

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт права

(наименование института полностью)

Кафедра

«Гражданское право и процесс»

(наименование)

40.04.01 Юриспруденция

(код и наименование направления подготовки)

Гражданское право и процесс

(направленность (профиль))

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)**

на тему

«Персональные данные как объект правовой охраны»

Обучающийся

И.Н. Новицкая

(Инициалы Фамилия)

(личная подпись)

Научный

руководитель

к.ю.н., Р.Ф. Вагапов

(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Оглавление

Введение	3
Глава 1 Общая характеристика понятия «персональные данные»	11
1.1 Понятие персональных данных	11
1.2 Категории персональных данных	20
Глава 2 Требования законодательства РФ к обработке персональных данных операторами и иными лицами, осуществляющими такую обработку	27
2.1 Принципы и условия обработки персональных данных	27
2.2 Права и обязанности лиц, участвующих в обработке персональных данных	33
Глава 3 Проблемы правового регулирования обработки персональных данных в Российской Федерации	43
3.1 Проблемы применения законодательства Российской Федерации в сфере персональных данных	44
3.2 Пути совершенствования законодательства в сфере обработки персональных данных	50
Заключение	61
Список литературы и используемых источников	65

Введение

Актуальность темы научно-исследовательской работы определена важностью обеспечения соблюдения прав, гарантированных гражданину Конституцией Российской Федерации, таких как право на неприкосновенность частной жизни, на личную и семейную тайну. В современном мире большинство коммуникаций происходят в цифровой области [50].

Государством и иными лицами создаются базы персональных данных, необходимые для реализации различных задач, ведь без этого их решение будет требовать гораздо больших затрат, как временных так и финансовых [5].

Учитывая тенденции развития современного общества, проблема защиты персональных данных становится все более актуальной. Это влечет за собой необходимость обеспечения надежной и эффективной защиты государством вышеуказанных конституционных прав человека [48, с. 114].

Российское законодательство о защите персональных данных постоянно претерпевает изменения и совершенствуется. Так, в 2022 году принят Федеральный закон № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности». Он внес важные изменения в положения Федерального закона № 152-ФЗ «О персональных данных».

Но даже несмотря на такие изменения в условиях цифровизации многих процессов нашей современной жизни граждане (субъекты персональных данных) продолжают сталкиваться с постоянными угрозами нарушения своих прав [49].

Несмотря на законодательно закрепленную за операторами персональных данных обязанность соблюдения принципов их обработки «на справедливой и законной основе», недопустимости обработки данных в случае их несоответствия цели обработки, а также недопустимости избыточной обработки данных по отношению к изначально заявленной цели их сбора, операторы персональных данных продолжают собирать все большие массивы

таких данных. Учитывая вышеизложенное, последствия так называемых утечек персональных данных наносят все больший как материальный, так и моральный вред субъектам, чьи данные оказались скомпрометированы. В связи с этим на сегодняшний день существует необходимость совершенствования законодательства, направленного на охрану персональных данных.

В то же время меры, направленные на обеспечение выполнения операторами персональных данных своих обязательств, лишь частично регламентированы законом. В остальной части операторам предоставлено право и самостоятельно устанавливать перечень и содержание таких мер. Это нередко влечет за собой бездействие операторов в вопросах обеспечения защиты персональных данных, а также создает угрозу конфиденциальности этих данных, покушения на нематериальные блага, принадлежащие гражданину [14].

Вопросы правового регулирования в сфере защиты прав граждан изучали многие авторы, например, такие как Голембиовская О.М., Кокурина М. А., Скрипник Д.А. и другие.

В монографии «Обеспечение безопасности персональных данных: формализация подходов» О. М. Голембиовская анализирует вопросы, связанные с оценкой уровней безопасности информационных баз данных, представляет средства защиты для разных уровней безопасности систем, содержащих персональные данные, а также предлагает метод определения степени ущерба для информационных систем, не обрабатывающих государственные сведения [6].

Работа Скрипник Д.А. «Обеспечение безопасности персональных данных» нацелена на разрешение вопросов основных понятий законодательства в сфере персональных данных, описывает категории персональных данных и этапы построения системы безопасной обработки этих данных [43].

Несмотря на многочисленные исследования в сфере обработки персональных данных полагаем, что определить способы решения проблемы обеспечения их безопасности и конфиденциальности, а также установить конкретные требования к деятельности операторов персональных данных в области их обработки, удалось не в полной мере.

В настоящем исследовании использовались формально-правовые методы – изучение правовой природы права человека на неприкосновенность частной жизни, защиту персональных данных; сравнительно-правовые – изучение и сравнение понятий и процессов, содержащихся и описываемых в различных нормативно-правовых актах в сфере обработки персональных данных в Российской Федерации.

Научная значимость результатов проведенного исследования заключается в потенциальном применении сделанных по его результатам выводов для совершенствования законодательства в сфере персональных данных.

Объектом исследования являются общественные отношения, связанные с обработкой персональных данных, возникающие в процессе реализации и охраны конституционного права человека и гражданина на неприкосновенность его частной жизни, личную и семейную тайну, защиты чести и достоинства.

Предметом исследования являются нормативно-правовые акты, регулирующие отношения, связанные с обработкой персональных данных, положения, определяющие понятия «персональные данные», «категории персональных данных», содержащие принципы и условия обработки личных данных, судебная практика по вопросам исследуемой темы.

Целью исследования является проведение анализа действующей нормативно-правовой базы в сфере обработки и защиты персональных данных, а также в подтверждении необходимости внесения изменений требований к такой обработке. Предполагается выявление актуальных проблем правового регулирования обработки персональных данных в Российской Федерации, поиск способов и путей совершенствования норм существующего законодательства в области обработки и эффективной защиты персональных данных.

Гипотеза исследования состоит в том, что механизм правового регулирования обработки персональных данных в Российской Федерации несовершенен и не обеспечивает в полной мере защиту их сохранности и конфиденциальности, что создает угрозу материальным и нематериальным благам, принадлежащим гражданину.

Для достижения поставленной цели необходимо решить следующие задачи:

1. изучение понятий «персональные данные», «категории персональных данных»;
2. анализ законодательных требований к обработке персональных данных операторами и иными задействованными в ней лицами;
3. выявление и анализ проблемных вопросов, связанных с практикой применения действующего законодательства Российской Федерации в области персональных данных;
4. предложение путей совершенствования действующего законодательства в сфере персональных данных.

Теоретико-методологическую основу исследования составили работы следующих авторов: Голембиовская О. М., Касаткин А. А., Кокурина М. А., Комаров С.А., Новиков Р.В., Платонова Н. И., Савин М. П., Скрипник Д. А. и других, Конституция Российской Федерации, Гражданский Кодекс Российской Федерации, Федеральный закон № 152-ФЗ «О персональных данных», Кодекс Российской Федерации об административных правонарушениях и другие нормативно-правовые акты, существующая судебная практика.

Опытно-экспериментальной базой исследования являются результаты изучения правоприменительной практики в сфере защиты прав субъектов персональных данных.

Научная новизна исследования заключается в проведении комплексного исследования правового регулирования обработки персональных данных в Российской Федерации.

Теоретическая и практическая значимость исследования заключается в расширении научных представлений о механизмах совершенствования законодательства Российской Федерации в сфере персональных данных.

Достоверность и обоснованность результатов настоящего исследования обеспечивались применением нормативно-правовых актов Российской Федерации в сфере персональных данных, многосторонним анализом судебной практики, работ отечественных и зарубежных авторов.

Личное участие автора в организации и проведении исследования состоит в самостоятельной подготовке, изучении и обобщении материала и написании текста магистерской диссертации.

Апробация и внедрение результатов работы велись в течение всего исследования и выразились в публикации статьи на тему исследования, в которой нашли отражение теоретические положения, выводы, практические предложения и рекомендации, содержащиеся в нем.

На защиту выносятся следующие положения:

1. Необходимость закрепления на законодательном уровне перечня мер, обязательных к принятию операторами в целях соблюдения требований Федерального закона № 152-ФЗ «О персональных данных». В законе отсутствует развернутый перечень обязательных для издания локальных актов для операторов, не являющихся государственными или муниципальными органами власти. Отсутствие списка обязательных контрольных вопросов, подлежащих проверке при проведении внутреннего контроля за обработкой персональных данных, а также относительно невысокие штрафы за допущенные нарушения влекут недостаточно внимательное отношение операторов к исполнению требований законодательства, что в свою очередь может явиться причиной нарушения прав субъектов персональных данных. Также на сегодняшний день не разработана методика проведения процедуры обезличивания персональных данных для операторов, не являющихся органами власти. Отсутствие четкого перечня мер, необходимых к принятию операторами персональных данных для соблюдения обязательных требований приводит к бездействию операторов в вопросах защиты персональных данных и создает угрозу нарушения прав человека, охраняемых гражданским законодательством.

2. Целесообразность разработки инструмента для создания политики оператора в отношении обработки персональных данных. Его реализация, по нашему мнению, способствовала бы корректному составлению такого документа и помогла бы избежать несоответствия документа законодательно закрепленной структуре. Полагаем, что создание «конструктора» политики

исключило бы неправильное толкование операторами норм пункта 2 части 1 статьи 18.1 закона о персональных данных, что в свою очередь способствовало бы более корректному содержанию указанного документа. Полнота представленных в политике сведений делает деятельность оператора по обработке персональных данных более прозрачной и понятной для граждан, что в дальнейшем упрощает для них процесс защиты своих прав в случае их нарушения.

