных;
- осуществления прав субъектов данных;
- информирования и защиты детей, а также способом, посредством которого должно быть получено согласие лиц, обладающих родительской ответственностью в отношении ребенка;
- мер и процедур для обеспечения безопасности обработки;
- уведомления надзорных органов об утечке персональных данных и информирования об указанных утечках персональных данных субъектов данных;
- передачи персональных данных третьим странам или национальным организациям;
- внесудебных процедур и иных процедур разрешения спорных вопросов между контролерами и субъектами данных в отношении обработки, без ущерба правам субъектов данных.

2. [Часть 2](#) комментируемой статьи конкретизирует перечень мер, направленных на обеспечение безопасности персональных данных. В данный перечень входит:

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

В рамках [ч. 11](#) настоящей статьи раскрывается понятие "угрозы безопасности персональных данных", под которой понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Например, согласно [указанию](#) Банка России от 10 декабря 2015 г. N 3889-У "Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных" определение типа угроз безопасности персональных данных, актуальных для информационной системы персональных данных, производится оператором информационной системы персональных данных.

Угрозами безопасности персональных данных, актуальными при их обработке в информационных системах персональных данных, являются следующие:

- угроза несанкционированного доступа к персональным данным лицами, обладающими полномочиями в информационной системе персональных данных, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационной системы персональных данных;

- угроза воздействия вредоносного кода, внешнего по отношению к информационной системе персональных данных;

- угроза использования методов социального инжиниринга к лицам, обладающим полномочиями в информационной системе персональных данных;

- угроза несанкционированного доступа к отчуждаемым носителям персональных данных;
- угроза утраты (потери) носителей персональных данных, включая переносные персональные компьютеры пользователей информационной системы персональных данных;

- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в организации защиты персональных данных;

- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в программном обеспечении информационной системы персональных данных;

угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;

угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационной системы персональных данных;

угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств криптографической защиты информации.

Требования к защите персональных данных при их обработке в информационных системах персональных данных утверждены **постановлением** Правительства от 1 ноября 2012 г. N 1119. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми ФСБ и Федеральной службой по техническому и экспортному контролю.

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 обеспечивают установленные Правительством РФ уровни защищенности персональных данных.

Перечень таких организационных и технических мер предусматривается ведомственными нормативными актами, среди которых:

а) **приказ** ФСБ от 10 июля 2014 г. N 378, который устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности;

б) **приказ** ФСТЭК от 18 февраля 2013 г. N 21, который устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных для каждого из уровней защищенности персональных данных, установленных в **Требованиях** к защите персональных данных при их обработке в информационных системах персональных данных, утв. **постановлением** Правительства от 1 ноября 2012 г. N 1119.

В частности, в состав таких мер входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных.

Приказом ФСТЭК от 11 февраля 2013 г. N 17 утверждены **Требования** о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

формирование требований к защите информации, содержащейся в информационной системе;

разработка системы защиты информации информационной системы;

внедрение системы защиты информации информационной системы;
аттестация информационной системы по требованиям защиты информации и ввод ее в действие;
обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

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

Процедура оценки соответствия должна происходить в соответствии с [Федеральным законом](#) от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании". Оценка соответствия представляет собой прямое или косвенное определение соблюдения требований, предъявляемых к объекту.

Кроме того, указанным законом предусматривается процедура сертификации как формы осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, документам по стандартизации или условиям договоров. Так, Закон РФ от 21 июля 1993 г. N 5485-1 "О государственной тайне" в [ст. 28](#) устанавливает, что средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области обороны, в соответствии с функциями, возложенными на них законодательством Российской Федерации. Сертификация осуществляется в соответствии с [Законом](#) РФ от 21 июля 1993 г. N 5485-1 в порядке, установленном Правительством РФ.

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

Следует учитывать, что форма оценки эффективности принимаемых мер по обеспечению безопасности персональных данных комментируемым законом не определена. Как правило, форма оценки эффективности принимаемых мер по обеспечению безопасности персональных данных определяется внутренними документами оператора.

[Постановление](#) Правительства от 1 ноября 2012 г. N 1119 устанавливает, что контроль за выполнением 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).

5) Учет машинных носителей персональных данных.

Оператором, как правило, составляется документ, определяющий конкретные носители, на которых осуществляется обработка и хранение персональных данных. За отсутствие указанного документа оператор может быть привлечен к ответственности.

Пример: постановлением мирового судьи общество признано виновным в совершении административного правонарушения, предусмотренного [ст. 13.11](#) КоАП, и подвергнуто административному наказанию в виде административного штрафа в размере 5000 рублей. Общество было привлечено к ответственности за следующие нарушения:

анкеты, которые содержат персональные данные и использование которых завершено, в установленном порядке не уничтожены;

хранение ранее использовавшихся в работе анкет с персональными данными осуществляется в картонных коробках в шкафу без запирающего устройства, что не обеспечивает ограничение доступа к персональным данным третьих лиц;

отсутствует документ, определяющий конкретные носители, на которых осуществляются обработка и хранение персональных данных;

отсутствуют документы, подтверждающие принятие мер, направленных на исполнение требований, установленных комментируемым законом (см. [постановление](#) Верховного Суда РФ от 21 марта 2017 г. N 91-АД17-2).

6) Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них.

В рамках [ч. 4](#) комментируемой статьи определено, что состав и содержание необходимых для

выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

Согласно [приказу](#) ФСТЭК от 18 февраля 2013 г. N 21 "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

Требования к системам обнаружения вторжений (СОВ) утверждены приказом ФСТЭК от 6 декабря 2011 г. N 638. Профили защиты делятся на 6 классов защиты, потому что другие связаны с охраной государственной тайны. Введено два типа систем обнаружения вторжений:

система уровня сети подключается к коммуникационному оборудованию (например, коммутатору) и контролирует сетевой трафик, наблюдая за несколькими сетевыми узлами;

система уровня узла устанавливается на отдельно взятое устройство и проводит анализ системных вызовов, журналов работы приложений и других источников.

Эти требования применяются к программным и программно-техническим средствам, обеспечивающим защиту (некриптографическими методами) информации ограниченного доступа.

Требования предназначены для организаций, создающих средства защиты информации, для заявителей на сертификацию, для испытательных лабораторий и органов по сертификации.

Указанные требования должны выполняться при оценке соответствия (включая сертификацию) средств технической защиты данных и средств обеспечения безопасности информационных технологий, применяемых для формирования государственных информационных ресурсов, организуемых ФСТЭК.

[Федеральным законом](#) от 30 декабря 2020 г. N 515-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части обеспечения конфиденциальности сведений о защищаемых лицах и об осуществлении оперативно-розыскной деятельности" комментируемый [пункт](#) был дополнен указанием на то, какие меры могут применяться при обнаружении фактов несанкционированного доступа к персональным данным. Внесение изменений осуществлено одновременно с введением в России запрета на разглашение личных данных лиц, пользующихся государственной защитой, и сведений об оперативно-розыскной деятельности.

Перечень мер, применяемых для обеспечения безопасности персональных данных, сформулирован неисчерпывающим образом и включает:

меры по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных;

меры по реагированию на компьютерные инциденты в информационных системах персональных данных.

Под компьютерной атакой при этом следует понимать целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

Компьютерный инцидент, в свою очередь, это факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

Данная терминология используется в [ст. 2](#) Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, утверждены приказом ФСТЭК от 6 мая 2019 г. N 196.

7) Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним. Восстановление производится путем копирования резервной копии.

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;

На практике выделяют следующие модели разграничения доступа: мандатное и дискреционное.

В мандатной модели обычные пользователи лишены возможности управлять настройками политик безопасности. Возможность доступа к тому или иному объекту определяется уровнем секретности объекта и уровнем доступа пользователя, которые жестко заданы для каждого пользователя и объекта. Данная модель обладает невысокой гибкостью и высокой трудоемкостью настройки политик безопасности, но при этом позволяет достичь высокого уровня управляемости безопасностью.

При дискреционном разграничении доступа (избирательном, контролируемом) управление доступом субъектов к объектам базируется на том, что пользователи в том или ином объеме могут управлять настройками политик безопасности.

Кроме того, существует ролевая модель доступа, представляющая собой набор групп, объединяющих пользователей с одинаковым уровнем доступа. Уровень доступа к тому или иному объекту определяется по совокупности групп, которым принадлежит субъект. Данная модель может использоваться как в дискреционной, так и в мандатной модели разграничения доступа.

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

Контроль может происходить как посредством внутренних, так и внешних проверок компетентными органами.

Внутренние проверки состояния защиты информации при ее обработке в информационных системах проводятся оператором в соответствии с планом мероприятий по защите персональных данных. Обо всех существенных нарушениях, выявленных в ходе проведения внутренних проверок состояния защиты информации, незамедлительно сообщается ответственному лицу. Проведенные внутренние проверки должны учитываться в журнале учета проводимых внутренних проверок.

Примером внешних проверок являются контрольные мероприятия Роскомнадзора. Роскомнадзор осуществляет проверку выполнения требований законодательства в области обеспечения безопасности персональных данных с целью защиты прав субъектов.

3. В соответствии с [ч. 3](#) рассматриваемой статьи к компетенции Правительства РФ отнесены полномочия определять:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных. [Постановлением](#) Правительства от 1 ноября 2012 г. N 1119 при обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных;

2) [требования](#) к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных. Данные требования установлены [постановлением](#) Правительства от 1 ноября 2012 г. N 1119;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. Такие [требования](#) определены [постановлением](#) Правительства от 6 июля 2008 г. N 512. В частности, материальный носитель должен обеспечивать:

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

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

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

невозможность несанкционированного доступа к биометрическим персональным данным, содержащимся на материальном носителе.

4. [Часть 5](#) настоящей статьи декларирует возможность федеральных органов исполнительной власти, осуществляющих функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органов государственной власти субъектов РФ, Банка России, органов государственных внебюджетных фондов, иных государственных органов в пределах своих полномочий принимать нормативные правовые акты, в которых определяются угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении

соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

Так, **приказом** Минэнерго от 2 августа 2019 г. N 819 определены угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении Минэнерго функций, определенных законодательством Российской Федерации.

Приказом Минюста от 21 ноября 2019 г. N 264 определяются угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, являющихся подсистемами федеральной государственной информационной системы "Автоматизированная информационная система Федеральной службы судебных приставов", и информационных системах персональных данных, не являющихся подсистемами федеральной государственной информационной системы "Автоматизированная информационная система Федеральной службы судебных приставов".

Часть 7 комментируемой статьи предусматривает необходимость согласовывать указанные проекты нормативных актов с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (ФСБ и ФСТЭК).

5. Кроме того, в соответствии с **ч. 6** рассматриваемой статьи ассоциации, союзы и иные объединения операторов вправе своими решениями 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.

Вместе с тем в соответствии с **ч. 7** проекты указанных решений также подлежат согласованию с ФСБ и ФСТЭК.

Правила согласования проектов решений ассоциаций, союзов и иных объединений операторов утверждены **постановлением** Правительства от 18 сентября 2012 г. N 940.

Проект решения, направляемый на согласование, должен содержать:

а) наименование объединения операторов;

б) наименование и реквизиты нормативного правового акта, принятого в соответствии с **ч. 5** комментируемой статьи, определяющего угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки, наряду с которыми объединение операторов определило дополнительные угрозы безопасности персональных данных;

в) перечень видов деятельности, при осуществлении которых в информационных системах персональных данных при обработке персональных данных актуальны дополнительные угрозы безопасности персональных данных;

г) перечень дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении указанных видов деятельности членами объединений операторов.

Проект решения подлежит рассмотрению в течение 30 рабочих дней со дня его поступления в ФСБ и ФСТЭК.

Основаниями для отказа в согласовании проекта решения являются:

а) наличие в проекте решения дополнительных угроз, которые реализуются в составе других дополнительных угроз безопасности персональных данных, не отраженных в проекте решения;

б) наличие в проекте решения дополнительных угроз, которые влекут за собой возникновение других дополнительных угроз безопасности персональных данных, не отраженных в проекте решения;

в) несоблюдение требований, установленных Правилами согласования проектов.

6. Согласно **ч. 8** рассматриваемой статьи контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются ФСБ и ФСТЭК в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

Кроме того, в силу **ч. 9** комментируемой статьи ФСБ и ФСТЭК решением Правительства с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их

обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

7. По правилам [ч. 10](#) комментируемой статьи 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.

Технологии хранения биометрических персональных данных вне информационных систем персональных данных должны обеспечивать:

- а) доступ к информации, содержащейся на материальном носителе, для уполномоченных лиц;
- б) применение средств электронной подписи или иных информационных технологий, позволяющих сохранить целостность и неизменность биометрических персональных данных, записанных на материальный носитель;
- в) проверку наличия письменного согласия субъекта персональных данных на обработку его биометрических персональных данных или наличия иных оснований обработки персональных данных, установленных законодательством в сфере отношений, связанных с обработкой персональных данных.

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. Право на доступ к своим персональным данным, декларируемое комментируемым законом, является основополагающим как для российского, так и зарубежного законодательства, регулирующего сбор, хранение и передачу персональных данных. Согласно [п. 63 преамбулы](#) Регламента ЕС о защите персональных данных субъект данных должен иметь право доступа к относящимся к нему собранным персональным данным; указанное право должно осуществляться беспрепятственно и с определенной периодичностью в целях получения информации об обработке и проверки ее законности.

Указанное право представляет собой, в первую очередь, право на получение субъектом персональных данных подтверждения об обработке его персональных данных, получения доступа к данным, а также к информации в отношении целей обработки, категории обрабатываемых данных, получателей персональных данных, предусмотренного срока хранения персональных данных и т.д.

Часть 1 комментируемой статьи возлагает на оператора обязанность сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными.

Таким образом, в рамках настоящей статьи проводится уточнение порядка реализации права субъекта персональных данных на доступ к его персональным данным, предусмотренного [ст. 14](#) комментируемого закона.

При непосредственном (личном) обращении субъекта персональных данных или его представителя исполнение обязанности оператором происходит в момент такого обращения.

В случае если оператор получил соответствующий запрос субъекта персональных данных, то у него имеется 30 дней с даты получения запроса на исполнение возложенной законом обязанности.

Вместе с тем оператору необходимо учитывать, что запрос должен отвечать предъявляемым к нему требованиям. В частности, в запросе на предоставление информации, касающейся обработки персональных данных субъекта персональных данных, должны быть указаны:

- 1) период обработки персональных данных;
- 2) перечень обрабатываемых персональных данных, в том числе указание на специальные, биометрические данные;

Специальные категории персональных данных касаются расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

- 3) цель обработки персональных данных;
- 4) способы обработки персональных данных;
- 5) Ф.И.О., паспортные данные, в том числе дата выдачи, выдавший орган субъекта персональных данных;

б) наименование или Ф.И.О. оператора, ИНН, адрес;

7) основание, по которому проводилась обработка персональных данных (например, номер, дата договора либо сведения, иным образом подтверждающие факт обработки персональных данных оператором);

8) указание на сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором;

9) доверенность представителя (в случае если заявление подписывается представителем заявителя).

Запрос субъекта персональных данных декларирован также в [ст. 15](#) Регламента ЕС о защите персональных данных, в рамках которой субъект данных имеет право запрашивать у контролера подтверждение относительно того, обрабатываются ли относящиеся к нему персональные данные, и если дело обстоит именно так, он имеет право на доступ к персональным данным и следующей информации:

цели обработки;

категории обрабатываемых персональных данных;

получатели или категории получателей, которым были или будут раскрыты персональные данные, в частности, получатели в третьих странах или международные организации;

по мере возможности, предусмотренный срок, в течение которого будут храниться персональные данные, или, при отсутствии соответствующей возможности, критерии, используемые для определения указанного периода;

существование права требования от контролера исправления или удаления соответствующих персональных данных, или ограничения их обработки, или возражения против указанной обработки;

существование права подачи жалобы в надзорный орган;

в случае если персональные данные получены не от субъекта данных, любая доступная информация об их источнике.

В случае непредставления оператором информации о персональных данных субъекта последний правомочен обратиться с требованием в суд об обязанности представить данную информацию. Вместе с тем следует учитывать, что в силу [ч. 1 ст. 56](#) ГПК каждая сторона должна доказать те обстоятельства, на которые она ссылается как на основания своих требований и возражений, если иное не предусмотрено федеральным законом.

Пример 1: в ходе рассмотрения требования об обязанности представить информацию, касающуюся обработки персональных данных, представленных в рамках кредитного договора, взыскании компенсации морального вреда, судебных расходов, судом было установлено, что заемщик направил заявление в банк о предоставлении информации, касающейся обработки его персональных данных, представленных в рамках кредитного договора, которое осталось без ответа.

Разрешая требования, суд первой инстанции пришел к обоснованному выводу об отказе в удовлетворении заявленных исковых требований, поскольку при заключении договора истцу были представлены все документы, содержащие полную информацию о предмете договора, а также о предложенных банком услугах. Истец была ознакомлена со всеми условиями договора, обязалась их соблюдать, при заключении договора истец выразила свое согласие на обработку всех своих персональных данных. Истец самостоятельно предоставила ответчику свои персональные данные в целях их обработки, ей были известны цели обработки персональных данных, наименование и место нахождения оператора.

При этом суд первой инстанции обоснованно указал, что заявление о предоставлении информации относительно обработки персональных данных направлено по адресу, который адресом места нахождения ответчика не является, сведений о получении заявления ответчиком в материалах дела не имеется, доказательств того, что ответчик осуществляет обработку ее персональных данных с нарушением требований закона или иным образом нарушает права и свободы истца, не представлено (см. [апелляционное определение](#) Санкт-Петербургского городского суда от 17 апреля 2018 г. N 33-8394/2018 по делу N 2-272/2018).

Пример 2: в ходе рассмотрения требования о возложении обязанности предоставить информацию об обработке персональных данных, взыскании денежной компенсации морального вреда истица указала, что непредоставление запрашиваемой информации по истечении 30 дней со дня направления запроса является незаконным и дает ей право требовать исполнения обязанности в натуре и возмещения морального вреда.

Однако судом в удовлетворении требования было отказано, так как доказательств личного обращения истицы к ответчику с предъявлением паспорта, а также оформления запроса в соответствии с требованиями закона в материалы дела не представлено, каких-либо нарушений прав истицы и злоупотребления своими правами со стороны ответчика судом не установлено (см. [апелляционное](#)

определение Московского городского суда от 16 декабря 2015 г. по делу N 33-47309/2015).

Пример 3: в ходе разбирательства судебная коллегия пришла к выводу о том, что ООО "МигКредит" в нарушение предусмотренной комментируемой статьей тридцатидневного срока не направило С. ответ на ее заявление о предоставлении информации об обработке персональных данных, полученных в рамках договора займа, или отказ в предоставлении запрашиваемой информации. Доказательств подготовки и направления такого ответа ни суду первой инстанции, ни суду апелляционной инстанции не представлено. Суд пришел к выводу о взыскании с ответчика в пользу истца компенсации морального вреда, отвечающей требованиям разумности и справедливости (см. **апелляционное определение** Московского городского суда от 14 декабря 2015 г. по делу N 33-47059/2015).

2. **Часть 2** рассматриваемой статьи декларирует право оператора отказать в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных. Однако данный отказ обязательно должен быть мотивирован основаниями, предусмотренными комментируемым законом.

Отказ оператора должен быть обоснован одним из следующих законодательно установленных ограничений:

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

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

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;

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

Письменный мотивированный ответ оператора должен быть дан в течение 30 дней.

3. По правилам **ч. 3** комментируемой статьи оператор обязан предоставить субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных, исключительно на безвозмездной основе.

Кроме того, законодатель обязывает оператора при выявлении неточных персональных данных заблокировать данные или обеспечить их блокирование с момента обращения субъекта персональных данных (при условии, что это не затрагивает права и законные интересы самого субъекта или третьих лиц). В случае если будет установлен факт неточности данных, оператор обязан уточнить их в течение 7 рабочих дней со дня представления таких сведений и снять блокировку.

Дополнительно законодатель возлагает на оператора обязанность уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

На оператора персональных данных возлагается обязанность по уничтожению персональных данных, не являющихся необходимыми для заявленной цели обработки, при заявлении об этом субъектом персональных данных.

Пример: в ходе рассмотрения требования об обязанности уничтожить персональные данные, находящиеся на всех материальных и электронных носителях общества, переданные им третьим лицам и размещенные в сети Интернет, судом было установлено, что истец никогда не являлся ни акционером общества (ответчика), ни членом совета его директоров и никогда не принимал участия в его работе, в связи с чем он потребовал, чтобы общество уничтожило его персональные данные. Требование было удовлетворено, поскольку доказано, что ответчик не имел законных оснований на обработку, хранение, распространение и использование персональных данных истца, так как последний на это своего согласия не давал и членом совета директоров общества не являлся (см. **постановление** Арбитражного суда Волго-Вятского округа от 27 ноября 2019 г. N Ф01-6281/2019 по делу N А82-782/2019).

Декларируемые в рамках данной **части** комментируемой статьи правила реализуются в европейском законодательстве в рамках **Регламента** ЕС о защите персональных данных посредством наделения субъектов персональных данных отдельными правомочиями. Так, Регламент закрепляет право на внесение изменений (исправление ошибок) - посредством которого субъект вправе требовать от контролера внесения изменений и устранение неточностей в отношении его персональные данные.

Кроме того, нормативно установлено право на удаление персональных данных (право на забвение), в соответствии с которым субъект данных вправе требовать от контролера незамедлительного удаления относящихся к нему персональных данных при наличии особых оснований (например, персональные данные больше не требуются для целей, для которых они были получены; субъект данных отозвал свое согласие; персональные данные обрабатывались незаконно и т.д.). Однако при получении запроса на удаление данных контролер должен принимать во внимание общественный интерес в указанных данных, основополагающее право на свободу выражения мнения и распространение информации и иные условия, обозначенные в **Регламенте**. В некоторых случаях, при невозможности удаления персональных данных, может быть применено ограничение обработки персональных данных.

4. **Частью 4** комментируемой статьи на оператора возлагается обязанность представить в Роскомнадзор необходимую информацию в течение 30 дней. Информация предоставляется в рамках соответствующего запроса Роскомнадзора, направляемого в пределах его компетенции как федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

Зачастую запросы Роскомнадзора обоснованы необходимостью рассмотрения обращений граждан по вопросам защиты их персональных данных.

За непредставление информации оператор может быть привлечен к ответственности по **ст. 19.7** КоАП, предусматривающей в виде санкций как предупреждение, так и наложение административного штрафа:

- на граждан в размере от 100 до 300 рублей;
- на должностных лиц - от 300 до 500 рублей;
- на юридических лиц - от 3000 до 5000 рублей.

Пример 1: компания была признана виновной в совершении административного правонарушения, предусмотренного **ст. 19.7** КоАП, с назначением административного наказания в виде административного штрафа - 3000 рублей.

Согласно материалам дела компания привлечена к административной ответственности за то, что в нарушение требований **ч. 4** комментируемой статьи в установленный срок ею не представлены в Роскомнадзор сведения, указанные в запросе руководителя названного административного органа от 17 декабря 2018 г. N 08ЖА-106548, а именно: информация о результатах принятия компанией мер по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения персональных данных российских пользователей социальной сети Twitter с использованием баз данных, находящихся на территории Российской Федерации, в том числе с предоставлением заверенной блок-схемы размещения рабочих мест, на которых осуществляется хранение персональных данных российских пользователей; справки о постановке на балансовый учет компании приобретенных серверных мощностей; договора купли-продажи серверных мощностей; копии договора аренды компанией технических площадок (ЦОД, серверные мощности) на территории Российской Федерации (см. **постановление** Верховного Суда РФ от 27 декабря 2019 г. N 5-АД19-239).

Пример 2: из материалов дела следует, что в целях исполнения Управлением Роскомнадзора по Уральскому федеральному округу возложенных на него полномочий по контролю и надзору за соответствием обработки персональных данных требованиям законодательства в адрес ГБПОУ СО "ТЛК имени Н.И. Кузнецова" был направлен запрос от 23 июня 2016 г. о предоставлении сведений по внесению сведений о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации.

Однако информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных, юридическое лицо направило с нарушением установленного срока - 8 сентября 2016 г., в связи с чем в отношении ГБПОУ СО "ТЛК имени Н.И. Кузнецова" уполномоченным должностным лицом был составлен протокол об административном правонарушении, предусмотренном **ст. 19.7** КоАП.

Обстоятельства правонарушения подтверждены совокупностью представленных доказательств, в том числе: запросом Управления Роскомнадзора от 23 июня 2016 г., почтовым уведомлением о

вручении, [информационным письмом](#) от 8 сентября 2016 г., протоколом об административном правонарушении.

Судебные инстанции пришли к правильному выводу о том, что действия ГБПОУ СО "ТЛК имени Н.И. Кузнецова", выразившиеся в несвоевременном представлении сведений в Управление Роскомнадзора, образуют объективную сторону состава административного правонарушения, предусмотренного [ст. 19.7](#) КоАП (см. постановление заместителя председателя Свердловского областного суда от 14 марта 2017 г. N 4а-117/2017).

Следует учитывать, что оператором является лицо, осуществляющее либо намеревающееся осуществлять обработку персональных данных, и комментируемый закон не связывает признание лица оператором с фактом включения (регистрации) такого лица в реестр операторов, осуществляющих обработку персональных данных. Поэтому правовое значение для квалификации деятельности лица в качестве деятельности оператора имеет факт осуществления этим лицом видов деятельности, при которых оно может обрабатывать персональные данные, а равно его намерение осуществлять такие виды деятельности.

Пример: в рамках рассмотрения требования о признании недействительным требования Роскомнадзора судом было установлено, что предпринимателю направлено требование о предоставлении сведений об обработке персональных данных. Из выписки из ЕГРИП судом было установлено, что основным видом деятельности заявителя является деятельность по коду [62.02](#) "деятельность консультативная и работы в области компьютерных технологий", дополнительными видами деятельности являются: [62.0](#) - "разработка компьютерного программного обеспечения, консультационные услуги в данной области и другие сопутствующие услуги"; [62.01](#) - "деятельность, связанная с использованием вычислительной техники и информационных технологий прочая" [63.11](#) - "деятельность по обработке данных, предоставление услуг по размещению информации и связанная с этим деятельность".

Таким образом, предприниматель вправе осуществлять деятельность по обработке персональных данных, следовательно, он является оператором в смысле положений [ст. 3](#) комментируемого закона и обязан соблюдать правила, установленные комментируемым законом и принимаемыми в его развитие нормативными правовыми актами.

Суд отказал в удовлетворении требования, поскольку предприниматель является оператором, обязан предоставлять по мотивированному запросу сведения, касающиеся его деятельности по обработке персональных данных (см. [постановление](#) Арбитражного суда Дальневосточного округа от 28 мая 2020 г. N Ф03-1734/2020 г. по делу N А51-8681/2019).

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

1. Комментируемая [статья](#) определяет круг обязанностей оператора персональных данных, возлагаемых на него в целях устранения нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных.

По замечанию А.И. Савельева, юридическая техника положений комментируемой [статьи](#) оставляет желать лучшего. Это проявляется как в нечеткости описания обстоятельств, в связи с которыми возникают соответствующие обязанности, так и в несогласованности положений данной статьи с нормами, содержащимися в [ст. 5](#) комментируемого закона. Использование повторяющихся и громоздких формулировок также не добавляет ясности правовым нормам, содержащимся в настоящей статье^{*(74)}.

По правилам [ч. 1](#) рассматриваемой статьи в случае выявления неправомерной обработки персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки.

Выявление неправомерной обработки персональных данных оператором может произойти на основании обращения субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо Роскомнадзора.

Вместе с тем в случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по

поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

Пример: в ходе рассмотрения дела о причинении морального вреда, защите чести, достоинства и деловой репутации истцом были заявлены требования об обязанности удалить сведения, причиняющие вред нематериальным правам.

Судом было установлено, что истец обратился к ответчику с просьбой удалить сведения с сайта. Просьба осталась без удовлетворения. Истец считает, что ответчик не имел права использовать фамилию истца без согласия, отмечает, что фамилия истца использована ответчиком с целью причинения вреда. Истец обращался к ответчику по электронной почте, в письме просил удалить запись от 17 января 2017 г., что подтвердил представитель ответчика, однако запись не была удалена.

Принимая во внимание, что ответчиком нарушены требования настоящего федерального закона при обработке персональных данных Ш. в части обязательности получения согласия субъекта на обработку его персональных данных, Ш. вправе требовать в судебном порядке от ответчика удалить с сайта РОО ТОФК <http://tofk.tom.ru> его персональные данные. В связи с изложенным судебная коллегия считает необходимым обязать ответчика удалить из записи от 17 января 2017 г. "Приказом президента ТОФК Ш. отстранен от должности исполнительного директора РОО "ТОФК", размещенной на сайте РОО ТОФК <http://tofk.tom.ru>, указание на персональные данные: фамилию и инициалы.