3. Необходимость определения требований к структуре любого согласия на обработку персональных данных. Полагаем, что в содержание любого согласия необходимо включать цель обработки персональных данных, их перечень, перечень действий с ними, сведения об операторе с указанием его реквизитов, способ отзыва согласия, соответствующий способу его дачи, а также срок его действия, исключающий указание о бессрочной обработке. Ведь часто согласия, размещаемые на интернет-сайтах или подлежащие подписанию иными способами, не содержат необходимых сведений, что делает практически невозможным для субъекта их отзыв. Отсутствие в законе четких требований к структуре согласия на обработку персональных данных приводит к некорректному составлению текстов таких документов операторами в нарушение требований, указанных в части 1 статьи 9 закона о персональных данных. Часто разработанные операторами шаблоны этих документов не отвечают критериям конкретности, предметности, информированности, сознательности и однозначности. А подписание таких согласий создает сложности доказывания вины оператора при реализации права гражданина на защиту своих прав в судебном порядке, взыскание компенсации морального ущерба.

4. Действующие требования к ведению интернет-сайтов, посредством которых производится обработка персональных данных, недостаточны. Зачастую эти сайты не содержат реквизитов операторов, обрабатывающих персональные данные посетителей интернет-ресурса. Считаем важным ввести обязанность размещения на таких сайтах сведений об операторе персональных данных с указанием его реквизитов. Ведь отсутствие этих сведений на сайте

может привести к нарушению прав субъекта персональных данных, в том числе предусмотренных статьями 14, 10.1 профильного закона.

5. Положения статьи 10.1 Федерального закона № 152-ФЗ «О персональных данных», в том числе связанные с правовыми основаниями распространения персональных данных, требуют корректировок. Шаблон согласия на обработку персональных данных, разрешенных для распространения, не дает операторам возможности производить распространение способами, отличными от распространения на собственном интернет-ресурсе, что затрудняет исполнение указанной нормы.

Кроме того полагаем, что список исключений, предусмотренных частью 15 статьи 10.1. Закона не является достаточно полным. Положения статьи 10.1 закона не применяются, в случае если обработка персональных данных производится в целях выполнения возложенных законодательством Российской Федерации на государственные и муниципальные органы власти, а также на подведомственные таким органам организации функций, полномочий и обязанностей. Но существуют нормы, которые обязывают и иные виды организаций распространять персональные данные. Например, частные медицинские организации, имеющие лицензию на осуществление медицинской деятельности, как и государственные, обязаны информировать пациентов о медицинском персонале, их уровне образования и квалификации. В то же время требования статьи 10.1 делают исключение только для организаций, подведомственных государственному или муниципальному органу власти. Следовательно, на иных лиц, обязанных распространять персональные данные в соответствии с законом, возлагается обязанность соблюдения норм, прописанных в статье 10.1. Из этого следует, что таким лицам необходимо получить со своих работников соответствующее согласие при наличии законодательно возложенной на оператора обязанности публикации данных.

6. Целесообразность введения требований к квалификации лиц, ответственных за организацию обработки персональных данных. Нарушения прав субъектов в большинстве случаев связаны с ненадлежащим контролем со стороны операторов за процессом обработки персональных данных, что

является следствием их низкой осведомленности в данном вопросе. Законодательно не установлены требования к квалификации лиц, ответственных за организацию обработки персональных данных. Назначение таких лиц нередко производится формально, что недопустимо в условиях постоянного роста количества утечек личных данных. Для крупных операторов может быть установлена обязательная аккредитация их деятельности в области обработки персональных данных. Это, по нашему мнению, является важной мерой для предотвращения незаконного оборота персональной информации, неразрывно связанной с правом граждан на неприкосновенность частной жизни.

Глава 1 Общая характеристика понятия «персональные данные»

1.1 Понятие персональных данных

В соответствии со статьей 23 Конституции Российской Федерации каждому гражданину гарантировано право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения» [13].

Собирать, хранить, использовать и распространять сведения о частной жизни лица без его согласия запрещено Конституцией. Нематериальные блага, принадлежащие гражданину, защищаются в соответствии с Гражданским Кодексом Российской Федерации и другими законами. Перечень этих благ не является исчерпывающим.

Термин «персональные данные» впервые он появился в отечественном законодательстве в середине 1990-х годов. Указом Президента Российской Федерации № 188 6 марта 1997 года утвержден «Перечень сведений конфиденциального характера», пунктом 1 которого было определено, что персональные данные – «это сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях» [22].

В декабре 2005 года Россией ратифицирована «Конвенция о защите физических лиц при автоматизированной обработке персональных данных», в соответствии с которой персональные данные определены как любая информация об определенном или поддающемся определению физическом лице (субъекте персональных данных) [17].

27 июля в 2006 году принят Федеральный закон № 152-ФЗ «О персональных данных».

«Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)» [16].

Как следует из указанного понятия с помощью таких сведений лицо можно определить, то есть идентифицировать. В качестве примера можно привести внешний вид субъекта. Так, если назвать из числа слушателей лекции лицо, сидящее в первом ряду и одетое в темно-синий костюм в клетку, остальные слушатели исходя из ситуации, поймут, о ком идет речь. То есть этот объем данных в конкретной ситуации позволит идентифицировать субъекта.

Однако возможность идентификации - это необязательное условие отнесение данных к персональным. Информация может иметь отношение к ее владельцу, но определить его личность с ее помощью не всегда будет возможно, хотя при этом она будет с ним неразрывно связана. Например, рост и вес конкретного человека – это его личные данные. Уровень образования, квалификация, ученая степень – все это сведения, относящиеся к субъекту. В то же время идентифицировать лицо исключительно по этим данным невозможно.

Очевидно, что номер паспорта – персональные данные. При этом определить конкретное лицо только на основании него без наличия доступа к специальным информационным базам данных весьма проблематично. Также невозможно идентифицировать лицо исключительно по его фамилии и инициалам, в то же время указанный объём данных признается персональными данными их владельца.

Как видно из вышеуказанных примеров, понятие «персональные данные» является достаточно неопределенным и может интерпретироваться по-разному в зависимости от контекста и ситуации.

На законодательном уровне отсутствует четкий перечень данных, которые могут расцениваться как персональные, что неизбежно создает определенные трудности для операторов персональных данных в исполнении требований действующих нормативно-правовых актов.

Как упомянуто выше, возможность отнесения данных к персональным может зависеть от контекста их использования.

Интересна сложившаяся практика по отнесению телефонного номера к персональным данным. Так, в соответствии с пунктом 2 правил оказания услуг телефонной связи, утвержденных постановлением Правительства Российской Федерации от 24 января 2024 года № 59 «О порядке оказания услуг телефонной связи» (далее – Правила), абонентский номер – это телефонный номер, однозначно определяющий (идентифицирующий) конечный элемент сети связи или подключенную к сети подвижной связи абонентскую станцию (абонентское устройство) с установленным в ней (в нем) идентификационным модулем [34].

В Правилах закреплено, что к пользовательскому (оконечному) оборудованию относится информация, связанная с местным, междугородним, международным телефонными соединениями. Согласно Федеральному закону от 07.07.2003 № 126-ФЗ «О связи» абонентский номер (номер телефона) – это выделяемая абоненту при заключении договора об оказании услуг телефонной связи совокупность цифровых знаков, служащих для обозначения и возможности идентификации конечного оборудования абонента в сети связи при соединении с ним абонентских устройств [18].

Из вышеуказанного понятия следует, что номер телефона без дополнительных сведений об абоненте, таких как фамилия, имя и отчество владельца не является его личными данными. То есть номер телефона – средство оказания услуг связи.

В соответствии с Гражданским кодексом Российской Федерации к персональным данным можно отнести имя гражданина, его фамилию, отчество (при наличии), место его жительства, а также иные данные, позволяющие относящиеся к конкретному человеку [7].

Выше обозначенный вывод подтвердил в своем решении по делу № 33-2984/17 Курганский областной суд (апелляционная инстанция) [2].

Так, истец сообщил, что на его личный номер телефона поступил звонок. Истец заявил, что совершив звонок, организация произвела обработку его персональных данных, настаивал на том, что номер его мобильного телефона является его личными данными в связи с тем, что принадлежит ему на основании договора с оператором связи и, следовательно, относится к нему как

к прямо определенному физическому лицу. Однако суд постановил, что номер телефона без указания сведений о его владельце, представляет собой обезличенную информацию, состоящую из набора цифр, который сам по себе личными данными не является. Суд отказал истцу в удовлетворении его требований.

Московский городской суд по результатам рассмотрения дела также постановил, что телефонный номер является средством передачи данных и звонков [3].

Однако существуют и иные судебные решения, например, по делу, рассмотренному мировым судьей в 2019 году (№ 12-973/19). Суть жалобы лица, обратившегося в суд за защитой своих прав, состояла в том, что гражданину стали поступать звонки от неизвестной ему организации, должником которой он не являлся. По результатам проведенной проверки было установлено, что номер телефона истца обрабатывался организацией-оператором как телефон должника, в связи с чем истцу периодически поступали звонки по вопросу задолженности третьего лица. В процессе осуществления взаимодействия истец неоднократно пояснял организации-кредитору, что не имеет сведений о должнике и его местонахождении.

По результатам рассмотрения дела суд установил, что персональные данные истца, а именно номер его мобильного телефона, обрабатывались организацией-оператором в нарушение принципов, заложенных в статье 5 закона о персональных данных.

Согласно статьи 151 Гражданского Кодекса Российской Федерации «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 нарушителя обязанность денежной компенсации указанного вреда. При определении размеров компенсации морального вреда суд принимает во внимание степень вины нарушителя и иные заслуживающие внимания обстоятельства» [7].

Неоднородность судебных решений по административным делам в части определения вины оператора, связанная с отсутствием в законодательстве четкого перечня персональных данных, создает сложности их защиты, в том числе доказывания причинения морального вреда владельцу этих данных, равно как и факта самого правонарушения.

Прямо противоположная позиция сложилась по вопросу отнесения к персональным данным фотографий и видеоизображений граждан [42].