Довод ответчика о том, что суд вышел за пределы заявленных требований, поскольку правовым основанием иска Ш. являлась защита неприкосновенности частной жизни, был признан несостоятельным, так как был опровергнут материалами дела (см. апелляционное определение Томского областного суда от 26 февраля 2019 г. по делу N 33-651/2019).

Обращаем внимание на то, что в соответствии с [п. 57](#) Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных, утв. [постановлением](#) Правительства от 13 февраля 2019 г. N 146, при выявлении по итогам проведения мероприятия по контролю без взаимодействия с оператором нарушения (признаков нарушения) требований оператору направляется требование об уточнении, блокировании или уничтожении недостоверных или полученных незаконным путем персональных данных в течение 10 дней с информированием органа по контролю и надзору об исполнении указанного требования либо с представлением мотивированных пояснений по существу выявленных признаков нарушения требований.

В случае неисполнения оператором указанного в [п. 57](#) Правил требования составляется протокол об административном правонарушении в соответствии с [КоАП](#).

Таким образом, оператор персональных данных обязательно должен заблокировать персональные данные, которые указаны в требовании Роскомнадзора. Вместе с тем субъект персональных данных должен проводить проверку обстоятельств обработки персональных данных. Результаты данной проверки должны оформляться документарно во избежание дальнейших споров с Роскомнадзором.

Установленная комментируемой [статьей](#) обязанность оператора корреспондирует праву на удаление (праву на забвение) субъекта персональных данных, декларируемому как комментируемым законом, так и положениями [ст. 17](#) Регламента ЕС о защите персональных данных, согласно которому субъект данных имеет право требовать от контролера незамедлительного удаления относящихся к нему персональных данных. Контролер должен незамедлительно удалить персональные данные, если применяется одно из следующих оснований:

персональные данные больше не требуются для целей, для которых они были получены или обрабатывались в иных случаях;

субъект данных отзывает свое согласие, проводилась обработка, и если отсутствует иное юридическое основание для обработки;

субъект данных возражает против обработки и отсутствуют имеющую преимущественную юридическую силу законные основания для обработки, или субъект данных возражает против обработки;

персональные данные обрабатывались незаконно;

персональные данные должны быть уничтожены в целях соблюдения юридической обязанности согласно законодательству Союза или государства-члена ЕС, под действие которого подпадает контролер;

персональные данные собирались в отношении предоставления услуг информационного общества.

Кроме того, если контролер обнародовал персональные данные и он обязан удалить персональные данные, он с учетом имеющихся технологических возможностей и расходов на имплементацию должен принять необходимые меры, в том числе технические меры, чтобы

проинформировать контролеров, которые обрабатывают персональные данные, о том, что субъект данных затребовал от них удаление любых ссылок, копий или точных повторений указанных персональных данных.

Стоит учитывать, что комментируемый закон устанавливает особенность блокировки персональных данных, на которую обращено внимание многими специалистами. 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*(75).

2. По правилу, установленному **ч. 2** рассматриваемой статьи, при подтверждении факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо Роскомнадзором, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение 7 рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

В случае неисполнения возложенной на оператора обязанности он может быть привлечен к ответственности, если будет доказано, что эти персональные данные являются неполными, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Таким образом, согласно **ч. 5 ст. 13.11** КоАП невыполнение оператором в сроки, установленные законодательством в области персональных данных, требования субъекта персональных данных или его представителя либо Роскомнадзора об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, влечет предупреждение или наложение административного штрафа:

- на граждан в размере от 1000 до 2000 рублей;
- на должностных лиц - от 4000 до 10 000 рублей;
- на индивидуальных предпринимателей - от 10 000 до 20 000 рублей;
- на юридических лиц - от 25 000 до 45 000 рублей.

3. Согласно **ч. 3** комментируемой статьи в случае выявления неправомерной обработки персональных данных оператор в срок, не превышающий 3 рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора.

Если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение.

На оператора комментируемый **закон** возлагает обязанность уведомить субъекта персональных данных или его представителя об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан. В случае, если обращение субъекта персональных данных или его представителя либо запрос Роскомнадзора были направлены Роскомнадзором, его тоже нужно уведомить.

Пример: при заявлении требований о признании недействительным договора об оказании услуг связи, взыскании компенсации морального вреда, о понуждении прекратить обработку персональных данных и уничтожить персональные данные, полученные по договору истец указывал, что неправомерные действия ответчика причинили ему нравственные страдания, поскольку номер телефона, присвоенный по оспариваемому договору, был использован для заключения договора с кредитной организацией. При этом истец не заключал и не подписывал с ответчиком данный договор.

При рассмотрении дела судебной коллегией установлен факт нарушения ответчиком прав истца как потребителя. Учитывая характер допущенных нарушений, конкретные обстоятельства дела, а также требования разумности и справедливости, с ответчика следует взыскать компенсацию морального вреда в размере 1000 рублей.

Таким образом, ответчик обязан прекратить обработку персональных данных истца по договору об оказании услуг связи в течение 3 рабочих дней в случае выявления их неправомерной обработки, то есть в рассматриваемом случае - после получения судебного акта о признании указанного договора недействительным.

Кроме этого, судебная коллегия приняла во внимание то обстоятельство, что между сторонами также заключен иной договор связи, а потому обработка персональных данных ответчиком, на что указано его представителем в судебном заседании и не оспорено истцом, должна осуществляться в

любом случае, независимо от результата рассмотрения настоящего спора (см. [определение](#) Воронежского областного суда от 12 ноября 2019 г. по делу N 33-5626/2019).

Согласимся с мнением специалистов, что комментируемый закон не предусматривает частичного уничтожения персональных данных оператором либо возможности их уничтожения в зависимости от вида носителя, на котором хранится такая информация. Поэтому не будет соответствовать требованиям комментируемого закона уничтожение персональных данных, допустим, только в некоторых электронных базах (например, содержащих список клиентов), но с сохранением их в других базах^{*(76)}.

Следует учитывать, что форма и срок уведомления субъекта персональных данных действующим законодательством для оператора не установлены. Вместе с тем, исходя из концепции построения рассматриваемой статьи, логично увязывать уничтожение неправомерно обрабатываемых персональных данных с достижением цели их обработки. В связи с этим срок информирования субъекта персональных данных не должен превышать 30 дней с момента уничтожения персональных данных^{*(77)}.

4. [Часть 4](#) комментируемой статьи обязывает оператора персональных данных прекратить их обработку и уничтожить персональные данные в срок, не превышающий 30 дней с даты достижения цели обработки персональных данных.

Законодателем обращено внимание на проблему, связанную с тем, что действующая рассматриваемая норма закона не содержит требований к уничтожению персональных данных. Следствием указанного обстоятельства является то, что оператор в отсутствие требований к уничтожению персональных данных сталкивается с проблемой, связанной с анализом достаточности принимаемых мер по уничтожению персональных данных.

В целях применения операторами единых подходов при уничтожении персональных данных в проекте Федерального закона "О внесении изменения в Федеральный закон "О персональных данных" в части уточнения требований к уничтожению персональных данных"^{*(78)} предлагается комментируемую [статью](#) дополнить ч. 7 следующего содержания: уничтожение персональных данных в случаях, предусмотренных настоящей статьей, осуществляется в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных.

По мнению разработчиков законопроекта, указанное изменение направлено на устранение вышеуказанной коллизии в отношении уничтожения персональных данных, а также на исключение возможности разносторонней трактовки понимания действий, подтверждающих со стороны оператора факт уничтожения персональных данных.

Таким образом, уничтожать персональные данные нужно будет с соблюдением требований, которые установит Роскомнадзор как уполномоченный орган. За невыполнение требования об уничтожении данных оператор может быть привлечен к ответственности по [ч. 5 ст. 13.11](#) КоАП.

Вместе с тем оператор имеет право продолжить обработку персональных данных, цели которой были достигнуты, в тех случаях, когда есть иная законная цель (например, дальнейшая обработка прямо предусмотрена законом).

Также комментируемый [закон](#) допускает для оператора возможность в договоре, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, или ином соглашении между оператором и субъектом персональных данных предусмотреть иные правила в отношении прекращения обработки и уничтожения персональных данных с момента достижения цели обработки персональных данных.

5. [Часть 5](#) настоящей статьи определяет обязанности оператора персональных данных в случае отзыва субъектом персональных данных согласия на обработку его персональных данных.

В соответствии с требованиями закона оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 дней с даты поступления указанного отзыва.

Иной порядок может быть предусмотрен в соглашении между оператором и субъектом персональных данных либо если оператору не предоставлено право осуществлять обработку персональных данных без согласия субъекта.

Следует учитывать, что сложившаяся правоприменительная практика по-разному решает вопрос ущемления права потребителя на дачу согласия на обработку персональных данных при заключении договора страхования. В одних случаях суды признают, что отсутствие у потребителя права выбора возможности согласия или отказа в согласии на обработку персональных данных ущемляет права

потребителей, что в силу [ст. 16](#) Закона РФ N 2300-1 "О защите прав потребителей" свидетельствует об их недействительности в этой части.

Пример: в рамках рассмотрения требования об оспаривании предписания управления Роспотребнадзора судом было установлено, что страховщику предписано устранить выявленные нарушения: условия типовых форм договоров страхования ущемляют права потребителей. Суд отказал в удовлетворении требования, поскольку договор не предусматривает право страхователя выбрать: согласиться ему на обработку своих персональных данных или отказаться от нее (см. [постановление](#) Арбитражного суда Северо-Западного округа от 18 июля 2016 г. N Ф07-5537/2016 по делу N А44-9647/2015).

Согласно другой позиции судебной практики отказ гражданина - потребителя от обработки его персональных данных делает невозможным заключение договора страхования с указанным гражданином. В полисах страхования указываются фамилия, имя и отчество страхователя, дата его рождения, паспортные данные, номер мобильного телефона, являющиеся персональными данными. Персональными данными также являются и сведения о банковском счете страхователя, запрашиваемые страховщиком в целях выплаты страхового возмещения. Отказ от обработки персональных данных лишает страховщика возможности внести сведения о страхователе и договоре страхования в электронные базы данных учета страховых полисов, осуществлять взаимодействие со страхователем с использованием интернета и телефонной связи, принимать и обрабатывать его заявление о наступлении страхового случая и производить ему выплату страхового возмещения.

Пример: согласно материалам дела Управление Роспотребнадзора обратилось к СПАО "РЕСО-Гарантия" о защите прав неопределенного круга потребителей. Заявитель указал, что в ходе проведения планового мероприятия по контролю исследовались типовые формы договоров. Было вынесено предписание об устранении выявленных нарушений, а именно о приведении договоров, предлагаемых к заключению гражданам (потребителям), в соответствие с действующим законодательством с исключением из них условий, ущемляющих права потребителей. Однако предписание до настоящего времени не исполнено. В удовлетворении требования было отказано (см. [апелляционное определение](#) Московского городского суда от 12 декабря 2018 г. по делу N 33-54212/2018).

6. Помимо прочего, [ч. 6](#) комментируемой статьи посвящена случаю, когда у оператора отсутствует возможность уничтожения персональных данных в течение предусмотренного [чч. 3-5](#) комментируемой статьи срока. Данные субъекта персональных данных должны быть уничтожены оператором в любом случае при возникновении соответствующей обязанности в срок не более чем 6 месяцев, если иной срок не установлен федеральными законами.

При этом оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение указанного срока.

Порядок документальной фиксации уничтожения персональных данных субъекта определяется оператором персональных данных самостоятельно. Уничтожение персональных данных субъекта осуществляется комиссией (иным должностным лицом), созданной (уполномоченным) на основании приказа оператора. Наиболее распространенными способами документальной фиксации уничтожения персональных данных субъекта является оформление соответствующего акта о прекращении обработки персональных данных либо регистрация факта уничтожения персональных данных в специальном журнале. Типовая форма акта и журнала утверждаются самим оператором.

[Статья 22](#). Уведомление об обработке персональных данных

1. Юридическое предназначение уведомления оператором органа публичной власти об обработке им персональных данных заключается в предоставлении последнему возможности осуществлять надлежащий надзор за состоянием законности в соответствующей сфере информационных правоотношений. Вместе с тем соотношение текущего количества операторов персональных данных с количеством проверок соблюдения операторами законности при обработке персональных данных, которые могут быть проведены Роскомнадзором в течение года, позволяет заключить, что надзорные мероприятия охватывают лишь 0,2 % от общего числа операторов персональных данных.

Справка: по данным Роскомнадзора, по состоянию на октябрь 2020 года в Реестре операторов, осуществляющих обработку персональных данных, включены 414 829 организаций*([79](#)). Согласно Публичному докладу Роскомнадзора в 2019 году проведено 989 проверок, в том числе 136 (13,75%) в отношении органов публичной власти, чья результативность составила 81,3%, то есть у 805 операторов были выявлены нарушения условий и порядка обработки*([80](#)).

Очевидно, что при перманентном росте числа органов и организаций, осуществляющих

обработку персональных данных, эффективность классического государственного надзора за соблюдением законности будет лишь снижаться. Приоритетными способами рационализации рассматриваемой сферы являются:

применение технологий искусственного интеллекта при поиске и выявлении нарушений правил и оснований оборота персональных данных;

стимулирование гражданского общества к информированию государства о фактах нарушения законодательства о персональных данных, которое возможно лишь при повышении правовой культуры населения и снижении толерантности к подобным правонарушениям;

совершенствование методики реализации риск-ориентированного подхода в государственном надзоре за деятельностью операторов персональных данных.

В этом контексте, как нам представляется, основными задачами норм комментируемой статьи будут являться:

1) оказание на операторов персональных данных дисциплинирующего воздействия, так как само наличие информации об операторе в государственной информационной системе обеспечивает внимательное отношение к соблюдению законодательства о персональных данных со стороны руководителя или иного уполномоченного должностного лица данной организации;

2) определение объема выборки для организации надзорных мероприятий Роскомнадзором;

3) снижение нагрузки на надзирающий орган в части доказывания факта осуществления органом или организацией функций оператора персональных данных.

2. **Часть 1** комментируемой статьи устанавливает базовое правило, согласно которому оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных. Указанным в норме органом власти выступает Роскомнадзор, чей непосредственный правовой статус нормативно закреплен Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утв. [постановлением](#) Правительства РФ от 16 марта 2009 г. N 228. В соответствии с Положением Роскомнадзор обеспечивает, организует и осуществляет государственный контроль и надзор за соответствием обработки персональных данных требованиям комментируемого закона и принятых в соответствии с ним нормативных правовых актов ([п. 5.1\(1\) Положения](#)) и ведет реестр операторов, осуществляющих обработку персональных данных ([п. 5.2.4 Положения](#)).

Применительно к комментируемой **части** следует обратить внимание на фразу "до начала обработки персональных данных обязан уведомить о своем намерении". Следует понимать, что подача уведомления после совершения любого из действий, которое признано стадией или элементом оборота персональных данных, является нарушением действующего законодательства.

Оригинальной в контексте отечественной правовой традиции является обязанность оператора, которая закреплена в [п. 59 преамбулы](#) Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами, согласно которой оператор в целях обеспечения эффективной защиты прав и свобод субъектов данных должен консультироваться с надзорным органом в некоторых случаях до начала процесса обработки. Учитывая то обстоятельство, что в норме обрабатывающая персональные данные организация именуется "контролер или обрабатывающее данные лицо", возможно сделать вывод об официальном признании ее оператором по аналогии с отечественным законодательством. Полагаем, что данным правоустановлением на оператора возлагается ответственность за любые неблагоприятные последствия оборота персональных данных, если оператор мог предполагать возможность их наступления даже в режиме правомерной обработки данных. Иными словами, обезопасить себя от преследования оператор может, только запросив консультацию у публичного органа, надзирающего за соблюдением прав субъектов персональных данных.

Другая интересная норма содержится в [ст. 30](#) той же Директивы: в ней предусматривается обязанность оператора уведомлять надзорный орган об утечке персональных данных. Термин "утечка персональных данных" раскрыт в [ст. 3](#) Директивы и [ст. 4](#) Регламента ЕС о защите персональных данных. Под таковой понимается нарушение безопасности, ведущее к случайному или незаконному разрушению, потере, изменению, несанкционированному раскрытию или доступу к переданным, сохраненным или иным образом обработанным персональным данным. Уведомление должно быть осуществлено не позднее 72 часов после того, как оператору стало известно об утечке, кроме случаев, когда утечка персональных данных с большой долей вероятности не приведет к риску для прав и свобод физических лиц. Если уведомление надзорного органа не было сделано в течение 72 часов, в нем необходимо указать причины задержки. Подобное уведомление должно содержать как минимум следующую информацию:

(а) описание характера утечки персональных данных, в том числе по возможности указание

категорий и приблизительного количества затронутых субъектов данных, а также категорий и приблизительного количества учетных записей персональных данных;

(b) имя, фамилию и контактные данные инспектора по защите персональных данных или иного контактного пункта, в котором можно получить более подробную информацию;

(c) описание возможных последствий утечки персональных данных;

(d) описание принятых или планируемых контролером мер для устранения нарушения в виде утечки персональных данных, в том числе, в соответствующих случаях, мер по смягчению его возможного отрицательного воздействия.

3. **Часть 2** комментируемой статьи предусматривает ряд исключений из приведенного выше правила. В соответствии с ней оператор вправе осуществлять без уведомления Роскомнадзора обработку персональных данных:

1) обрабатываемых в соответствии с трудовым законодательством, - обработка и система защиты подобных данных достаточно строго урегулирована законодательными и подзаконными актами о труде и прохождении службы, в связи с чем "двойной" надзор представляется чрезмерным (см. [комментарий](#) к ст. 10);

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных, - наличие данной нормы обусловлено предположением о возможности субъекта персональных данных самостоятельно выявить и сообщить в Роскомнадзор о нарушении правил оборота его персональных данных в рамках договорных отношений (см. [комментарий](#) к ст. 6);

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных, - исключение обусловлено оборотом указанными объединениями и организациями специальных категорий персональных данных и необходимостью защиты конституционной свободы совести и вероисповедания от чрезмерного государственного вторжения (см. [комментарий](#) к ст. 10);

4) разрешенных субъектом персональных данных для распространения при условии соблюдения оператором запретов и условий, предусмотренных [ст. 10.1](#) настоящего федерального закона (см. [комментарий](#) к ст. 10.1);

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных, - таким образом от надзора освобождаются "малые" операторы персональных данных, ущербом от нарушения правил оборота персональных данных которых в контексте риск-ориентированного подхода государственного надзора можно пренебречь;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, - исключение обусловлено краткосрочностью обработки такими операторами персональных данных субъекта, которые должны быть уничтожены после достижения соответствующей цели;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка, - исключение обусловлено режимом ограниченного доступа (государственной, служебной и профессиональной тайны) сведений, содержащихся в указанных информационных системах;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами РФ, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных, - исключение обусловлено использованием риск-ориентированного подхода при надзоре за операторами персональных данных;

9) обрабатываемых в случаях, предусмотренных законодательством РФ о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства (см. [комментарий](#) к ст. 14).

Отсутствие необходимости в уведомлении Роскомнадзора об обороте персональных данных не освобождает оператора от ответственности за неправомерный или нецелевой оборот этих сведений.

4. **Частями 3-7** комментируемой статьи определены форма, содержание, условия и порядок подачи и учета уведомления оператора персональных данных. Положения комментируемых норм детализируются в рамках **Методических рекомендаций** по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения, которые утверждены **приказом** Роскомнадзора от 30 мая 2017 г. N 94.

4.1. Форма. Уведомление об обработке персональных данных может быть направлено в адрес Роскомнадзора в виде документа на бумажном носителе или в форме электронного документа на усмотрение оператора.

4.2. Обязательные реквизиты уведомления во многом схожи с категориями сведений, предоставляемыми оператору персональных данных субъектом при даче согласия на их обработку (см. **комментарий** к ч. 3 ст. 9):

наименование (фамилия, имя, отчество), адрес оператора;

цель обработки персональных данных;

категории персональных данных;

категории субъектов, персональные данные которых обрабатываются;

правовое основание обработки персональных данных;

перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

описание мер, предусмотренных **ст. 18.1** и **19** комментируемого закона, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих 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;

срок или условие прекращения обработки персональных данных;

сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

сведения о месте нахождения базы данных информации, содержащей персональные данные граждан РФ;

сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ.

4.3. К существенным условиям подачи уведомления об обработке персональных данных операторами персональных данных следует отнести:

добровольность и свободу интерпретации операторами персональных данных указанных в **ч. 2** комментируемой статьи исключений;

возложение бремени доказывания наличия оснований осуществления обработки персональных данных без уведомления Роскомнадзора на оператора персональных данных;

недопустимость возложения на оператора персональных данных расходов, связанных с рассмотрением уведомления и внесением соответствующих сведений в реестр;

общедоступность сведений, содержащихся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке.

4.4. Алгоритм учета поданного оператором персональных данных уведомления органами Роспотребнадзора выглядит следующим образом:

1) оператор персональных данных до начала непосредственной обработки персональных данных направляет в Роскомнадзор уведомление;

2) срок рассмотрения уведомления уполномоченным должностным лицом Роскомнадзора составляет 30 календарных дней, включая день получения уведомления; в течение этого срока должно быть принято решение:

о внесении содержащихся в уведомлении сведений в Реестр операторов, осуществляющих обработку персональных данных;

о приостановлении процедуры рассмотрения уведомления и возвращении его оператору персональных данных для дополнения (исправления) в случае предоставления им неполных или недостоверных сведений;

3) в случае получения оператором от органа Роскомнадзора запроса на уточнение или обновление содержащихся в уведомлении сведений, ему рекомендуется направить ответ в течение 30 дней со дня получения запроса;

4) в случае выявления оператором несоответствия действительности указанных в уведомлении сведений, а также в случае прекращения оператором обработки персональных данных, ему рекомендуется в течение 10 дней в адрес органа Роскомнадзора направить соответствующее

информационное письмо;

5) в случае получения органом Роскомнадзора письма от оператора персональных данных, в котором сообщается о необходимости дополнения или обновления содержащихся в Реестре данных, изменения вносятся после проверки в течение 10 дней со дня получения письма;

6) в период учета оператора персональных данных в Реестре сведения о нем могут быть истребованы на основании заявления о предоставлении выписки.

4.5. Непредставление в Роскомнадзор уведомления об обработке персональных данных, его несвоевременное представление или представление уведомления, содержащего неполные или недостоверные сведения, влечет административную ответственность в соответствии со [ст. 19.7 КоАП](#).

Пример: постановлением Верховного Суда РФ от 10 июля 2020 г. N 56-АД20-7 в удовлетворении требования об отмене актов о привлечении к ответственности, предусмотренной [ст. 19.7 КоАП](#), за непредставление сведений (информации) было отказано, решение первой инстанции оставлено без изменения. Как отметил Суд, из материалов дела усматривается, что основанием для привлечения К. к административной ответственности на основании приведенной нормы КоАП послужили изложенные в обжалуемых актах выводы о выявленном в результате плановой выездной проверки, проведенной в период с 20 февраля 2017 г. по 28 февраля 2017 г. Управлением Роскомнадзора по Приморскому краю в отношении учреждения, проректором которого (по общим вопросам) являлся К., факте представления в неполном объеме сведений (информации), содержащихся в уведомлении об обработке персональных данных N 4242, а также в информационных письмах о внесении изменений (вх. N 25-07188, 600/25, 6711/25, 1225), в Роскомнадзор. При этом административным органом установлено, что категории персональных данных, обрабатываемых учреждением, не соответствуют перечню категорий персональных данных, указанных в уведомлении об обработке персональных данных.

Вместе с тем, правоприменительно следует учитывать закрепленные в ч. 2 комментируемой статьи основания, наличие которых указывает на отсутствие состава указанного административного правонарушения.

Пример: постановлением Верховного Суда РФ от 5 августа 2011 г. N 20-АД11-3 производство по делу о привлечении к ответственности по [ст. 19.7 КоАП](#) за непредставление в государственный орган сведений прекращено в связи с отсутствием в действиях заявителя состава правонарушения. Как усматривается из материалов дела, 13 октября 2010 г. Управлением Роскомнадзора в адрес руководителя Коллегии адвокатов N 1 г. Избербаш было направлено письмо, согласно которому указанной организации предлагалось представить уведомление об обработке персональных данных. Письмом председателя Коллегии адвокатов в представлении уведомления об обработке персональных данных было отказано. По факту непредставления уведомления государственным инспектором Роскомнадзора в отношении Коллегии адвокатов составлен протокол об административном правонарушении, предусмотренном [ст. 19.7 КоАП](#).

Мировой судья, разрешая данное дело, исходил из того, что деятельность Коллегии адвокатов связана с обработкой персональных данных, в связи с чем указанная организация обязана уведомить уполномоченный орган, направив уведомление установленного образца. Поскольку Коллегия адвокатов уведомления об обработке персональных данных не представила, то ее действия образуют состав административного правонарушения, предусмотренного [статьей 19.7 КоАП](#).

Верховный Суд РФ отметил, что [п. 2 ч. 2 ст. 22](#) комментируемого закона определяет, что оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных, полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом. В соответствии со [ст. 25](#) Федерального закона от 31 мая 2002 г. N 63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации" адвокатская деятельность осуществляется на основе соглашения между адвокатом и доверителем. Соглашение об оказании юридической помощи в коллегии адвокатов заключается между адвокатом и доверителем и регистрируется в документации коллегии адвокатов. Соглашение представляет собой гражданско-правовой договор на оказание юридической помощи самому доверителю или назначенному им лицу. Как следует из [п. 5 ч. 4 ст. 6](#) указанного федерального закона, адвокат не вправе разглашать сведения, сообщенные ему доверителем в связи с оказанием последнему юридической помощи, без согласия доверителя. Согласно [ст. 8](#) указанного федерального закона адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю. Вышеизложенное свидетельствует о том, что мировым судьей при рассмотрении настоящего дела об административном правонарушении не были учтены положения, предусмотренные [п. 2 ч. 2 ст. 22](#) комментируемого закона, позволяющие осуществлять обработку персональных данных без уведомления

уполномоченного органа по защите прав субъектов персональных данных. Именно на этом основании производство по делу было прекращено на основании [п. 2 ч. 1 ст. 24.5](#) КоАП.

Статья 22.1. Лица, ответственные за организацию обработки персональных данных в организациях

1. Комментируемая статья опирается в своем регулирующем воздействии на нормы [ч. 3 ст. 18.1](#) и [ст. 22](#) настоящего федерального закона. Совокупный анализ содержания этих норм в контексте [ч. 1](#) и [2](#) комментируемой статьи позволяет говорить о еще одной обязанности оператора персональных данных, который является коллективным субъектом права (юридическим лицом), - она заключается в необходимости назначения таким оператором лица, ответственного за организацию обработки персональных данных (сокращенно - ответственный).

В негосударственных организациях ответственный назначается локальным актом управления из числа ее работников либо организацией заключается соглашение с иным юридическим лицом или индивидуальным предпринимателем на оказание организации услуги юридического сопровождения обработки персональных данных. В отношении органов публичной власти требования императивны - руководитель органа индивидуальным актом управления назначает ответственного за организацию обработки персональных данных из числа государственных или муниципальных служащих и (или) работников указанного органа, замещающих должности, не являющиеся должностями государственной гражданской службы РФ или муниципальной службы, на основании трудового договора.

Независимо от формы организации и правового статуса ответственный подотчетен оператору персональных данных и получает указания от него.

2. Выполнение ответственным делегированных ему обязанностей требует непосредственного доступа к сведениям, подлежащим направлению в надзирающий орган государственной власти, - Роскомнадзор (см. комментарий к [ч. 3 ст. 9](#) и [ч. 3 ст. 22](#)). В связи с этим на оператора персональных данных [ч. 3](#) комментируемой статьи возлагается обязанность обеспечить ответственному доступ к подобным сведениям. Очевидно при этом, что, ознакомившись со сведениями конфиденциального характера в силу служебных или профессиональных обязанностей, ответственный несет ответственность за неправомерное разглашение такой информации.

3. [Часть 4](#) комментируемой статьи закрепляет непосредственные обязанности ответственного за организацию обработки персональных данных оператором - юридическим лицом:

1) Осуществляет внутренний контроль за соблюдением оператором и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных. Подобные требования нормативно закреплены в [постановлении](#) Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". Согласно [п. 3](#) Требований безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные, или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора. Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

Применяемые средства и способы защиты персональных данных обусловлены рисками, которые могут возникнуть в случае неправомерного доступа к этим данным. Согласно [п. 6](#) Требований под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия. Выделяются 3 типа угроз:

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.

Уровень угрозы для информационной системы конкретного оператора персональных данных обуславливает установление одного из четырех уровней защищенности персональных данных, при этом

условия и основания применения, а также требования к тому или иному уровню защищенности приведены в [пп. 9-16](#) Требований. Контроль за выполнением 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).