Так, изображение гражданина без указания дополнительной информации является его персональными данными. Это подтверждается, в том числе, решением мирового судьи судебного участка ЗАТО г. Заозерска Кольского судебного района Мурманской области, которым было рассмотрено дело № 5-84/2023.

Судье поступил протокол, оставленный по результатам рассмотрения территориальным органом Роскомнадзора материалов, поступивших из правоохранительных органов. Надзорный орган пришел к выводу о нарушении прав несовершеннолетнего лица как владельца персональных данных.

Согласно материалам дела, фотографии несовершеннолетнего были размещены в социальной сети «ВКонтакте» на личной странице третьего лица. Фотографии были доступны для просмотра неограниченному кругу лиц. При этом согласие законного представителя несовершеннолетнего у нарушителя отсутствовало. Сам законный представитель против размещения фотографий своего ребенка в сети Интернет возражал, в связи с чем обратился за защитой его прав в правоохранительные органы.

Правовых оснований распространения фотографий несовершеннолетнего нарушитель представить не смог, представленные нарушителем пояснения оказались несостоятельными, в связи с чем в отношении него был составлен административный протокол. Суд поддержал позицию надзорного органа и признал лицо, разместившее фотографию ребенка на своей странице, виновным. Нарушителю назначен административный штраф [32].

Охрана изображения гражданина регулируется прежде всего Гражданским Кодексом Российской Федерации, но также и законом о персональных данных. Незаконное использование изображения гражданина

часто влечет за собой не только нарушение его прав как субъекта персональных данных, но и создает угрозу его чести, достоинству [44].

Еще одним примером обработки персональных данных является обработка данных посетителей интернет-сайтов. Все чаще на сайтах устанавливаются метрические программы. Они позволяют собрать статистику посещаемости сайта, понять, какие лица им интересуются, определить их пол, возраст, а также устройство, которым пользуется посетитель сайта, страну его местонахождения, используемый браузер. Эти данные помогают сформировать сведения о поведении посетителя на сайте, его предпочтениях, что может определенным образом характеризовать это лицо [51].

В соответствии с пунктом 18 Условий использования сервиса Яндекс.Метрика и AppMetrica все данные, собираемые и хранимые сервисом, Яндекс рассматривает как конфиденциальную информацию пользователя и его персональные данные. Исходя из положений закона о персональных данных к таким сведениям относится любая информация, имеющая отношение к прямо или косвенно определённом или определяемому физическому лицу (владельцу персональных данных).

Следовательно, данные, собираемые посредством метрических сервисов, относятся к персональным данным пользователей сайта. С этой позицией согласился судья Московского городского суда при рассмотрении дела № 33-38783/2016 [27].

Такую же позицию занял Таганский районный суд г. Москвы по делу № 02-4261/2018, который указал в своем решении, что использование метрических программ, в том числе Яндекс.Метрика, Google Analytics, предназначенных для оценки посещаемости интернет-сайтов, «представляет собой действия по сбору и обработке персональных данных» [39].

Но следует отметить, что отнесение сведений, собранных с помощью метрических программ, к личным данным, к которым в свою очередь применяются общие принципы и требования их обработки, значительно затрудняет выполнение обязательных требований. Субъект имеет право на получение информации, касающейся обработки его персональных данных.

Данная информация должна включать, среди прочего, подтверждение факта обработки персональных данных, ее сроки и иные данные.

Организации обязаны разработать внутренние нормативные акты в отношении их деятельности по обработке персональных данных. Эти документы должны определять «для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований» [16].

Акт об уничтожении данных должен содержать сведения об их владельце. Это следует из приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении требований к подтверждению уничтожения персональных данных» [24].

Но лицо, производящее сбор персональных данных посетителей сайта, не всегда может определить, кому именно принадлежат те данные, которые собрал метрический сервис. Как правило, установить, какое именно лицо посещало тот или иной сайт невозможно без наличия необходимых ресурсов, технических и интеллектуальных. В правоохранительных органах такие задачи решают сотрудники бюро специальных технических мероприятий. Подавляющее большинство операторов не могут сопоставить сведения, собираемые посредством метрических программ с определенными посетителями сайта.

Возникают вопросы, как выделить конкретные данные для их уничтожения по истечению сроков хранения в связи с применением к данной категории персональных данных общих требований к их обработке. Кроме того существуют сложности доказывания субъектом принадлежности ему данных, собранных посредством метрических программ, в случае если субъект полагает, что его права, предусмотренные частью 7 статьи 14 профильного закона или иными его нормами, нарушены оператором.

Вышеупомянутые сервисы действительно собирают достаточный объём информации о посетителях сайта, которая в дальнейшем используется

оператором в своих интересах. Например, сведения о предпочтениях посетителя сайта могут быть использованы в рекламных целях. Гражданину начинают поступать навязчивые предложения от организаций, чьи сайты он посещал [40].

Нередко они доставляют гражданину немалые неудобства, особенно, если такие предложения направляются с использованием телефонной связи. Однако при обращении к оператору с целью получения информации о порядке обработки его персональных данных субъект фактически лишен возможности ее получить. Таким образом, данные, полученные с помощью метрических сервисов, однозначно имеют отношение к субъекту и являются его персональными данными [33].

В то же время применение к ним общих требований к обработке затрудняют реализацию операторами своих обязанностей, а субъектами - своих прав.

В соответствии со статьей 152.2 Гражданского кодекса Российской Федерации, «если иное прямо не предусмотрено законом, не допускается без согласия гражданина сбор, хранение, распространение и использование любой информации о его частной жизни, в частности сведений о его происхождении, о месте его пребывания или жительства, о личной и семейной жизни» [7].

В то же время в соответствии с действующим приказом МВД России № 984 от 31.12.2017 «наименование субъекта Российской Федерации, наименование населенного пункта, улицы, номера дома, квартиры» является адресом места жительства, что подпадает под понятие «персональные данные».

Однако судебная практика по вопросам отнесения адреса к персональным данным также неоднозначна, что подтверждается, в частности, решением судьи Московского районного суда г. Твери Тверской области, рассмотревшего дело № 12-24/2016. Так, истец сообщил, что получил по своему адресу письмо, содержащее требование устранить задолженность по оплате жилищно-коммунальных услуг. Истец настаивал на том, что данные о его адресе и сумме задолженности позволяют персонализировать физическое лицо по месту жительства, в связи с чем считал их обработку нарушающей его права как субъекта персональных данных. В то же время суд с позицией истца не

согласился, решив, что указанный объем данных, а именно адрес и сумма задолженности не позволяет отнести их к персональным данным, что не соотносится с вышеуказанным приказом МВД России [35].

Адрес не всегда является личной информацией проживающего по нему гражданина. Например, этот адрес может обрабатываться оператором как адрес доставки товара или адрес оказания услуги. Так, Подпорожским городским судом Ленинградской области рассмотрено дело № 2-335/2020, по результатам которого истцу было отказано в удовлетворении требования компенсации морального вреда. Судья установил, что «в рамках агентского договора № от 17 сентября 2014 года ответчик передал ООО «Агентство Р.О.С.долгЪ» сведения о номере лицевого счета, адресе, по которому образовалась задолженность, а также размере задолженности. При этом личные данные должника, к которым относятся в первую очередь, фамилия, имя, отчество должника, дата и место рождения и другие, позволяющие однозначно идентифицировать должника, ответчиком в адрес ООО «Агентство Р.О.С.долгЪ» не передавались» [38].

Роскомнадзор считает, что указание в списке должников по оплате коммунальных услуг сведений в объеме «номер квартиры» и «сумма задолженности» не является противозаконным. Данная позиция подкрепляется судебной практикой, в том числе, с такой позицией согласился Свердловский областной суд при рассмотрении дела № 33-15137/2019 [4].

Так, истец обратился в суд, полагая, что размещение в свободном доступе сведений об адресе принадлежащего ему жилого помещения и о сумме задолженности за коммунальные услуги нарушает его права как субъекта персональных данных, просил взыскать с ответчика компенсацию причиненного истцу морального вреда незаконной обработкой его персональных данных. Однако суд не счел указанный объем сведений достаточным для его отнесения к данным истца и отказал в компенсации морального вреда.

Учитывая вышеизложенные примеры, полагаем, что термин «персональные данные» не обладает достаточной ясностью и конкретностью. Он имеет максимально широкую характеристику. Это приводит к затруднениям в определении того, какая именно информация является персональными

данными, и, следовательно, должна обрабатываться с учетом требований законодательства в указанной сфере. Отсутствие четкого перечня персональных данных в законодательстве приводит к различным интерпретациям этого термина, увеличивает риск нарушения операторами обязательных норм в сфере обработки персональных данных. Неопределенность самого понятия «персональные данные» способствует неоднозначности судебной практики, что существенно усложняет процесс доказывания причинения морального вреда владельцам персональных данных.

1.2 Категории персональных данных

Статьей 4 закона о персональных данных определено, что законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из настоящего Федерального закона и других определяющих случаи и особенности обработки персональных данных федеральных законов. На основании и во исполнение федеральных законов государственные органы, Банк России, органы местного самоуправления в пределах своих полномочий могут принимать нормативные правовые акты, нормативные акты, правовые акты (далее - нормативные правовые акты) по отдельным вопросам, касающимся обработки персональных данных [16].

Термин «категории персональных данных» неоднократно упоминается в законодательстве.

Организации обязаны разработать документы, определяющие «политику оператора в отношении обработки персональных данных» [16].

Эти документы должны определять «для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки» [16].

Операторы должны «уведомить уполномоченный орган об обработке (о намерении обрабатывать) персональных данных» [16].

В документе необходимо указывать категории обрабатываемых данных.

В законе упоминаются такие категории данных как биометрические и специальные. Правила их обработки определены соответствующими статьями закона. Общие условия обработки персональных данных указаны в статье 6 [46].

Информация о «расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни» была отнесена регулятором к специальной категории персональных данных [16].

Требования к их обработке установлены в статье 10 закона. Наиболее распространенным примером специальной категории персональных данных являются данные о здоровье.

Однако в процессе обработки персональных данных нередко возникает вопрос, какая же именно информация и в каком объеме составляет данные о состоянии здоровья человека. Так, закон о персональных данных подобного определения не содержит. Пункт 1 статьи 2 Федерального закона № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» говорит о том, что здоровье – «состояние физического, психического и социального благополучия человека, при котором отсутствуют заболевания, а также расстройства функций органов и систем организма» [20].

Из части 1 статьи 22 вышеуказанного закона следует, что к информации о здоровье относятся «сведения о результатах медицинского обследования, наличии заболевания, об установленном диагнозе и о прогнозе развития заболевания, методах оказания медицинской помощи, связанном с ними риске, возможных видах медицинского вмешательства, его последствиях и результатах оказания медицинской помощи» [20].

Самым простым примером персональных данных специальной категории можно считать сведения, которые содержатся в медицинских картах, а также справках, представляемых по месту учебы или работы. Такие справки содержат сведения об установленном диагнозе, хоть и в закодированном виде.

Информация медицинской документации в объеме «Годен/не годен», категории годности, в том числе к военной службе также относится к специальной категории персональных данных, ведь она содержит сведения о результатах медицинского обследования.

Отсутствие в профильном законе понятия «состояние здоровья» ведет к разности толкования данного термина. При этом чаще всего «состояние здоровья» связывают с наличием какого-либо заболевания, поставленным диагнозом. В то же время из положений статьи 2 закона № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» можно сделать вывод, что здоровье – это еще и психическое состояние, социальное благополучие субъекта [20].

К биометрическим персональным данным относятся 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 [29].

Обрабатываться такие персональные данные могут только при соблюдении требований 11 статьи закона. В то же время четкого перечня таких данных не существует. Очевидно, что к ним относятся отпечатки пальцев, код ДНК, радужная оболочка глаза. Однако если исходить из понятия, указанного в статье 11 закона, биометрические данные не ограничиваются исключительно отпечатками пальцев и подобными данными. Ведь это может быть и иная информация, которую оператор будет использовать для определения личности.

Существует ряд сложностей в том, как определить, когда персональные данные, такие, например, как фотография гражданина, начинают использоваться для идентификации его личности, а также как гарантировать законность обработки этих данных, не нарушив прав гражданина.

Судебные решения также не единообразны в данном вопросе.

В качестве одного из примеров правоприменительной практики в вопросе отнесения фотоизображения гражданина к его биометрическим персональным данным можно привести спор, легший в основу решения Верховного суда Российской Федерации по делу № А42-342/2017 [26].

Так, предприятие оспорило выданное по итогам проведения плановой выездной проверки предписание территориального управления Роскомнадзора. Надзорный орган установил, что предприятие оформляло пропуска своим посетителям. Для идентификации посетителей на пропусках размещались фотографии этих лиц. Исходя из цели обработки фотографических изображений, а именно, идентификации посетителей предприятия, надзорный орган указал, что по смыслу закона такие данные являются биометрическими.

Законом установлено, что биометрические данные могут обрабатываться при условии подписания субъектом особого согласия. Его структура должна соответствовать указанной в части 4 статьи 9 закона. Контролируемому лицу было выдано предписание, с которым он не согласился. Однако вышестоящие суды признали, что выданное предписание законно и не нарушает права оператора. А вот обработка биометрических данных посетителей предприятия, пользующихся пропусками, действительно требовала их письменного согласия.

Пятый кассационный суд общей юрисдикции определил, что видеоизображения, получаемые с помощью видеокамеры, находящейся в общей долевой собственности истца и ответчика признаны биометрическими персональными данными [28].

Согласно действующей на сегодняшний день позиции регулятора, изложенной в 2022 году в письме Роскомнадзора № 08-78032, по общему правилу возможность отнесения сведений к биометрическим персональным данным определяется законом. Например, к таким данным относится цифровая фотография лица владельца заграничного паспорта нового поколения, которая записана на содержащийся в нем носитель информации. Требования к формату изображения лица человека, предназначенного для хранения в записи биометрических данных, установлены Национальным стандартом РФ ГОСТ Р ИСО/МЭК 19794-5-2013, утвержденным приказом Росстандарта от 6 сентября 2013 г. № 987-ст.

Но определить, соответствует ли фотоизображение вышеуказанному формату операторам также нелегко, что в свою очередь создает риски неисполнения требований к обработке таких данных. Ведь согласно закону, обработка биометрических фотографических изображений должна

осуществляться только с согласия человека. Такое согласие должно соответствовать установленным законом требованиям. Его структура закреплена в статье 9 профильного закона (часть 4). В остальных случаях обработка фотографий физических лиц осуществляется на общих правовых основаниях. Одновременно следует отметить, что охрана изображения гражданина регулируется статьей 152.1 Гражданского Кодекса РФ, которой определены случаи, когда возможно использование фотографий граждан.

Иные данные относятся к общей категории, их перечень которых остается открытым.

Таким образом, можно сделать вывод, что категории персональных данных - это общие данные, «специальные и биометрические данные» [16].

Данная позиция подтверждена приказом регулятора от 24.02.2021 года № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных к распространению» [25].

Такую же классификацию категорий предполагает и уведомление об обработке данных, форма которого размещена на портале персональных данных Роскомнадзора.

В то же время Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» установлены требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных. Документ выделяет «биометрические, специальные, общедоступные и иные категории» [23].

Общедоступными данными в призма вышеуказанного Постановления являются «данные, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона № 152-ФЗ «О персональных данных», то есть данные, включенные в «общедоступные источники персональных данных (в том числе справочники, адресные книги)» [16].

К таким данным статьей 8 закона отнесены фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

Но определение «общедоступные источники персональных данных» является открытым. Из положений статьи 8 закона следует, что к ним, помимо прочих, относятся адресные книги и справочники. Какие еще источники и по какому принципу могут быть отнесены к общедоступным в законе не говорится.

Одновременно, актуальная редакция закона о персональных данных не включает в себя термин «общедоступные персональные данные». После вступления в силу Федерального закона от 30 декабря 2020 года № 519-ФЗ данный термин был исключен из закона о персональных данных. С 1 марта 2021 года в законодательстве было введено новое понятие – «персональные данные, разрешенные субъектом персональных данных для распространения» [16].

Различия в условиях и правовых основаниях обработки персональных данных, разрешенных для распространения, и данных, включенных в общедоступные источники, требуют внимательного подхода и глубокого понимания законодательства. Важно, чтобы операторы осознавали риски и соблюдали требования, чтобы избежать возможных правовых последствий.

Так для легального размещения персональных данных в общедоступных источниках требуется получить письменное согласие субъекта данных, которое оформляется в соответствии частью 4 статьи 9 закона «О персональных данных». Форма же согласия на распространение персональных данных утверждена приказом регулятора от 24.02.2021 года № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных к распространению» [25].

Указанные выше аспекты вызывают вопросы относительно исполнения положений Постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в части корректности

отнесения тех или иных персональных данных к категории общедоступных или иных, определения требований к уровню их защищенности.

Разность трактовки понятий «категории персональных данных» в различных нормативных правовых актах влечет различные интерпретации требований закона. Очевидно, что обработка специальных и биометрических данных выведена под правовое регулирование отдельных статей профильного закона не просто так. Это особо чувствительная информация, требования к обработке которой ужесточены. Штрафы за нарушение обработки персональных данных указанных категорий выше, как и степень вины нарушителя, что дает возможность взыскания компенсации причиненного незаконными действиями морального вреда в большем размере. В связи с вышеизложенным, считаем целесообразным четко определить термины «категории персональных данных» на законодательном уровне. Также видим необходимым привести их значение к единому стандарту в разных нормативных документах.

Глава 2 Требования законодательства РФ к обработке персональных данных операторами и иными лицами, осуществляющими такую обработку

2.1 Принципы и условия обработки персональных данных

Принципы обработки персональных данных описаны в статье 5 закона о персональных данных. Так, обработка персональных данных должна осуществляться на законной и справедливой основе. При этом правомерность обработки персональных данных указана в части 1 статьи 6 Федерального закона № 152-ФЗ «О персональных данных».

Одним из правовых оснований обработки персональных данных является согласие на такую обработку. Но это не единственное условие. Также данные могут обрабатываться, в том числе, в рамках исполнения договора, заключенного субъектом персональных данных, а также «для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем» [16].

Разрешено производить обработку его персональных данных, в случае 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» [16].

Обработка персональных данных допускается, если она «осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах, а также, если она необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве» [16].

Иногда получить согласие субъекта персональных данных невозможно, но обработка его данных необходима «для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных» [16].

Она признается правомерной в соответствии с положениями, указанными в пункте 6 части 1 статьи 6 закона.

Обработка данных, связанная с исполнением «функций организаций, участвующих в предоставлении государственных и муниципальных услуг» не требует согласия на обработку персональных данных [16].

Без согласия их владельца персональные данные могут обрабатываться «для осуществления прав и законных интересов оператора или третьих лиц», если данные анонимизированы и «используются в статистических или иных исследовательских целях» [16].

Тем не менее, в законе не уточняется, какие именно права оператора подразумеваются в пункте 7 части 1 статьи 6.

Важно помнить, что обязанность доказать правомерность обработки данных возлагается на оператора. Операторы должны не только соблюдать требования законодательства, но и быть готовыми предоставить доказательства законности своей деятельности в случае проверки или запроса со стороны контролирующих органов. В связи изложенным все более актуальными становятся вопросы уровня знаний и правильного понимания операторами требований профильного закона.