2) Доводит до сведения работников оператора положения законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных. Подобное информирование схоже с правовым просвещением, основание и формы применения которого определены в [ст. 18](#) Федерального закона от 23 июня 2016 г. N 182-ФЗ "Об основах системы профилактики правонарушений в Российской Федерации". Согласно данной норме доведение до сведения лиц и организации информации, направленной на обеспечение защиты прав и свобод человека и гражданина, общества и государства от противоправных посягательств, может быть реализовано путем применения различных мер образовательного, воспитательного, информационного, организационного или методического характера. В этом контексте ответственное за организацию обработки персональных данных лицо может выступать с соответствующими докладами (сообщениями) на общем собрании работников (служащих), осуществлять рассылку информации через корпоративный чат, размещать их на информационных стендах на территории организации, ее сайте или сайте профсоюзных организаций соответствующего профиля.

3) Организует прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов. Следует отметить, что наиболее удобно реализовывать данную функцию со стороны представителя кадрового подразделения юридического лица, через которое происходит набор и прием на работу (службу) претендентов.

Глава 5. Государственный 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. Комментируемая [статья](#) определяет правовой статус федерального органа исполнительной власти, осуществляющего функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных, - уполномоченного органа по защите прав субъектов персональных данных.

В соответствии с [постановлением](#) Правительства РФ от 16 марта 2009 г. N 228 таковым является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Роскомнадзор - федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере СМИ, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы. Роскомнадзор возглавляет руководитель, назначаемый на должность и освобождаемый от должности Правительством РФ по представлению Министра цифрового развития, связи и массовых коммуникаций РФ.

Структура Роскомнадзора включает центральный аппарат ведомства и 71 территориальный орган, сформированные в соответствии с административно-территориальным делением Российской Федерации. Система центрального аппарата Роскомнадзора обусловлена возложенными на Службу задачами и включает руководителя, 5 его заместителей и 10 структурных подразделений:

Управление организационной работы;

Административное управление;

Финансовое управление;

Управление разрешительной работы, контроля и надзора в сфере массовых коммуникаций;

Управление контроля и надзора в сфере электронных коммуникаций;

Управление разрешительной работы в сфере связи;

Управление контроля и надзора в сфере связи;

Управление по надзору в сфере информационных технологий;

Правовое управление;

Управление по защите прав субъектов персональных данных.

Последнее из названных подразделений является специализированным органом, реализующим

полномочия Роскомнадзора в сфере нормативного регулирования и реализации государственной политики в сфере персональных данных. [Положение](#) об Управлении по защите прав субъектов персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций утверждено [приказом](#) Роскомнадзора от 28 мая 2010 г. N 324, во втором разделе приложения за Управлением закреплено 51 полномочие, реализуемое самостоятельно или во взаимодействии с иными подразделениями Службы, иными органами государственной власти.

2. [Часть 1.1](#) комментируемой статьи определяет основную форму деятельности Роскомнадзора в части защиты прав субъектов персональных данных, - это государственный контроль и надзор за соответствием обработки персональных данных требованиям комментируемого закона и принятых в соответствии с ним нормативных правовых актов.

Законодательную основу государственного контроля и надзора на момент написания комментария образуют положения [Федерального закона](#) от 26 декабря 2008 г. N 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля", однако с 1 июля 2021 года ему на смену придет [Федеральный закон](#) от 31 июля 2020 г. N 248-ФЗ "О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации".

В [ч. 1 ст. 1](#) данного федерального закона дается определение государственного контроля (надзора) и муниципального контроля в Российской Федерации - это деятельность контрольных (надзорных) органов, направленная на предупреждение, выявление и пресечение нарушений обязательных требований, осуществляемая в пределах полномочий указанных органов посредством профилактики нарушений обязательных требований, оценки соблюдения гражданами и организациями обязательных требований, выявления их нарушений, принятия предусмотренных законодательством Российской Федерации мер по пресечению выявленных нарушений обязательных требований, устранению их последствий и (или) восстановлению правового положения, существовавшего до возникновения таких нарушений.

[Часть 2](#) той же статьи предусматривает, что государственный контроль (надзор), муниципальный контроль должны быть направлены на достижение общественно значимых результатов, связанных с минимизацией риска причинения вреда (ущерба) охраняемым законом ценностям, вызванного нарушениями обязательных требований. В соответствии с [п. 22 ч. 3 ст. 2](#) указанного нормативного акта его положения не применяются к организации и осуществлению государственного контроля и надзора за обработкой персональных данных, осуществляемые без взаимодействия с контролируемым лицом.

Помимо того, комментируемая [часть](#) содержит отсылку к положениям [постановления](#) Правительства РФ от 13 февраля 2019 г. N 146 "Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных". Согласно [п. 3](#) Правил государственный контроль и надзор включает в себя деятельность Роскомнадзора, направленную на предупреждение, выявление и пресечение нарушения операторами персональных данных требований комментируемого закона и принятых в соответствии с ним нормативных правовых актов посредством:

- а) организации и проведения плановых и внеплановых проверок;
- б) принятия мер по пресечению и (или) устранению последствий выявленных нарушений;
- в) проведения мероприятий по контролю без взаимодействия с операторами;
- г) проведения мероприятий по профилактике нарушений.

Плановые проверки в отношении операторов проводятся в соответствии с ежегодными планами деятельности органов Роскомнадзора, размещаемыми на их официальных сайтах в Интернет. Основанием для включения плановой проверки в отношении оператора в план по контролю является истечение 3 лет со дня:

государственной регистрации оператора в качестве юридического лица, индивидуального предпринимателя;

окончания последней плановой проверки оператора.

Плановая проверка в отношении оператора включается в план по контролю и проводится с периодичностью не чаще одного раза в 2 года со дня окончания его последней плановой проверки в следующих случаях:

а) оператор осуществляет обработку персональных данных в информационных системах персональных данных, имеющих в соответствии с федеральными законами статус государственных информационных систем;

б) оператор осуществляет сбор биометрических и специальных категорий персональных данных;

в) оператор осуществляет трансграничную передачу персональных данных на территорию иностранного государства, не обеспечивающего адекватную защиту прав субъектов персональных данных;

г) оператор осуществляет обработку персональных данных по поручению иностранного государственного органа, иностранного юридического лица, иностранного физического лица, которые не зарегистрированы в установленном порядке на территории Российской Федерации.

Внеплановые проверки проводятся на основании приказа органа по контролю и надзору, изданного:

1) в случае неисполнения или частичного исполнения оператором предписания об устранении выявленного нарушения, выданного органом по контролю и надзору;

2) по результатам рассмотрения обращений граждан, поступивших в орган по контролю и надзору, при условии наличия в обращении материалов, подтверждающих факт нарушения их прав, определенных [ст. 14-17](#) комментируемого закона, действиями (бездействием) оператора при обработке их персональных данных;

3) в соответствии с поручениями Президента РФ, Правительства РФ;

4) на основании требования прокурора об осуществлении внеплановой проверки;

5) на основании решения руководителя органа Роскомнадзора по итогам рассмотрения докладной записки, содержащей выводы о наличии нарушений требований, выявленных по результатам проведения мероприятий по контролю без взаимодействия с оператором.

3. [Часть 2](#) комментируемой статьи уполномочивает Роскомнадзор и его территориальные органы рассматривать обращения субъектов персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки с последующим принятием юридического решения. Правоотношения в сфере реализации права гражданина на обращение в государственные органы регулируются Федеральным законом от 2 мая 2006 г. N 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации". В [ст. 4](#) данного закона определены основные термины:

Обращение гражданина - направленные в государственный орган, орган местного самоуправления или должностному лицу в письменной форме или в форме электронного документа предложение, заявление или жалоба, а также устное обращение гражданина в государственный орган, орган местного самоуправления.

Предложение - рекомендация гражданина по совершенствованию законов и иных нормативных правовых актов, деятельности государственных органов и органов местного самоуправления, развитию общественных отношений, улучшению социально-экономической и иных сфер деятельности государства и общества.

Заявление - просьба гражданина о содействии в реализации его конституционных прав и свобод или конституционных прав и свобод других лиц, либо сообщение о нарушении законов и иных нормативных правовых актов, недостатках в работе государственных органов, органов местного самоуправления и должностных лиц, либо критика деятельности указанных органов и должностных лиц.

Жалоба - просьба гражданина о восстановлении или защите его нарушенных прав, свобод или законных интересов либо прав, свобод или законных интересов других лиц.

[Федеральным законом](#) предусмотрены следующие общие сроки регистрации и рассмотрения обращений граждан:

1) письменное обращение регистрируется в течение 3 дней с момента поступления;

2) если письменное обращение содержит вопросы, решение которых не входит в компетенцию адресата, оно в течение 7 дней со дня регистрации направляется компетентному органу или должностному лицу с уведомлением гражданина, направившего обращение;

3) ответы на запросы, направленные в связи с рассмотрением обращения, предоставляются в течение 15 дней с момента получения;

4) письменное обращение рассматривается в течение 30 дней со дня его регистрации;

5) срок рассмотрения обращения может быть продлен не более чем на 30 дней компетентным должностным лицом.

Прием, регистрация и разрешение поступивших обращений граждан осуществляется с учетом положений приказа Роскомнадзора от 31 марта 2014 г. N 49 "Об утверждении Инструкции по делопроизводству Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальных органов".

4. Основопологающее для защиты прав субъектов персональных данных значение имеют положения [ч. 3](#) комментируемой статьи, которыми определяются полномочия Роскомнадзора в рассматриваемой сфере.

Предоставленные Роскомнадзору права можно разделить на общие (присущие большинству органов государственной власти) и специальные (характерные преимущественно или исключительно для сферы защиты прав субъектов персональных данных).

К общим полномочиям следует отнести права:

а) запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

б) направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством РФ порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных (см. [ст. 20](#) Федерального закона от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности");

в) 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;

г) направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, сведения, указанные в [п. 7 ч. 3 ст. 22](#) комментируемого закона.

К общим полномочиям следует отнести и предусмотренное [ч. 5.1](#) комментируемой статьи право Роскомнадзора сотрудничать с органами, уполномоченными по защите прав субъектов персональных данных в иностранных государствах, в частности осуществлять международный обмен информацией о защите прав субъектов персональных данных, утверждать перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных.

Глобализация информационного оборота обуславливает особое внимание отечественного и зарубежного законодателя к вопросам организации взаимодействия уполномоченных национальных органов на международном уровне. Так, в Директиве ЕС о защите физических лиц при обработке персональных данных компетентными органами отмечается, что обеспечение согласованного и высокого уровня защиты персональных данных физических лиц и облегчение обмена персональных данных между компетентными органами государств-членов ЕС имеет решающее значение для обеспечения эффективного судебного сотрудничества по уголовным делам и полицейского сотрудничества. Исходя из этого уровень защиты прав и свобод физических лиц при обработке персональных данных компетентными органами в целях предотвращения, расследования, выявления или уголовного преследования преступлений или исполнения уголовных наказаний, включая защиту от угроз общественной безопасности и предотвращение таких угроз, должен быть эквивалентным во всех государствах-членах ЕС ([п. 7 преамбулы](#)).

Специальные полномочия Роскомнадзора возможно разделить по направленности на нормотворческие, надзорные, восстановительные и охранительные.

1) Нормотворческие полномочия реализуются Службой посредством внесения в Правительство РФ предложений о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных.

2) Надзорные полномочия применяются в порядке, описанном в [п. 2](#) комментария к настоящей статье, и выражаются в проверке сведений, содержащихся в уведомлении об обработке персональных данных, или привлечении для осуществления такой проверки иных государственных органов в пределах их полномочий.

3) Восстановительный потенциал усматривается в полномочиях:

требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

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.

4) Охранительная направленность усматривается в полномочиях Роскомнадзора, связанных с применением к операторам персональных данных мер государственного принуждения, в том числе, посредством:

ограничения доступа к информации, обрабатываемой с нарушением законодательства РФ в области персональных данных, в порядке, установленном законодательством РФ;

принятия меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований комментируемого Федерального закона;

привлечения к административной ответственности лиц, виновных в нарушении комментируемого [Федерального закона](#).

5. В [ч. 4, 5 и 7](#) комментируемой статьи закреплены обязанности органов Роскомнадзора:

1) защищать и обеспечивать конфиденциальность персональных данных, ставших известными

органу Роскомнадзора в ходе осуществления им своей служебной деятельности. Подобные сведения для должностных лиц рассматриваемого органа защищаются в режиме служебной тайны, их утрата или разглашение влечет дисциплинарную и административную ответственность по [ст. 13.14](#) "Разглашение информации с ограниченным доступом" КоАП;

2) организовывать в соответствии с требованиями настоящего федерального закона и других федеральных законов защиту прав субъектов персональных данных (см. [комментарий](#) к гл. 3);

3) 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 (см. [п. 3](#) комментария к настоящей статье);

4) вести реестр операторов. Подзаконной нормативной базой реализации данной обязанности выступают нормы [приказа](#) Роскомнадзора от 30 мая 2017 г. N 94 "Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения" (см. [комментарий](#) к ст. 22);

5) осуществлять меры, направленные на совершенствование защиты прав субъектов персональных данных;

6) принимать в установленном законодательством РФ порядке по представлению ФСБ, ФСО или ФСТЭК меры по приостановлению или прекращению обработки персональных данных;

7) информировать государственные органы, а также субъектов персональных данных по их обращениям или запросам о положении дел в области защиты прав субъектов персональных данных;

8) ежегодно направлять отчет о своей деятельности Президенту РФ, в Правительство РФ и Федеральное Собрание РФ, обеспечивать его опубликование в СМИ;

9) выполнять иные предусмотренные законодательством РФ обязанности.