Обработка персональных данных «должна ограничиваться достижением конкретных, заранее определенных и законных целей». Обработка персональных данных, несовместимая с целями сбора, законодателем запрещена [16].

В то же время данный запрет не всегда соблюдается. К сожалению, встречаются случаи, когда получив персональные данные от субъекта или третьего лица, лица, их обрабатывающие начинают использовать эти данные не в тех целях, с которыми их собирали. Существующая судебная практика доказывает, что такие случаи нередки.

Так, гражданин написал обращение в компанию, обслуживающую домофонное оборудование, указав в обращении свои персональные данные.

Однако через некоторое время заявителю от указанной компании стали приходить квитанции за обслуживание домофона. При этом договор на такое обслуживание заключен не был, в связи с чем гражданин заявил в надзорный орган о нарушении его прав. Обращение гражданина было рассмотрено. По результатам рассмотрения надзорным ведомством доводы заявителя были подтверждены, составлен административный протокол. А основанием для возбуждения дела об административном правонарушении стала обработка персональных данных обратившегося лица, несовместимая с целями сбора.

Суд поддержал позицию надзорного органа. Судья установил, что персональные данные, полученные организацией при рассмотрении обращения заявителя, могли были быть им использованы исключительно для рассмотрения самого обращения. При этом использование персональных данных заявителя в целях взимания платы за обслуживание домофона противоречит принципам, закрепленным в статье 5 закона. Оператору назначено наказание в соответствии с частью 1 статьи 13.11 Кодекса об административных правонарушениях Российской Федерации [31].

Гражданин также имеет право на возмещение морального вреда, причиненного незаконными действиями по обработке его персональных данных.

Исковые требования субъекта персональных данных к оператору о компенсации ему морального вреда были удовлетворены судьей Первомайского районного суда города Мурманска при рассмотрении дела от 27.05.2022 г. № 2-1877/2022. «Персональные данные истца были неправомерно использованы организацией-оператором с целью оформления на его имя четырнадцати сим-карт без его ведома и согласия, что противоречит принципам и требованиям закона о персональных данных» [37].

Законодательством о персональных данных определено, что «обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки» [16].

Личные дела работников нередко содержат избыточный объем персональных данных, как самих работников, так и их близких родственников. Например, при заключении трудового договора кандидату на трудоустройство

предлагается заполнить анкету, утвержденную распоряжением Правительства РФ от 26.05.2005 № 667-р «Об утверждении формы анкеты, представляемой гражданином Российской Федерации, поступающим на государственную гражданскую службу Российской Федерации или на муниципальную службу в Российской Федерации». Форма анкеты подразумевает внесение в нее внушительного объема данных работников, их близких родственников, в том числе места их жительства, работы, сведения о наличии гражданства иного государства и прочие данные.

Трудовым кодексом РФ сбор такого объема персональных данных не предусмотрен [1].

В то же время некоторые стремятся собрать как можно больше информации о своих работниках. Поэтому они используют вышеуказанную анкету для формирования личного дела работника и берут с работника согласие на обработку такого объема персональных данных. Зачастую операторы самостоятельно разрабатывают подобные анкеты для своих работников. При этом подобные действия работодателя могут не соответствовать принципам, заложенным в статье 5 закона, ведут к нарушениям таких прав субъектов как право на неприкосновенность частной жизни. Закон говорит о недопустимости избыточной обработки данных.

Следует учесть, что сведения о родственниках сотрудника могут быть представлены в объеме, предусмотренном унифицированной формой Т-2. В таком случае обработка не нарушает требований закона. Но стоит не забывать, что согласно этой форме объем персональных данных близких родственников работников должен ограничиваться указанием их фамилии, имени, отчества, года рождения, а также степени родства с работником.

Обработка же большего объема информации о родственниках работника влечет за собой нарушение требований части 5 статьи 5 закона о персональных данных и представляет собой их избыточную обработку. Как правило, у работодателей отсутствуют согласия родственников их работников на обработку сведений о них. При этом закон говорит о необходимости наличия такого согласия и обеспечения соблюдения требований части 5 статьи 5 закона.

Иным примером избыточности может служить требование указать при регистрации на сайте, продающем цветы, свои паспортные данные. Обязательное указание при оформлении дисконтной карты в магазине места работы владельца карты также не соответствует заявленной цели сбора и является избыточным.

Еще одним примером избыточности является требование предоставления биометрических данных. Оператор «не вправе отказывать в обслуживании в случае отказа субъекта персональных данных предоставить биометрические персональные данные и (или) дать согласие на их обработку, если в соответствии с федеральным законом получение такого согласия не является обязательным» [16].

Биометрия часто используется в системе контроля управления доступом в фитнес-центрах. Операторы оправдывают свои действия необходимостью создания безопасных условий при посещении клуба, требованиям по антитеррористической защищенности места массового скопления людей, а также нехватке персонала, обеспечивающего пропускной режим в клубе. Однако такие действия как понуждение к сдаче биометрических данных противоречат требованиям действующего законодательства в сфере персональных данных, создают угрозу нематериальным благам человека.

Сбор избыточных персональных данных может приводить к их дальнейшей неправомерной обработке, использованию в целях, отличных от ранее заявленных, а также увеличивает риск совершения мошеннических действий в отношении их владельца. Ведь чем больше доступно информации о человеке, тем более уязвима его безопасность.

Вместе с тем понятие «избыточный сбор персональных данных» как таковое профильным законом также не определено. Критерии избыточности законодательно не установлены.

Еще одним важным принципом обработки персональных данных является необходимость их своевременного уничтожения при достижении целей их обработки или в случае утраты необходимости в достижении этих целей. Хранение личных данных вместо их своевременного уничтожения - частый случай в современной реальности.

В качестве примера можно привести ситуацию, когда организация продолжает хранить поступившие резюме кандидатов на трудоустройство после принятия решения об отказе в приеме на работу. Как правило, операторы персональных данных обуславливают такие действия возможным появлением новых вакансий в будущем и вероятным приглашением кандидата на новое собеседование, утверждая, что цель обработки данных, содержащихся в резюме, не достигнута.

Тем не менее, данный аргумент вызывает дискуссии, поскольку цели обработки персональных данных должны быть определены заранее, в соответствии с пунктом 2 статьи 5 закона о персональных данных.

Относительно недавно в законе о персональных данных были обновлены критерии, которым должно соответствовать согласие на обработку данных: оно должно быть «конкретным, предметным, информированным, сознательным и однозначным» [16].

Это в свою очередь предполагает указание цели обработки персональных данных и срока действия согласия.

Требования к его структуре законодатель не устанавливает. Отсутствие в законе разъяснений, что конкретно понимается под такими понятиями как информированность, конкретность, предметность и однозначность приводит к различным толкованиям этих критериев операторами.

С целью обеспечения исполнения операторами законодательно закрепленных принципов обработки персональных данных считаем целесообразным закрепить в профильном законе понятие «избыточная обработка персональных данных», определить четкие критерии избыточности при обработке данных. Также полагаем необходимым ввести требования к структуре любого согласия на обработку персональных данных, предполагающие обязательное указание в нем конкретной цели обработки персональных данных, перечня обрабатываемых персональных данных, перечня действия с ними, срока действия согласия и порядка его отзыва. Полагаем, что указанное будет способствовать более ответственному отношению операторов к составлению согласий, формированию единообразия

в подходах к их созданию. Наличие в согласиях всех необходимых элементов упрощает процесс доказывания субъектом нарушения его прав в суде.

2.2 Права и обязанности лиц, участвующих в обработке персональных данных

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» [16].

Закон о персональных данных устанавливает обязанности операторов, которые направлены на защиту прав субъектов персональных данных.

Так, оператор, являющийся юридическим лицом, обязан назначить лицо, ответственное за организацию обработки персональных данных. У этого лица есть ряд обязанностей, которые включают в себя следующие: «осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных, организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов» [16].

Лицо, ответственное за организацию обработки персональных данных выполняет важные функции. Систематическое осуществление внутреннего аудита процессов обработки персональных данных направлено на обнаружение возможных нарушений прав субъектов данных. Это позволяет принимать необходимые профилактические меры по предотвращению нарушений в данной области.

Часть операторов, несмотря на требования законодательства, не уделяют должного внимания выбору и назначению ответственного за организацию обработки данных. «Обязанности, возложенные на такое лицо, исполняются лишь на бумаге, а зачастую не исполняются вообще. Например, положения законодательства Российской Федерации о персональных данных фактически до работников не доводятся, лицо, ответственное за организацию обработки персональных данных ограничивается лишь формальным подписанием листов ознакомления» [15].

Обязанности ответственного лица часто являются второстепенными по отношению к основным обязанностям работника по занимаемой должности.

Статистика показывает, что большинство случаев утечек персональных данных происходит вследствие человеческого фактора [8].

Низкий уровень знаний персонала, обрабатывающего персональные данные, отсутствие соответствующего обучения, высокие затраты на содержание в штате специалистов по информационной безопасности приводят к снижению уровня защищенности персональных данных.

«Данная проблема, в том числе связана с тем, что в Российской Федерации не существует административной ответственности за неисполнение оператором обязанности по назначению лица, ответственного за организацию обработки персональных данных, невыполнением им предусмотренных законодательством функций и обязанностей, равно как и не существует требований к его квалификации.

Кроме того Федеральным законом № 152-ФЗ «О персональных данных» не предусмотрено обязательное назначение такого лица для индивидуальных предпринимателей, в то время как деятельность индивидуального предпринимателя может быть связана с обработкой значительного объема персональных данных» [15].

Федеральным законом от 14.07.2022 № 266-ФЗ внесены изменения в статью 21 Федерального закона № 152-ФЗ «О персональных данных», а именно введена часть 3.1, которой установлены обязанности любого оператора персональных данных по обязательному и своевременному уведомлению надзорного органа о произошедших инцидентах, выразившихся в

неправомерной или случайной передаче (предоставлении, распространении, доступе) персональных данных, которая повлекла нарушение прав субъектов персональных данных. Теперь оператор в случае «утечки» персональных данных «обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных: в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом; в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента [16].

Учитывая вышесказанное необходимо обеспечить особо тщательный контроль за сохранностью личных данных как нематериального блага [9].

Считаем необходимым «закрепить на законодательном уровне необходимость назначения лица, ответственного за организацию обработки персональных данных, для индивидуальных предпринимателей, установить требования к квалификации такого лица, а также ввести административную ответственность за неисполнение таким лицом предусмотренных Федеральным законом № 152-ФЗ «О персональных данных» обязанностей» [15].

Законодатель в последнее время все больше конкретизирует обязанности операторов. Так, Федеральным законом от 14 июля 2022 № 266-ФЗ уточнены обязательные требования к документу, определяющему политику в отношении обработки персональных данных, введена обязанность оператора персональных данных по проведению проверок своей деятельности по обработке персональных данных.

Каждый оператор обязан проводить внутренний контроль соответствия обработки персональных данных профильному законодательству, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных и локальным актам оператора. Оператор самостоятельно решает, как часто и каким образом проводить контроль, основываясь на объеме данных, категориях информации, смены персонала организации-оператора и иных факторах. Пункт 4 части 1 статьи 18.1 профильного закона описывает общие требования к проведению внутреннего контроля. Все остальное зависит от степени ответственности оператора.

Приказ Роскомнадзора от 24.12.2021 № 253 утвердил форму проверочного листа, представляющего собой список вопросов, ответы на которые позволяют оценить соблюдение оператором требований закона.

Некоторые операторы по собственной инициативе используют данный проверочный лист при осуществлении внутреннего контроля. Однако это не является обязательным. Определение порядка проведения внутреннего контроля является правом оператора. Часто план внутреннего контроля содержит лишь общие формулировки, не позволяющие понять, что конкретно и на какой предмет возможного правонарушения необходимо проверить, что, несомненно, приводит к формальному исполнению требования законодательства о проведении такого контроля. А зачастую такой план и вовсе у оператора отсутствует.

На наш взгляд, применение утверждённого проверочного листа обеспечило бы возможность более эффективного выявления и предотвращения правонарушений.

Некоторые требования в области персональных данных определены другими актами. Так, персональные данные работника должны обрабатываться работодателем «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» [45].

«Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие» [45].

Работники должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки их персональных данных, а также об их обязанностях и правах в этой области.

Подавляющее большинство работников оператора связано с обработкой данных при выполнении своих служебных обязанностей. Очевидно, что работники кадровых служб обрабатывают гораздо больший массив персональных данных, чем, например, работники договорных отделов. В то же время в независимости от объема обрабатываемых данных согласно законодательству все такие работники должны быть ознакомлены с соответствующими требованиями. Ведь в противном случае они не смогут обеспечить законность обработки личных данных, что может привести к нарушению прав владельцев этих данных.

«Информировать работников о требованиях закона, знакомить с внутренними актами оператора, касающимися обработки персональных данных – обязанность лица, отвечающего за организацию такой обработки. В случае отсутствия такого лица, например, у индивидуального предпринимателя, данная обязанность возлагается на самого оператора» [15].

Надо отметить, что обязанность по разработке документа, определяющего политику оператора в отношении персональных данных, локальных актов по вопросам такой обработки возлагается только на юридическое лицо. Прямого указания о наличии такой обязанности у индивидуального предпринимателя в законе не содержится. Одновременно пунктом 8 статьи 86 Трудового кодекса определена обязанность работодателя ознакомить своих работников под роспись с документами, устанавливающими порядок обработки их персональных данных, а также об их правах и обязанностях в этой области, что не предполагает исключений для индивидуальных предпринимателей [11].

В соответствии с частью 2 статьи 18.1 закона о персональных данных оператор, осуществляющий сбор персональных данных с использованием сети

Интернет, обязан опубликовать в соответствующей сети документ, определяющий его политику в отношении обработки персональных данных, а также сведения о реализуемых требованиях к их защите [16].

Оператор должен «опубликовать в соответствующей информационно-телекоммуникационной сети, в том числе на страницах принадлежащего оператору сайта в информационно-телекоммуникационной сети Интернет, с использованием которых осуществляется сбор персональных данных, документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети» [16].

На сайте должна быть предусмотрена возможность выражения согласия на обработку персональных данных.

Зависимости от организационно-правовой формы оператора в законе нет. Следовательно, при сборе персональных данных через «Интернет» любой оператор разместить на сайте политику в отношении обработки персональных данных. Полагаем, что указанное свидетельствует о целесообразности наличия обязанности по разработке указанного документа у всех операторов [36].

Учитывая положения Трудового кодекса Российской Федерации и закона о персональных данных, считаем целесообразным возложить обязанность по разработке политики обработки персональных данных и связанных с ней локальных актов и на индивидуальных предпринимателей. Это может стать важным шагом к усовершенствованию и усилению защиты прав субъектов персональных данных, не только повысит уровень ответственности, но и создаст более безопасную среду для обработки личной информации.

Особого внимания требуют вопросы обработки личных данных в информационно-телекоммуникационной сети Интернет. Ведь многие процессы в нашей повседневной жизни неразрывно связаны с ее использованием. Это предоставление различных услуг, получение образования, совершение покупок, заключение договоров или просто общение. При этом практически всегда эти процессы связаны с обработкой данных.

В соответствии с частью 5 статьи 18 вышеуказанного закона оператор, осуществляющий сбор персональных данных сети Интернет, «обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации», за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 указанного закона [16].

Следовательно, центры обработки персональных данных должны быть локализованы на территории нашего государства [19].

Кроме того, сбор данных с помощью сервисов, расположенных за рубежом, нарушает требования части 5 статьи 18 Федерального закона № 152-ФЗ «О персональных данных». Но многие операторы персональных данных не знакомы с данным требованием или игнорируют его, продолжая производить сбор личных данных с помощью форм, размещённых за территорией РФ. Нарушение требований локализации баз данных при сборе персональных данных влечет за собой максимальные штрафы, установленные статьей 13.11 КоАП РФ, так как может нанести значительный вред охраняемым законом благам, в том числе, таким как право на неприкосновенность частной жизни [10].

Недавно была принята норма, предъявляющая требования к операторам по обработке персональных данных, разрешенных субъектом для распространения. Она нацелена на защиту персональных данных, ограничения возможности их бесконтрольного использования. В соответствии с новой статьей 10.1 согласие на распространение, то есть предоставление персональных данных неограниченному кругу лиц, «оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных» [16].

Не позднее трех рабочих дней с момента получения такого согласия оператор должен опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения [16].

Структура согласия утверждена приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24 февраля 2021 № 18. Она предполагает обязательное указание информационного ресурса оператора, на котором будут размещены, из чего следует невозможность указания в таком согласии информационных ресурсов иных операторов.

Судебная практика показывает положительный эффект введенной нормы. Суды выносят решения о привлечении к административной ответственности лиц, неправомерно распространяющих персональные данные, в том числе в социальных сетях. Так, гражданин как оператор персональных данных разместил на своей странице в социальной сети фотоизображения иного лица, а также его несовершеннолетнего ребенка в отсутствие согласия указанного лица. Рассмотрев поступившие материалы, надзорный орган составил протокол об административном правонарушении. Суд, в свою очередь, назначил нарушителю наказание в виде штрафа [32].

Следует отметить, что для государственных или муниципальных органов правительством Российской Федерации установлен отдельный перечень мер, направленных на обеспечение выполнения ими обязанностей, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных». Для них определен четкий перечень локальных актов, которые необходимо утвердить распоряжением руководителя. Одним из основных являются правила обработки персональных данных. Кроме того необходимо разработать правила рассмотрения запросов субъектов персональных данных, осуществления внутреннего контроля процессов, связанных с обработкой персональных данных, правила работы с обезличенными персональными данными. Также такие категории операторов обязаны иметь «перечень информационных систем персональных данных, составить перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, перечень лиц, ответственных за проведение мероприятий по обезличиванию» [21].

Считаем, что включение в закон «О персональных данных» аналогичных требований для иных операторов способствовало бы более ясному осознанию ими своих обязанностей, повысило бы степень ответственности операторов при осуществлении такой деятельности.

В законе о персональных данных нет четкого упоминания о том, на что имеет право оператор. Отдельной главой определены лишь его обязанности.

Оператор вправе самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством в сфере персональных данных.

Оператор имеет право в определенных случаях самостоятельно создавать форму согласия на обработку персональных данных, устанавливать необходимость разработки локальных актов, помимо документа, определяющего политику оператора в отношении обработки персональных данных, который является обязательным для юридических лиц.

Статья 6, а именно часть 3 указанной статьи профильного закона дает оператору право делегировать свои полномочия по обработке персональных данных иному лицу «на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта» [16].

К такому поручению теперь предъявляются более серьезные требования.

Нововведением является и то, что теперь оператору необходимо указывать в заключаемом договоре обязанность второй стороны соблюдать конфиденциальность персональных данных, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 закона о персональных данных, обязанность уведомлять оператора о произошедших инцидентах, произошедших при обработке персональных данных.

Лицо, с которым заключается договор, обязано «по запросу оператора персональных данных в течение срока действия поручения оператора, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии с

законом, обязано обеспечивать безопасность персональных данных при их обработке» и исполнять иные обязанности [16].