Аналогичные полномочия закреплены в [ст. 46](#) Директивы ЕС о защите физических лиц при обработке персональных данных компетентными органами в отношении национальных органов, которые государства-члены ЕС создают для осуществления надзора за операторами персональных данных на соответствующей территории:

(a) контролировать и обеспечивать применение положений, принятых в соответствии с настоящей [Директивой](#) и имплементационными мерами;

(b) повышать уровень информированности общества и понимания рисков, норм, гарантий и прав в отношении обработки;

(c) консультировать в соответствии с законодательством государства-члена ЕС, национальный парламент, правительство и другие институты и органы о законодательных и административных мерах, связанных с защитой прав и свобод физических лиц при обработке их данных;

(d) повышать уровень информированности контролеров и обрабатывающих данные лиц относительно их обязанностей согласно настоящей [Директиве](#);

(e) по запросу предоставлять информацию любому субъекту данных относительно осуществления его прав согласно настоящей [Директиве](#) и, в соответствующих случаях, сотрудничать в связи с этим с надзорными органами других государств-членов ЕС;

(f) рассматривать жалобы, поданные субъектом данных или органом, организацией или объединением в соответствии со [ст. 55](#) настоящей Директивы, расследовать в соответствующих случаях предмет жалобы и в разумный срок информировать заявителя о ходе и результатах расследования, в частности, если необходимо дальнейшее расследование или сотрудничество с другим надзорным органом;

(g) проверять законность обработки в соответствии со ст. 17 настоящей Директивы и в разумный срок информировать субъекта данных о результатах проверки согласно [параграфу 3](#) указанной статьи или о причинах, по которым проверка не проводилась;

(h) сотрудничать с другими надзорными органами, включая обмен информацией и предоставление взаимной помощи, с тем чтобы гарантировать согласованное применение и исполнение настоящей [Директивы](#);

(i) проводить расследования относительно применения настоящей [Директивы](#), в том числе на основании информации, полученной от другого надзорного органа или органа государственной власти;

(j) проводить мониторинг соответствующих изменений, если они влияют на защиту персональных данных, в частности, разработки информационных и коммуникационных технологий;

Охранительные публично-правовые полномочия надзорного органа ("корректирующие") закреплены в [ст. 47](#) той же Директивы. Согласно данной норме каждое государство-член ЕС на законодательном уровне предусматривает, что каждый надзорный орган должен располагать следующими полномочиями:

(a) выдавать предупреждения контролеру или обрабатывающему данные лицу о том, что запланированная обработка данных может нарушать положения, принятые в соответствии с указанной

Директивой;

(b) требовать от контролера или обрабатывающего данные лица привести процесс обработки данных в соответствии с положениями, принятыми согласно настоящей **Директиве** при необходимости в установленном порядке и в установленный срок, в частности, потребовав исправления или удаления персональных данных или ограничения обработки согласно **ст. 16** указанной Директивы;

(c) наложить временное или окончательное ограничение на обработку данных, включая запрет обработки.

6. **Часть 6** комментируемой статьи содержит норму, повсеместно встречающуюся в определяющих правовой статус органов власти нормативных актах, согласно которой решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке. Законодательную основу этой деятельности образуют нормы **КАС** и **ГПК**. Не стоит также забывать, что принимаемые должностными лицами решения могут быть также обжалованы в административном порядке, например в соответствии с положениями **КоАП** или **Федерального закона** от 2 мая 2006 г. N 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации".

7. **Части 8 и 9** комментируемой статьи определяют внутриорганизационные основы деятельности органов Роскомнадзора по защите прав субъектов персональных данных:

финансирование Роскомнадзора и его территориальных органов, равно как и любого другого федерального органа государственной власти, осуществляется исключительно из федерального бюджета;

при Роскомнадзоре создается на общественных началах консультативный совет, задачи, полномочия, порядок работы и состав которого нормативно закреплены в приказах Роскомнадзора **от 29 января 2016 г. N 82** "О Консультативном совете при уполномоченном органе по защите прав субъектов персональных данных" и от 6 июля 2012 г. N 679 "Об утверждении состава Консультативного совета при уполномоченном органе по защите прав субъектов персональных данных".

Статья 24. Ответственность за нарушение требований настоящего Федерального закона

1. **Часть 1** комментируемой статьи закрепляет охранительную правовую норму, предполагающую привлечение к ответственности за нарушение настоящего федерального закона лиц, виновных в его нарушении.

Закрепленная норма носит отсылочный характер к специальным законодательным актам. Это означает, что комментируемый закон предусматривает обязательность привлечения к ответственности за неисполнение его положений. Сам же механизм ответственности, а точнее, подразумеваемые составы правонарушений и процедурные правила привлечения к ответственности за их совершение виновных лиц, устанавливаются иным законодательным актом. В данном случае имеются в виду составы правонарушений, предусмотренные **КоАП**, составы преступлений, предусмотренные **УК**, и дисциплинарные проступки, предусмотренные **ТК** и законами об отдельных видах государственной службы.

В **КоАП** содержатся следующие статьи, в соответствии с которыми можно квалифицировать действия (бездействия), нарушающие установленный комментируемым законом правовой режим персональных данных:

ст. 13.11 КоАП "Нарушение законодательства Российской Федерации в области персональных данных". Административная ответственность наступает при обработке персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработке, несовместимой с целями сбора персональных данных.

Привлечение к ответственности возможно в случае обработки персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством РФ в области персональных данных, если эти действия не содержат уголовно наказуемого деяния, либо осуществляется обработка персональных данных с нарушением установленных законодательством РФ в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных.

См. судебную практику по заявлениям об обжаловании актов о привлечении к административной ответственности по **ст. 13.11 КоАП**: **решение** Санкт-Петербургского городского суда от 5 марта 2020 г. N 7-358/2020 по делу N 12-962/2019; **постановление** Московского городского суда от 28 ноября 2019 г. N 4а-5085/2019; **определение** Московского городского суда от 8 ноября 2019 г. по делу N 7-13939/2019; **решение** Свердловского областного суда от 11 сентября 2018 г. по делу N 72-1000/2018;

ст. 13.14 КоАП "Разглашение информации с ограниченным доступом". Административная ответственность наступает 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.

См. судебную практику по заявлениям об обжаловании актов о привлечении к административной ответственности по [ст. 13.14 КоАП](#): [постановление](#) Московского городского суда от 27 июня 2019 г. N 4а-2598/2019; [постановление](#) Ивановского областного суда от 14 сентября 2018 г. N 4а-242/2018; [постановление](#) Пермского краевого суда от 15 октября 2019 г. по делу N 44а-1396/2019; [постановление](#) Кемеровского областного суда от 25 апреля 2018 г. по делу N 4А-468/2018.

В связи с применением положений комментируемого [закона](#), соблюдением установленных им правил и ограничений на практике нарушения могут быть квалифицированы и по иным статьям.

Так, например, [ст. 5.39 КоАП](#) в качестве состава правонарушения предусматривает неправомерный отказ в предоставлении гражданину, в том числе адвокату в связи с поступившим от него адвокатским запросом, и (или) организации информации, предоставление которой предусмотрено федеральными законами, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации.

[Статья 13.12 КоАП](#) предусматривает административное правонарушение в виде нарушения правил защиты информации. [Статья 13.13 КоАП](#) устанавливает ответственность за незаконную деятельность в области защиты информации, а [ст. 19.7 КоАП](#) - за непредставление сведений (информации).

В качестве уголовно-наказуемых деяний [УК](#) предусматривает следующие составы преступлений, затрагивающих правовой режим персональных данных:

[ст. 137 УК](#) - нарушение неприкосновенности частной жизни;

[ст. 140 УК](#) - отказ в предоставлении гражданину информации;

[ст. 272 УК](#) - неправомерный доступ к компьютерной информации.

В качестве мер административной и уголовной ответственности в данном случае подразумеваются санкции за совершение правонарушений и преступлений, указанных выше.

[Статья 90 ТК](#) устанавливает ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника: лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном ТК и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами. [Статья 192 ТК](#) регламентирует правила применения дисциплинарных взысканий.

ТК в качестве меры ответственности в сфере персональных данных предусматривает расторжение трудового договора по инициативе работодателя в случае разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника ([ст. 81](#)).

Систематизация и анализ судебной практики свидетельствует о немалом количестве нарушений настоящего федерального закона, влекущих привлечение к административной и уголовной ответственности в сфере защиты персональных данных (см., например: [решение](#) Санкт-Петербургского городского суда от 5 марта 2020 г. N 7-358/2020 по делу N 12-962/2019; [постановление](#) Московского городского суда от 28 ноября 2019 г. N 4а-5085/2019; [постановление](#) Московского городского суда от 28 ноября 2019 г. N 4а-5085/2019; [определение](#) Московского городского суда от 8 ноября 2019 г. по делу N 7-13939/2019; [решение](#) Свердловского областного суда от 11 сентября 2018 г. по делу N 72-1000/2018).

Распространение получили дела о взыскании морального вреда в связи с распространением персональных данных в сети Интернет в различных базах данных (см., например, [апелляционное определение](#) Алтайского краевого суда от 27 мая 2020 г. по делу N 33-2930/2020).

В каждом конкретном случае при обращении в суд с заявлением об обжаловании актов уполномоченных органов о привлечении к ответственности за нарушение законодательства о персональных данных необходимо соблюсти правило подведомственности рассмотрения дел судами, в противном случае суды откажут в принятии к рассмотрению заявления, и таких случаев в судебной практике также немало (см., например: [постановление](#) Арбитражного суда Северо-Западного округа от 20 февраля 2020 г. N Ф07-944/2020 по делу N А56-110762/2019; [постановление](#) Арбитражного суда Восточно-Сибирского округа от 29 августа 2018 г. N Ф02-3914/2018 г. по делу N А10-2117/2018; [постановление](#) Арбитражного суда Волго-Вятского округа от 27 августа 2018 г. N Ф01-3950/2018 по делу N А11-5722/2018).

Установление в законодательстве различных видов ответственности за нарушение правового

режима персональных данных как разновидности конфиденциальной информации - важная составляющая правовой политики Российской Федерации в сфере обращения информации, направленной на обеспечение законности в данной сфере, соблюдение информационных прав и свобод человека и гражданина, предотвращение злоупотреблений и правонарушений со стороны субъектов, владеющих информацией.

2. **Часть 2** комментируемой статьи предусматривает гражданско-правовую ответственность за нарушение настоящего федерального закона в виде возмещения морального вреда и возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

По сути, данная **статья** устанавливает для граждан гарантийный механизм взыскания убытков и компенсации морального вреда в связи с реализацией своего права на защиту информации - защиту персональных данных. Возмещение убытков и компенсация морального вреда являются способами защиты гражданских прав.

Материальная ответственность в сфере защиты персональных данных основывается на **ч. 2** комментируемой статьи, отсылающей к положениям ГК. Гражданско-правовая ответственность за нарушение правил, установленных комментируемым законом, базируется на **ст. 15, 24, 56, 151, гл. 25, гл. 59** ГК.

Ущерб, который может быть причинен в результате неправомерных действий в отношении персональных данных, довольно подробно охарактеризован в **п. 85 преамбулы** Регламента ЕС о защите персональных данных. В нем отмечается, что утечка персональных данных, если она не была вовремя и соответствующим образом устранена, может привести к физическому, материальному или нематериальному ущербу для физических лиц, например, потере контроля над персональными данными или ограничению прав, дискриминации, хищению персональных данных или мошенничеству с данными, финансовым потерям, несанкционированному отказу от псевдонимизации, ущербу репутации, нарушению конфиденциальности персональных данных, защищенных обязанностью соблюдать профессиональную тайну, или любому другому неблагоприятному экономическому или социальному положению для соответствующего лица (см. также **пп. 141-152 преамбулы** Регламента).

В Российской Федерации моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим федеральным законом, а также требований к защите персональных данных, установленных в соответствии с ним в иных актах (например, в **постановлении** Правительства от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"), подлежит возмещению в соответствии с законодательством Российской Федерации.

В данном случае подразумевается отсылка к положениям **ст. 151, 1099-1101** ГК. **Статьи 151, 1099** ГК закрепили общие положения о компенсации морального вреда, **ст. 1100** ГК - основания его компенсации, **ст. 1101** ГК - способ и размер компенсации. Применяются также нормы **ст. 1064** ГК об общих основаниях ответственности за причинение вреда.

Понятие морального вреда официально определено Верховным Судом РФ. Согласно **п. 2** постановления Пленума Верховного Суда РФ от 20 декабря 1994 г. N 10 под моральным вредом понимаются нравственные или физические страдания, причиненные действиями (бездействием), посягающими на принадлежащие гражданину от рождения или в силу закона нематериальные блага (жизнь, здоровье, достоинство личности, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна и т.п.), или нарушающими его личные неимущественные права (право на пользование своим именем, право авторства и другие неимущественные права в соответствии с законами об охране прав на результаты интеллектуальной деятельности) либо нарушающими имущественные права гражданина. В этом же акте Пленума Верховного Суда РФ подробно разъяснены процессуальные особенности рассмотрения судами дел о возмещении морального вреда.

Требования граждан относительно возмещения убытков и компенсации морального вреда, причиненных нарушением настоящего федерального закона в части защиты их персональных данных, подлежат рассмотрению в судах в порядке искового производства. К исковому производству в данном случае применимы как правила гражданского процесса, так и правила арбитражного процесса: в зависимости от того, кому, точнее - в связи с какой деятельностью, причинен вред, нанесен ущерб.

Если речь идет о возмещении убытков и компенсации морального вреда гражданину - индивидуальному предпринимателю в связи с его экономической деятельностью, то соответствующий иск подлежит рассмотрению в арбитражном суде в порядке арбитражного судопроизводства (на основе положений **АПК**). Такой иск связан с возникновением экономического спора. Во всех остальных случаях (не связанных с возникновением экономических споров) требования граждан относительно возмещения убытков и компенсации морального вреда в связи с нарушением правового режима их персональных данных подлежат рассмотрению судом в порядке гражданского судопроизводства - применяются

положения [ГПК](#).

С позиций судопроизводства также важно заметить, что при обращении граждан в суды с исками о возмещении убытков и компенсации морального вреда, причиненных нарушением прав в сфере персональных данных, правил их обработки, важно правильно составить исковое заявление как с содержательной точки зрения (привести веские доказательства нарушений прав граждан на защиту их персональных данных), так и с точки зрения правильного указания ответчика, указания заинтересованных лиц. Ответчиком по делам данных категорий выступает оператор персональных данных или иные лица, в ведении которых оказываются персональные данные, то есть субъекты, имеющие полномочия в части обработки и обеспечения сохранности персональных данных.

Анализируя официальную судебную доктрину рассмотрения судами дел о возмещении морального вреда (в частности, положения [постановления](#) Пленума Верховного Суда РФ от 20 декабря 1994 г. N 10), в ракурсе о рассмотрении судами споров в сфере защиты персональных данных и возмещения вреда, причиненного в связи с нарушением специального законодательства о персональных данных, отметим следующие моменты:

1) Моральный вред в сфере и в связи с нарушением законодательства о персональных данных может заключаться в нравственных переживаниях в связи с раскрытием семейной, врачебной тайны, распространением не соответствующих действительности сведений, порочащих честь, достоинство или деловую репутацию гражданина, временным ограничением или лишением каких-либо прав, в связи с заболеванием, перенесенным в результате нравственных страданий и др.