Следует учесть, что лицо, действующее по поручению оператора, несет ответственность исключительно перед оператором, а ответственность перед субъектом персональных данных несет сам оператор, что исключает возможность привлечения такого лица к административной ответственности в случае нарушения им прав субъекта персональных данных [16].

Если оператор передает обработку персональных данных иностранному субъекту, то «ответственность перед субъектом персональных данных за действия указанных лиц несет оператор и лицо, осуществляющее обработку персональных данных по поручению оператора» [16].

Полагаем, что административную ответственность также должно нести лицо, исполняющее поручение оператора. Это, на наш взгляд, способствовало бы повышению уровня их ответственности при обработке персональных данных, и, как следствие, снижению количество утечек персональной информации.

Глава 3 Проблемы правового регулирования обработки персональных данных в Российской Федерации

3.1 Проблемы применения законодательства Российской Федерации в сфере персональных данных

Интенсивное развитие информационных технологий в современном мире несомненно улучшают качество нашей жизни, дает гражданам все новые и новые возможности в реализации своих потребностей, а государству делает проще исполнение ежедневных задач, в том числе снижая временные затраты на их реализацию. С другой стороны, активная цифровизация происходящих вокруг нас процессов увеличивает риски неправомерного доступа к персональным данным, создает угрозу нарушения охраняемых Гражданским Кодексом РФ прав человека. А право гражданина на защиту его личных данных гарантировано Конституцией РФ [12].

Вслед за развитием информационных технологий также происходит совершенствование законодательства в области персональных данных. Эти изменения направлены на укрепление защиты прав граждан.

Однако даже в условиях постоянного усовершенствования законодательных норм граждане и лица, обрабатывающие персональные данные, продолжают сталкиваться со сложностями применения отечественного законодательства в указанной сфере.

Очевидно, что некоторые трудности в применении законодательства о персональных данных являются следствием неопределенности терминов, установленных в законе, а также несоответствия этих терминов в различных нормативно-правовых актах.

Перечень персональных данных ни в законе, ни в иных актах не определен, сам термин является обширным, имеет достаточно абстрактную формулировку. К персональным данным относятся любые идентификационные данные человека. При этом некоторые сведения не могут сами по себе быть отнесены к персональным данным, в то время как в сочетании с другими данными таковыми становятся.

При отнесении определённых сведений к персональным данным важно учитывать существующую судебную практику. Тем не менее, она не является однозначной, что в свою очередь может приводить к сложности реализации права субъекта персональных данных на компенсацию причиненного ему морального вреда.

Согласно закону под обработкой персональных данных следует понимать любое действие с персональными данными, в том числе их «сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных» [16].

Следовательно, хранение персональных данных является вариантом их обработки.

Субъект персональных данных имеет право на получение сведений о том, как обрабатываются его личные данные [47].

Это право гарантировано статьей 14 закона. Оператор обязан предоставить субъекту по его запросу, в том числе, сведения о сроках обработки персональных данных, сроках их хранения.

Информация о сроках обработки и хранения персональных данных должна также содержаться и в документах, определяющих политику оператора в отношении обработки персональных данных. Эти сроки могут быть различными. Наглядной иллюстрацией вышеуказанного может являться обработка персональных данных в процессе исполнения договорных обязательств. Можно сказать, что активный этап обработки персональных данных завершается в момент исполнения договора. Далее наступает этап хранения договора в пределах сроков исковой давности, после чего документы подлежат уничтожению.

Такая же ситуация происходит при ведении кадрового делопроизводства. После увольнения работника его личное дело продолжает храниться оператором на законных основаниях в течение определенного законодательством срока, например, 50 лет.

Однако в законе о персональных данных понятие «хранение персональных данных» отдельно не определено. Включение такого действия как хранение в обработку персональных данных создает сложности в исполнении требований части 7 статьи 14 и пункта 2 части 1 статьи 18.1 закона, в частности, при разделении сроков обработки и хранения данных. Полагаем необходимым ввести в закон о персональных данных понятие «хранение» персональных данных, вывести его из-под понятия «обработки» с целью обеспечения возможности более четкого исполнения требований части 7 статьи 14 и пункта 2 части 1 статьи 18.1 закона о персональных данных.

Условия обработки персональных данных без использования средств автоматизации определены соответствующим положением, утвержденным Постановлением Правительства РФ № 687 от 15 сентября 2008 года.

Согласно вышеуказанному 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 [30].

Из вышеизложенного можно сделать вывод, что практически любой процесс обработки персональных данных является неавтоматизированным.

Одной из задач операторов персональных данных является подача уведомления о намерении проводить такую обработку. Электронные формы уведомлений доступны на портале персональных данных. Закон, а также формы, требуют обязательного указания способа обработки персональных данных, который может быть автоматизированным, неавтоматизированным или смешанным.

Для удобства заполнения сведений на портале персональных данных предусмотрены всплывающие подсказки, помогающие корректно заполнить обязательные поля уведомления. Согласно пояснениям при заполнении поля о способах обработки персональных данных необходимо выбрать или «с

использованием средств автоматизации», если обработка персональных данных производится с помощью средств вычислительной техники; или «без использования средств автоматизации», если обработка персональных данных производится на материальных носителях. Также предусмотрена смешанная обработка персональных данных.

В то же время из содержания указанного положения следует, что вся обработка персональных данных должна рассматриваться как неавтоматизированная. Понятие «автоматизированная обработка персональных данных» содержится в профильном законе. Это «обработка персональных данных с помощью средств вычислительной техники» [16].

Понятие неавтоматизированной обработки определено соответствующим положением. Понятие «смешанная обработка персональных данных» в законе или иных нормативно-правовых актах не определено. Предполагается, что под смешанной обработкой следует понимать использование вычислительной техники и материальных носителей. В то же время это невозможно без участия человека, что по смыслу положения делает такую обработку неавтоматизированной.

Разность понятий в законе и вышеуказанном положении создает сложность в применении норм законодательства в части определения способов обработки персональных данных, а также исполнения требований к такой обработке различными способами.

Для обеспечения законности распространения оператору следует получить от владельца данных согласие, форма которого определена регулятором. Создание собственных шаблонов согласий на распространение законом запрещено.

Установленная форма согласия предполагает обязательное указание к ней информационного ресурса, принадлежащего оператору, на котором будут распространяться данные. Это адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы), посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных [25].

Из указанного следует, что согласие дается на распространение персональных данных в сети Интернет.

Очевидно, что распространение информации не может ограничиваться только сетью Интернет. Персональные данные могут быть доступны неограниченному числу людей, например, через размещение на доске объявлений в организации, находящейся в общественном доступе, на информационных табличках в открытых для посещения местах, в объявлениях или другими способами.

Установленная форма согласия не допускает распространение персональных данных на ресурсах, которые не принадлежат оператору. Это затрудняет применение законодательной нормы при распространении персональных данных другими способами, отличными от размещения этих данных на собственном интернет-ресурсе. Полагаем целесообразным внести изменения в установленную форму согласия на распространение персональных данных в части возможности указания в нем иных способов распространения, помимо уже предусмотренных.

Статья 10.1 закона не применяется, в случае если обработка персональных данных производится в целях выполнения возложенных законодательством Российской Федерации на государственные и муниципальные органы власти, а также на подведомственные таким органам организации функций, полномочий и обязанностей [16].

Но существуют нормы, которые обязывают и иные виды организаций распространять персональные данные. Например, частные медицинские организации, имеющие лицензию на осуществление медицинской деятельности, как и государственные, обязаны информировать пациентов о медицинском персонале, их уровне образования и квалификации. В то же время требования статьи 10.1 делают исключение только для организаций, подведомственных государственному или муниципальному органу власти (часть 15 статьи 10.1). Следовательно, на иных лиц, обязанных распространять персональные данные в соответствии с законом, возлагается обязанность соблюдения норм, прописанных в статье 10.1. Из этого следует, что таким лицам необходимо получить со своих работников соответствующее согласие

при наличии законодательно возложенной на оператора обязанности публикации данных.

Предлагаем внести изменения в положения части 15 статьи 10.1 и дополнить перечень исключений операторами, обязанность распространения персональных данных на которых возложена законодательно.

Важно подчеркнуть, что положения «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», утверждённого Постановлением Правительства РФ от 21 марта 2012 г. № 211 в части требований к структуре определяющего политику оператора в отношении обработки персональных данных документа отличаются от положений пункта 2 части 1 статьи 18.1 закона о персональных данных.

Так государственные и муниципальные органы должны в соответствии с вышеуказанным перечнем разработать правила обработки личных данных, 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 [21].

В то же время Федеральным законом определено также требование об указании в таких документах способов обработки персональных данных. Пункт 2 части 1 статьи 18.1 закона содержит такие формулировки как «категории и перечень персональных данных», в то время как для государственных и муниципальных органов это понятие звучит как «содержание персональных данных». Разность требований закона и постановления правительства влечет за собой возможное несоответствие издаваемых государственными и муниципальными органами локальных актов требованиям закона. Полагаем необходимым привести в соответствие требования пункта 2 части 1 статьи 18.1 закона о персональных данных и положения «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» с целью формирования единых требований к структуре документа, определяющего политику в отношении обработки персональных данных.

Особого внимания, по нашему мнению, требуют вопросы правомерности внесения персональных данных в общедоступные источники, к которым отнесены, в том числе справочники и адресные книги.

Являются ли сайты такими источниками персональных данных в законе четко не указано, но по смыслу статьи 10.1 интернет-ресурсы выведены под правовое регулирование этой статьи. Хотя по своей природе интернет-сайты являются очевидным примером общедоступного источника, в статье 8 закона они не упоминаются.