2) В каждом конкретном случае суду надлежит устанавливать следующие обстоятельства, получить ответы на следующие вопросы:

какие права субъекта персональных данных нарушены, какие нарушены правила обработки персональных данных, установленные законодательством, повлекшие в этой сфере причинение морального вреда;

в чем конкретно заключаются нравственные и (или) физические страдания субъекта персональных данных в связи с нарушением его прав и требований законодательства в области персональных данных;

какова степень тяжести нравственных и (или) физических страданий субъекта персональных данных, связанных с индивидуальными особенностями гражданина, которому причинен вред в связи с нарушением его прав и требований законодательства в сфере персональных данных. Удовлетворяя исковое требование о возмещении вреда, суды должны оценить его существенность для гражданина. При решении вопроса, является ли существенным вред, причиненный правам и охраняемым законом интересам гражданина, следует учитывать характер наступивших последствий, в том числе значимость морального вреда, размер материального ущерба, степень ущемления трудовых, личных неимущественных прав и интересов гражданина ([п. 4](#) постановления Пленума Верховного Суда СССР от 18 апреля 1986 г. N 9);

чем подтверждается факт причинения потерпевшему нравственных или физических страданий в виде морального вреда вследствие нарушения его прав, нарушения установленных законодательством правил обработки персональных данных;

действиями (бездействием) каких субъектов причинены нравственные и (или) физические страдания субъекту персональных данных; каковы полномочия этих субъектов в сфере персональных данных. Если полномочия, например, истребовать информацию, содержащую персональные данные, у субъекта имеются, то его действия законны, иск о возмещении вреда, причиненного предоставлением информации такому субъекту, не подлежит удовлетворению.

Пример: [постановлением](#) Пятнадцатого арбитражного апелляционного суда от 13 марта 2018 г. N 15АП-19317/2017 по делу N А53-26648/2017 в иске о признании незаконными действий судебного пристава-исполнителя по истребованию информации ограниченного доступа было отказано, поскольку судебные приставы наделены соответствующими правами на получение информации;

при каких обстоятельствах и какими действиями (бездействием) нравственные и (или) физические страдания субъекту персональных данных нанесены, степень вины причинителя, необходимо доказать факт нарушения права на защиту персональных данных. В противном случае иск не подлежит удовлетворению (см., например, [постановление](#) Седьмого арбитражного апелляционного суда от 26 февраля 2020 г. N 07АП-6458/2014(104) по делу N А67-874/2014);

в какой сумме субъект персональных данных оценивает компенсацию причиненных ему нравственных или физических страданий в виде морального вреда и др.

Другим словами, для принятия в каждом конкретном случае решения о компенсации морального вреда в сфере защиты персональных данных судам надлежит обстоятельно оценить все обстоятельства спора, в том числе наличие и подтверждение соответствующих полномочий у субъекта персональных данных, факт разглашения персональных данных как формы конфиденциальной информации,

последствия разглашения персональных данных третьим лицам, соблюдение субъектами персональных данных и иными лицами порядка (процедур) получения, оформления запросов на предоставления им требуемой информации с персональными данными и т.д.

Именно на данные моменты субъектам персональных данных надлежит обратить внимание при составлении документов для обращения в суд за защитой своих прав в сфере персональных данных, при обосновании своей позиции как участника процесса.

Так, если лицо, в ведении которого оказываются персональные данные, не уверено, что их запрашивает сам носитель персональных данных (персональные данные о самом себе), то оно и не обязано предоставлять эти персональные данные для ознакомления. Здесь имеются в виду случаи несоблюдения процедур обращения за получением персональных данных о себе (без подтверждающих личность письменных документов, обращения по почте, устно и т.д.), в случае обращения через представителя - без надлежаще оформленной доверенности.

Пример: согласно фактическим обстоятельствам дела, содержащимся в материалах [апелляционного определения](#) Ростовского областного суда от 23 ноября 2017 г. по делу N 33-19735/2017 по требованию об обязании предоставить информацию, взыскать компенсацию морального вреда, истец указал, что между ним и ООО был заключен договор займа, он направил заявление о предоставлении информации, касающейся обработки персональных данных, предоставленных в рамках договора займа, однако по истечении 30 дней с момента получения запроса ответчик письменный ответ не направил.

По выясненным обстоятельствам, истцом в адрес ответчика направлено заявление о предоставлении информации, касающейся обработки ее персональных данных, в котором он просил подтвердить факт обработки его персональных данных ООО, сообщить правовые основания и цели обработки его персональных данных; сообщить наименование и сведения о лицах, которые имеют доступ к его персональным данным или которые могут быть раскрыты на основании договора с банком; сообщить наименование или фамилию, имя, отчество лица, осуществляющего обработку персональных данных по поручению ООО. Кроме того, отдельным заявлением истец просил предоставить копию кредитного договора и реквизиты банка, которые были утеряны истцом. Обращение было отправлено по почте.

Суд отметил, что доказательств личного обращения истца к ответчику с предъявлением документа, удостоверяющего его личность или направлением нотариально удостоверенного заявления, не было представлено, в связи с чем каких-либо нарушений прав истца и злоупотребления своими правами со стороны ответчика не имеется. Поэтому решением суда в удовлетворении требования отказано. Суды вышестоящих инстанций это решение оставили в силе.

Заметим, что если требование о компенсации морального вреда вытекает из нарушения личных неимущественных прав и других нематериальных благ, то на него в силу [ст. 208 ГК](#) исковая давность не распространяется, кроме случаев, предусмотренных законом. В случае, когда требование о компенсации морального вреда вытекает из нарушения имущественных или иных прав, для защиты которых законом установлена исковая давность или срок обращения в суд, на такое требование распространяются сроки исковой давности или обращения в суд, установленные законом для защиты прав, нарушение которых повлекло причинение морального вреда ([п. 7](#) постановления Пленума Верховного Суда РФ от 20 декабря 1994 г. N 10). В сфере обращения персональных данных могут иметь место нарушения как личных неимущественных прав, так и имущественных или иных прав, в зависимости от того, о каких персональных данных и целях их обработки и распространения идет речь.

Размер компенсации морального вреда зависит от характера и объема причиненных истцу нравственных или физических страданий, степени вины ответчика в каждом конкретном случае, иных заслуживающих внимания обстоятельств, и не может быть поставлен в зависимость от размера удовлетворенного иска о возмещении материального вреда, убытков и других материальных требований. При определении размера компенсации вреда должны учитываться требования разумности и справедливости. Степень нравственных или физических страданий оценивается судом с учетом фактических обстоятельств причинения морального вреда, индивидуальных особенностей потерпевшего и других конкретных обстоятельств, свидетельствующих о тяжести перенесенных им страданий ([абз. 2 ст. 151 ГК](#), [п. 8](#) постановления Пленума Верховного Суда РФ от 20 декабря 1994 г. N 10).

Компенсация морального вреда осуществляется в денежной форме ([ч. 1 ст. 1101 ГК](#)).

Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Включение в настоящий федеральный закон положений о компенсации морального вреда - важный шаг в обеспечении и защите прав граждан, в том числе прав, относящихся к разряду информационных.

Как показывает систематизация и анализ рассмотренных судами дел о правовых спорах в сфере

защиты персональных данных, иски о взыскании морального вреда на основании комментируемой статьи получают все большее распространение (см., например: [апелляционное определение](#) Московского городского суда от 18 февраля 2020 г. N 33-6992/2020; [апелляционное определение](#) Московского городского суда от 12 февраля 2020 г. по делу N 33-5874/2020; [апелляционное определение](#) Московского городского суда от 24 января 2020 г. N 33-3179/2020; [апелляционное определение](#) Московского городского суда от 06 декабря 2019 г. по делу N 33-55352/2019; [апелляционное определение](#) Верховного суда Республики Карелия от 17 марта 2020 г. N 33-986/2020 по делу N 2-7912/2020; постановление Президиума Ленинградского областного суда от 9 июля 2019 г. N 44г-48/2019 по делу N 2-36/2018; [Апелляционное определение](#) Санкт-Петербургского городского суда от 26 марта 2019 г. N 33-4314/2019 по делу N 2-4433/2018; [апелляционное определение](#) Санкт-Петербургского городского суда от 17 декабря 2018 г. N 33-26356/2018 по делу N 2-1928/2018; Апелляционное определение Самарского областного суда от 17 октября 2019 г. N 33-12118/2019).

Исковые требования о компенсации морального вреда в связи с защитой правового режима персональных данных предъявляются не только как самостоятельные иски (см. [апелляционное определение](#) Московского городского суда от 24 января 2020 г. N 33-3179/2020), но и в дополнение к сформулированным исковым требованиям по иным основаниям взысканий, например, это иски:

о признании незаключенным договора займа, неправомерном распространении в связи с этим персональных данных (см. [апелляционное определение](#) Московского городского суда от 18 февраля 2020 г. N 33-6992/2020);

о признании информации запрещенной к распространению, включении электронного ресурса в единый реестр доменных имен, взыскании денежных средств (см. [апелляционное определение](#) Московского городского суда от 12 февраля 2020 г. по делу N 33-5874/2020);

о защите прав потребителей (см. [апелляционное определение](#) Московского городского суда от 16 января 2020 г. по делу N 33-451/2020);

о признании недействительным договора об обязательном пенсионном страховании, незаконными действий по обработке персональных данных, обязанности передать в ПФР средства пенсионных накоплений, уничтожить персональные данные, взыскании убытков, процентов за неправомерное пользование средствами пенсионных накоплений, компенсации морального вреда (см. [апелляционное определение](#) Верховного суда Республики Карелия от 17 марта 2020 г. N 33-986/2020 по делу N 2-7912/2020) и т.д.

Глава 6. Заключительные положения

Статья 25. Заключительные положения

1. Согласно [ст. 6](#) Федерального закона от 14 июня 1994 г. N 5-ФЗ "О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания" федеральные конституционные законы, федеральные законы, акты палат Федерального Собрания вступают в силу одновременно на всей территории Российской Федерации по истечении 10 дней после дня их официального опубликования. Исключения из общего порядка могут быть предусмотрены в самих законах или актах палат акты палат Федерального Собрания с указанием соответствующего порядка.

Комментируемый закон в настоящей [статье](#) определяет порядок вступления всех норм закона в силу одномоментно по истечении 180 дней после дня его официального опубликования.

Исходя из правовой позиции Конституционного Суда РФ, изложенной в [постановлении](#) от 24 октября 1996 г. N 17-П "По делу о проверке конституционности части первой статьи 2 Федерального закона от 7 марта 1996 года "О внесении изменений в Закон Российской Федерации "Об акцизах", днем официального опубликования закона является день его опубликования в Российской газете. Таким образом, днем официального опубликования комментируемого закона является 29 июля 2006 г., а датой вступления в силу - 26 января 2007 г.

2. [Часть 2](#) рассматриваемой статьи определила правило о том, что после дня вступления в силу настоящего федерального закона, то есть с 26 января 2007 г., обработка персональных данных, включенных в информационные системы персональных данных до дня его вступления в силу, осуществляется в соответствии комментируемым законом.

Вместе с тем [ч. 2.1](#) комментируемой статьи установила обязанность для операторов персональных данных, которые осуществляли обработку персональных данных до 1 июля 2011 г., представить в Роскомнадзор как в уполномоченный орган по защите прав субъектов персональных данных следующие сведения, установленные настоящим федеральным законом:

правовое основание обработки персональных данных;

Ф.И.О. физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ.

Пример: как следует из материалов дела, в период с 1 апреля 2016 г. по 28 апреля 2016 г. Роскомнадзор проводил проверку соответствия обработки персональных данных требованиям законодательства в области персональных данных в администрации муниципального образования "Город Астрахань".

По результатам данной проверки составлен акт и выдано предписание об устранении нарушений, в том числе - **ч. 2.1** комментируемой статьи. В уведомлении об обработке персональных данных отсутствовали сведения, которые необходимо было представить не позднее 1 января 2013 г. в уполномоченный орган, а именно - перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных.

Суд при рассмотрении дела пришел к выводу о нарушении администрацией **ч. 2.1** комментируемой статьи (см. [постановление](#) Двенадцатого арбитражного апелляционного суда от 23 ноября 2016 г. N 12АП-11071/2016 по делу N А06-5241/2016).

Указанная в рассматриваемой норме обязанность операторов должна была быть исполнена в срок не позднее 1 января 2013 г.

3. В силу **ч. 4** настоящей статьи на операторов, которые осуществляли обработку персональных данных до дня вступления в силу комментируемого закона и продолжили осуществлять такую обработку после дня его вступления в силу, возложена обязанность не позднее 1 января 2008 г. направить в Роскомнадзор уведомления об обработке (о намерении осуществлять обработку) персональных данных, за исключением случаев, предусмотренных настоящим федеральным законом.

В рамках реализации положений **ч. 3 ст. 22** комментируемого закона [приказом](#) Роскомнадзора от 16 июля 2010 г. N 482 были утверждены образцы [формы](#) уведомления об обработке персональных данных, а также [рекомендации](#) по заполнению образца формы уведомления.

О перечне оснований, по которым оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных, см. [комментарий](#) к ст. 22.

4. В рамках законодательного урегулирования отношений, возникающих в связи с присоединением с 1 июля 2012 г. к городу федерального значения Москве новых территорий ([постановление](#) Совета Федерации Федерального Собрания РФ от 27 декабря 2011 г. N 560-СФ "Об утверждении изменения границы между субъектами Российской Федерации городом федерального значения Москвой и Московской областью"), [Федеральным законом](#) от 5 апреля 2013 г. N 43-ФЗ комментируемая статья была дополнена **ч. 5**. В ней предусмотрены особенности правовой регламентации отношений, связанных с обработкой персональных данных, осуществляемой государственными органами, юридическими лицами, физическими лицами при предоставлении государственных и муниципальных услуг, исполнении государственных и муниципальных функций в субъекте РФ - городе федерального значения Москве.

Таким образом, регламентация указанных отношений должна происходить в рамках [Федерального закона](#) от 5 апреля 2013 г. 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" как специального закона, регламентирующего данные отношения. По всем другим аспектам регулирования приоритетом обладает комментируемый закон.

*(1) Подробнее см.: Разъяснения // Обработка и хранение персональных данных в РФ. Изменения с 1 сентября 2015 года // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: офиц. сайт. URL: <https://digital.gov.ru/ru/personaldata/> (дата обращения: 10.12.2020).

*(2) [Постановление](#) Правительства РФ от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

*(3) См.: Эрделевский А. Банковский вклад и права потребителей // Законность. 1998. N 4.

*(4) См.: Освещение частной жизни в СМИ / Авт.-сост. Г.Ю. Арапова, С.И. Кузеванова, М.А. Ледовских. 2-е изд., испр. и доп. Воронеж, 2010. С. 6.

*(5) См.: Ефремов А.А. Новые информационные технологии в практике Европейского суда по правам человека // Прецеденты Европейского суда по правам человека. 2016. № 6. С. 10-15.

*(6) См.: Грачева М.А. Защита права на уважение частной жизни в Европейском суде по правам человека // Вестник Московского университета МВД России. 2013. N 5. С. 135-140.

*(7) См.: Освещение частной жизни в СМИ / Авт.-сост. Г.Ю. Арапова, С.И. Кузеванова, М.А. Ледовских. 2-е изд., испр. и доп. Воронеж, 2010. С. 6.

*(8) Поскольку интересные с точки зрения российского законодательства дефиниции, данные в Регламенте о защите персональных данных и Директиве ЕС совпадают, в рамках комментария к ст. 3 будем далее проводить сравнительный анализ только с Регламентом о защите персональных данных.

*(9) URL: <https://82.rkn.gov.ru/directions/pers/p15374/> (дата обращения: 10.12.2020).

*(10) URL: <https://82.rkn.gov.ru/directions/pers/p15374/> (дата обращения: 10.12.2020).

*(11)

URL:

<https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/federalnyj-zakon-o-personalnykh-dannykh/chto-yavlyatsya-personalnymi-dannyimi-po-zakonu/> (дата обращения: 10.12.2020).

*(12) См.: Багаев В. Является ли IP-адрес персональными данными? URL: https://zakon.ru/blog/2010/12/1/yavlyatsya_li_ipadres_personalnymi_dannyimi (дата обращения: 10.12.2020).

*(13) Судебная практика по защите персональных данных. URL: <https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnykh-dannykh/sudebnaya-praktika-po-zashchite-personalnykh-dannykh/> (дата обращения: 10.12.2020).

*(14) URL: <https://82.rkn.gov.ru/directions/pers/p15374/> (дата обращения: 10.12.2020).

*(15) URL: <https://digital.gov.ru/ru/personaldata/> (дата обращения: 10.12.2020).

*(16) URL: <https://digital.gov.ru/ru/personaldata/> (дата обращения: 10.12.2020).

*(17)

URL:

https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf (дата обращения: 10.12.2020).

*(18) URL: <https://digital.gov.ru/ru/personaldata/> (дата обращения: 10.12.2020).

*(19) URL: http://rkn.gov.ru/docs/Otchet_ZPD_rus.pdf (дата обращения: 10.12.2020).

*(20) См.: Крюкова Д.Ю., Мокрецов Ю.В. Актуальные проблемы правового регулирования оборота и защиты персональных данных в России // Пенитенциарная наука. 2017. С. 34-38.

*(21) См.: URL: https://gdpr-text.com/ru/read/article-4/#comment_gdpr-a-004_1-02 (дата обращения: 10.12.2020).

*(22)

URL:

<http://iso27000.ru/chitalnyi-zai/zaschita-personalnykh-dannykh/federalnyi-zakon-obo-personalnykh-dannyhbb-i-deyatelnost-smi-problemy-proverki-narusheniya> (дата обращения: 10.12.2020).

*(23) Судебная практика по защите персональных данных. URL: <https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnykh-dannykh/sudebnaya-praktika-po-zashchite-personalnykh-dannykh/> (дата обращения: 10.12.2020).

*(24) URL: <https://77.rkn.gov.ru/p3852/p13239/p13309/> (дата обращения: 10.12.2020).

*(25) См.: Постановление Правительства РФ от 13 ноября 2019 N 1443 "О внесении изменения в Правила создания, формирования и ведения автоматизированной информационной системы "Реестр нарушителей прав субъектов персональных данных".

*(26) <https://bosfera.ru/bo/personalnye-dannye-instrukciya-po-primeneniyu-sudebnaya-praktika> (дата обращения: 10.12.2020).

*(27) <https://rtmtech.ru/articles/prestupleniya-v-sfere-kompyuternoj-informatsii-st-272-uk-rf/> (дата обращения: 10.12.2020).

*(28) <http://ukodeksrf.ru/ch-2/rzd-9/gl-28/st-272-uk-rf> (дата обращения: 10.12.2020).

*(29) URL: <https://www.advodom.ru/practice/cybercrime-5.php> (дата обращения: 10.12.2020).

*(30) См.: Сизов А.В. Квалификация нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети // Информационное право. 2007. N 4.

*(31) https://rkn.gov.ru/docs/Otchet_ZPD_rus.pdf (дата обращения: 10.12.2020).

*(32) Роскомнадзор разработал методологию обезличивания персональных данных. URL: <https://rkn.gov.ru/news/rsoc/news23181.htm> (дата обращения: 10.12.2020).

*(33) Роскомнадзор разработал методологию обезличивания персональных данных. URL: <https://rkn.gov.ru/news/rsoc/news23181.htm> (дата обращения: 10.12.2020).

*(34)

URL:

<https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/federalnyj-zakon-o-personalnykh-dannykh/>

yh-dannyh/chto-yavlyaetsya-personalnymi-dannymi-po-zakonu/ (дата обращения: 10.12.2020).

*(35) URL: <https://rkn.gov.ru/news/rsoc/news62380.htm> (дата обращения: 10.12.2020).

*(36) См.: Международная система защиты персональных данных. URL: <https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/mezhdunarodnaya-sistema-zashchity-personalnyh-dannyh/> (дата обращения: 10.12.2020).

*(37) См.: Осминин Б.И. Приоритетное применение международных договоров в национальной правовой системе: условия и последствия // *Журнал российского права*. 2017. N 12. С. 162.

*(38) См.: Исполинов А. Поправки в Конституцию и приоритет международного права: в поисках новой формулы. URL: https://zakon.ru/blog/2020/1/22/popravki_v_konstituciya_i_prioritet_mezhdunarodnogo_prava_v_poiskah_novoj_formuly (дата обращения: 10.12.2020).

*(39) URL: <https://sozd.duma.gov.ru/bill/744029-7> (дата обращения: 10.12.2020).

*(40) Модернизированная Конвенция Совета Европы предоставляет россиянам новые права в сфере защиты персональных данных. URL: <https://rkn.gov.ru/news/rsoc/news62380.htm> (дата обращения: 10.12.2020).

*(41) См.: Милушева Т.В. Принцип справедливости в контексте проблемы правового ограничения государственной власти // Принципы российского права: общетеоретический и отраслевой аспекты / Н.И. Матузов, А.В. Малько, К.А. Струсь и др.; под ред. Н.И. Матузов, А.В. Малько. Саратов, изд-во ГОУ ВПО "Саратовская государственная академия права", 2010. С. 215.

*(42) См.: Милушева Т.В. Принцип справедливости в контексте проблемы правового ограничения государственной власти // Принципы российского права: общетеоретический и отраслевой аспекты / Н.И. Матузов, А.В. Малько, К.А. Струсь и др.; под ред. Н.И. Матузов, А.В. Малько. Саратов, изд-во ГОУ ВПО "Саратовская государственная академия права", 2010. С. 202-203.

*(43) См. также: *указание* Банка России и ПАО "Ростелеком" от 9 июля 2018 г. N 4859-У/01/01/782-18 "О перечне угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 ФЗ "Об информации, информационных технологиях и о защите информации", в единой биометрической системе".

*(44) *Федеральный закон* от 4 июня 2018 г. N 125-ФЗ "О ратификации Договора между Российской Федерацией и Королевством Камбоджа о выдаче".

*(45) См. также: *постановление* Правительства от 31 июля 2017 г. N 913 "Об утверждении Правил представления юридическими лицами информации о своих бенефициарных владельцах и принятых мерах по установлению в отношении своих бенефициарных владельцев сведений, предусмотренных Федеральным законом "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма", по запросам уполномоченных органов государственной власти".

*(46) См.: Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону "О персональных данных". М.: Статут, 2017.

*(47) См.: Разъяснения Роскомнадзора "О вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки" // Экономика и жизнь (Бухгалтерское приложение). 2013. N 36.

*(48) *Приказ* МВД N 659, МЧС N 717, Министра обороны N 473, Минфина N 208н, Минюста N 209, Минтранса N 385, СВР N 63, ФСБ N 429, ФСО N 185, Росгвардии N 376, ГУСП N 145, Генпрокуратуры N 502, СК N 94 от 23 сентября 2020 г.

*(49) *Приказ* МВД России от 23 ноября 2017 г. N 882 "Вопросы эксплуатации программного обеспечения для реализации сервиса объединенной поисковой федеральной системы генетической идентификации "Ксенон-2".

*(50) Общие вопросы // Сайт Единой биометрической системы. URL: <https://bio.rt.ru/faq/project/> (дата обращения: 10.12.2020).

*(51) *Приказ* Роскомнадзора от 15 марта 2013 г. N 274 "Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных".

*(52) См.: Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С. Комментарий к Федеральному закону от 27.07.2006 N 152-ФЗ "О персональных данных" (постатейный). М., 2013; *Федеральный закон "О персональных данных": научно-практический комментарий (постатейный)* / А.Х. Гафурова, Е.В. Доротенко, Ю.Е. Контемиров и др.; под ред. А.А. Приезжевой. М.:

Редакция "Российской газеты", 2015. Вып. 11. 176 с.

*(53) См.: Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону "О персональных данных". М.: Статут, 2017. 320 с.

*(54) Подробнее см. на официальном сайте Мэра Москвы. URL: <https://www.mos.ru/karta-moskvicha/> (дата обращения: 10.12.2020).

*(55) **Определение** Конституционного Суда РФ от 10 июля 2003 г. N 287-О "Об отказе в принятии к рассмотрению жалобы гражданина Можнева Ивана Федоровича и коллективной жалобы граждан Гирдюк Татьяны Сергеевны, Маркеловой Людмилы Николаевны, Рашинской Галины Владимировны и других на нарушение их конституционных прав абзацем первым пункта 7 статьи 84 Налогового кодекса Российской Федерации".

*(56) Дело по заявлению об оспаривании действий Инспекции Министерства РФ по налогам и сборам по присвоению идентификационного номера налогоплательщика было направлено на новое рассмотрение в суд первой инстанции ввиду неправильного применения данным судом норм материального права, в частности присвоение физическому лицу без его согласия идентификационного номера налогоплательщика не нарушает свободу совести и вероисповедания либо иные конституционные права и свободы граждан: **определение** Верховного Суда РФ от 1 марта 2006 г. N 13-В05-13.

*(57) Распоряжение Правительства от 9 июня 2005 г. N 748-р "Об одобрении Концепции создания системы персонального учета населения Российской Федерации".

*(58) **Решение** Верховного Суда РФ от 29 мая 2012 г. N АКПИ12-645 "Об отказе в удовлетворении заявления о признании недействующим Постановления Правительства РФ от 28 ноября 2011 г. 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".

*(59) См.: Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С. Комментарий к Федеральному закону от 27.07.2006 N 152-ФЗ "О персональных данных" (постатейный). М., 2013.

*(60) Официальный сайт Роскомнадзора. URL: <https://15.rkn.gov.ru/p8880/p15987/> (дата обращения: 10.12.2020).

*(61) См.: **Апелляционное определение** Московского городского суда от 30 марта 2012 г. по делу N 11-2145; **апелляционное определение** Ростовского областного суда от 15 мая 2019 г. по делу N 33-8088/2019; **апелляционные определения** Московского городского суда от 10 июля 2015 г. по делу N 33-23164/2015.

*(62) Официальный сайт Роскомнадзора. URL: <https://rkn.gov.ru/news/rsoc/news51712.htm> (дата обращения: 10.12.2020).

*(63) См.: Скрипник Д.А. Обеспечение безопасности персональных данных: учебное пособие. М., Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. URL: <http://www.iprbookshop.ru/89449.html> (дата обращения: 10.12.2020).

*(64) См.: Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С. Комментарий к Федеральному закону от 27 июня 2006 г. N 152-ФЗ "О персональных данных" (постатейный). М., 2013.

*(65) См.: Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону "О персональных данных". М.: Статут, 2017.

*(66) См.: Базилевич А.В. защиты субъективных гражданских прав: автореферат дис. ... кандидата юридических наук / Казан. гос. ун-т. Ульяновск, 2001. 29 с.

*(67) См.: Жуйков В.М. Теоретические и практические проблемы конституционного права на судебную защиту: Дис. ... доктора юрид. наук. М., 1997. С. 4, 5.

*(68) Официальный сайт Роскомнадзора. URL: <https://rkn.gov.ru/treatments/p436/> (дата обращения: 10.12.2020).

*(69) См.: Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С. Комментарий к Федеральному закону от 27.07.2006 N 152-ФЗ "О персональных данных" (постатейный). М., 2013.

*(70) Итоги работы с обращениями граждан в Роскомнадзоре в 2019 году / Обращения граждан и юридических лиц // Официальный сайт Роскомнадзора. URL: <https://rkn.gov.ru/treatments/p436/> (дата обращения: 10.12.2020).

*(71) См.: Кухаренко Т.А., Захарова Н.А. Комментарий к Федеральному закону от 27 июля 2006 г. N 152-ФЗ "О персональных данных". М., 2016 г.

*(72) См., например: Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин

А.С. Комментарий к Федеральному закону от 27.07.2006 N 152-ФЗ "О персональных данных" (постатейный). М., 2013; Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону "О персональных данных". М.: Статут, 2017.

*(73) См.: Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С. Комментарий к Федеральному закону от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (постатейный). М., 2013.

*(74) См.: Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону "О персональных данных". М.: Статут, 2017.

*(75) См.: Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С. Комментарий к Федеральному закону от 27.07.2006 N 152-ФЗ "О персональных данных" (постатейный). М., 2013; Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону "О персональных данных". М.: Статут, 2017.

*(76) См.: Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону "О персональных данных". М.: Статут, 2017.

*(77) См.: Федеральный закон "О персональных данных": научно-практический комментарий (постатейный) / А.Х. Гафурова, Е.В. Доротенко, Ю.Е. Контемиров и др.; под ред. А.А. Приезжевой. М.: Редакция "Российской газеты", 2015. Вып. 11.

*(78) URL: <https://regulation.gov.ru/projects#npa=93621> (дата обращения: 10.12.2020).

*(79) URL: <https://rkn.gov.ru/personal-data/register> (дата обращения: 10.12.2020).

*(80) URL: https://rkn.gov.ru/docs/docP_2866.pdf (дата обращения: 10.12.2020).