Таким образом определить правовое основание обработки (включения) персональных данных в общедоступных источниках, на интернет-сайтах, для операторов может стать проблематичным, ведь с одной стороны, таким основанием является согласие, соответствующее части 4 статьи 9 закона, а с другой существуют требование статьи 10.1, предполагающие наличие иного вида согласия.

Контроль целесообразности и законности передачи данных за пределы нашей страны на сегодняшний день является одной из приоритетных задач. Теперь до начала передачи нужно уведомить о ней Роскомнадзор. А до подачи уведомления оператор обязан получить от органов власти другого государства, иностранных лиц, которым планируется передача персональных данных, определенные законом сведения.

Это сведения о правовом регулировании в области персональных данных иностранного государства, под юрисдикцией которого находятся органы власти иностранного государства, иностранные физические лица, иностранные юридические лица, которым планируется трансграничная передача персональных данных, о мерах защиты данных, условиях прекращения их обработки, сведения об органах власти иностранного государства, иностранных физических лицах, иностранных юридических лицах, которым планируется

трансграничная передача персональных данных (наименование либо фамилия, имя и отчество, а также номера контактных телефонов, почтовые адреса и адреса электронной почты [16].

Однако порядок получения таких сведений, их объем этих сведений, а также формы их предоставления в надзорный орган законом не определены, что, безусловно, создает вопросы по исполнению данной нормы, в связи с чем полагаем необходимым определить в законе такой порядок.

3.2 Пути совершенствования законодательства в сфере обработки персональных данных

За последние годы закон о персональных данных претерпел колоссальные и очень важные изменения. Они коснулись многих его аспектов.

Так, законодателем были введены нормы, ограничивающие бесконтрольную передачу персональных данных в другие государства. Важные изменения внесены в статью 12 профильного закона. Определены требования к деятельности операторов, планирующих передавать данные российских граждан за границу. Теперь трансграничная передача персональных данных может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства, защиты экономических и финансовых интересов Российской Федерации, обеспечения дипломатическими и международно-правовыми средствами защиты прав, свобод и интересов граждан Российской Федерации, суверенитета, безопасности, территориальной целостности Российской Федерации и других ее интересов на международной арене с даты принятия уполномоченным органом по защите прав субъектов персональных данных решения, предусмотренного частью 12 статьи 12 закона [16].

Внесены изменения в сроки, в течение которых субъекты персональных данных и Роскомнадзор должны получить ответы на свои запросы. Теперь эти сроки существенно сокращены и составляют 10 рабочих дней, что, безусловно, способствует более оперативному решению рассматриваемых вопросов.

Также в закон введен принцип экстерриториальности. Теперь он применяется «к обработке персональных данных граждан Российской Федерации, осуществляемой иностранными юридическими лицами или иностранными физическими лицами, на основании договора, стороной которого являются граждане Российской Федерации, иных соглашений между иностранными юридическими лицами, иностранными физическими лицами и гражданами Российской Федерации либо на основании согласия гражданина Российской Федерации на обработку его персональных данных» [16].

У операторов появилась обязанность информировать уполномоченные органы о произошедших у них утечках персональных данных, а также о результатах проведенных внутренних расследований. Это необходимо сделать в кратчайшие сроки, которые также определены законом. В случае выявления инцидента оператор обязан уведомить регулятора в течение 24 часов с момента, когда ему стало известно о происшествии. Кроме того, необходимо уведомить Роскомнадзор «в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента» [16].

В практике многих операторов – поручение обработки персональных данных третьим лицам. Так, многие организации поручают ведение бухгалтерского учета и кадрового делопроизводства сторонним организациям. С такими организациями заключается договор поручения, передаются персональные данные работников. Также такие организации могут вести деятельность по обработке персональных данных на основании государственного или муниципального контракта или соответствующего акта, принятого государственным органом или муниципальным органом власти.

Требования к договорам поручения обработки персональных данных существенно усложнились в недавнее время. Теперь при поручении такой обработки третьему лицу необходимо предусмотреть в договоре условия такого поручения и прописать обязанности лица, действующего по поручению. К таким обязанностям, в частности, относятся соблюдение конфиденциальности при обработке персональных данных, соблюдение требований к локализации баз персональных данных на территории Российской Федерации. Лица,

действующие по поручению оператора, «обязаны предоставлять оператору по его запросу документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, а также обеспечивать безопасность персональных данных при их обработке» [16].

Оператор должен проявлять интерес к правильному выбору лиц, с которыми он заключает договоры, поскольку согласно законодательству именно он несет ответственность перед субъектом за действия организации, действующей по его поручению, в случае нарушения прав этого лица.

Также важным изменением является и то, что иностранные лица, обрабатывающие персональные по поручению оператора, теперь несут ответственность перед субъектом в случае нарушения его прав наравне с оператором.

Но, несмотря на постоянное усовершенствование норм законодательства сфере персональных данных, в нем остаются положения, требующие, по нашему мнению, изменений.

Рассмотрим в качестве примера статью 22 закона, которой установлена обязанность уведомления уполномоченного органа по защите прав субъектов персональных данных о намерении осуществлять обработку персональных данных.

Исключения из вышеуказанной обязанности коснулись лишь лиц, обрабатывающих данные, включенные в государственные информационные системы, созданные в целях защиты безопасности государства и общественного порядка, в случае обработки данных с соответствии с 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, а также если персональные данные обрабатываются исключительно без использования средств автоматизации [16].

Однако учитывая понятие «неавтоматизированная обработка персональных данных», закрепленное положением, утвержденным Постановлением Правительства РФ № 687 от 15 сентября 2008 года, обязанность подачи уведомлений об обработке персональных данных

снимается практически с любого оператора, что явно противоречит целям изменений статьи 22.

Полагаем целесообразным определить понятия способов обработки персональных данных с целью их правильного толкования и указания и предусмотренных законодательством случаях, а также скорректировать понятие, указанное в положении, утвержденном Постановлением Правительства РФ № 687 от 15 сентября 2008 года, с учетом положений закона о персональных данных.

В соответствии с положениями статьи 9 закона о персональных данных согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным [16].

Тем не менее, отсутствие в законодательстве ясных требований к содержанию согласия на практике зачастую приводит к тому, что формулировки таких согласий не соответствуют указанным критериям. Это, в свою очередь, может привести к нарушению прав владельцев данных.

Например, из текста согласия не всегда можно понять, какие действия будут производиться с персональными данными. Некоторые операторы указывают общее понятие «обработка», под которое подпадает, в том числе, предоставление, доступ, распространение и иные виды обработки, прямо не предположенные формулировками согласия. Также не всегда в согласии указан оператор, которому оно дается, отсутствуют его реквизиты. Особенно часто такая ситуация встречается при сборе персональных данных посредством интернет-сайта, когда согласие дается не оператору, а сайту.

В России существует административная ответственность за обработку персональных данных в целях, отличных от ранее заявленных. Отсутствие в согласии указания четкой цели обработки персональных данных лишает субъекта возможности контроля правомерности их дальнейшего использования.

Считаем необходимым закрепить в законе требования к структуре любого согласия на их обработку. По нашему мнению, структура согласия должна в обязательном порядке содержать цель такой обработки, перечень обрабатываемых персональных данных, перечень действий с ними, сведения об

операторе с указанием его идентификационных данных, способ отзыва данного согласия, соответствующий способу его дачи, а также срок его действия, исключая указание о бессрочной обработке. Ведь часто согласия содержат весьма абстрактные формулировки, что делает практически невозможным для субъекта понимание их сути.

Также полагаем необходимым закрепить на законодательном уровне требования к содержанию интернет-сайтов, на которых производится обработка (в том числе сбор, распространение) персональных данных, а также ввести административную ответственность за неисполнение этих требований.

Считаем важным ввести обязанность размещения на таких сайтах сведений об операторе персональных данных с указанием его реквизитов. Ведь отсутствие этих сведений на сайте может привести к нарушению прав субъекта персональных данных, в том числе предусмотренных статьями 14, 10.1 профильного закона.

Согласно положениями статьи 10.1 гражданин может обратиться к лицу, распространяющему его персональные данные, с требованием о прекращении распространения. Однако нередко ситуация, когда на сайте отсутствует форма обратной связи, а в случае ее наличия нет сведений об операторе, которому направляется обращение. Судебная защита прав субъекта в таком случае влечет за собой определенные затраты.

Одновременно субъект имеет право на получение информации об обработке его персональных данных, закрепленное в статье 14 закона.

Но отсутствие на интернет-ресурсах сведений об операторе персональных данных, его реквизитах, местонахождении ограничивает возможность реализации субъектом своего права на обращение к нему.

В недавнем времени в законе закрепили требования к структуре документа, определяющего политику оператора в отношении обработки персональных данных.

Она во многом схожа со структурой уведомления о намерении осуществлять обработку персональных данных. Полагаем, что разработка функционала создания шаблона политики наподобие размещенного на портале персональных данных функционала создания уведомления значительно

снизила бы количество ошибок при составлении документа. Создание «конструктора» документа, определяющего политику оператора в отношении обработки персональных данных, по нашему мнению, исключило бы неправильное толкование операторами норм пункта 2 части 1 статьи 18.1 и помогло бы избежать несоответствия созданных документов требованиям закона. Это способствовало бы более полному и корректному наполнению указанного документа, с которым имеет право ознакомиться любой гражданин.

Интересным является и тот факт, что закон не обязывает индивидуальных предпринимателей издавать локальные акты по вопросам, связанным с обработкой персональных данных. Хотя при этом индивидуальным предпринимателем может обрабатываться большой массив данных, а в штате может состоять достаточно много работников, которые, в свою очередь, должны быть ознакомлены с документами своего работодателя, определяющими порядок обработки их персональных данных, как требует Трудовой кодекс РФ.

Тем не менее, закон все же возлагает на индивидуального предпринимателя обязанность размещать на сайте политику в отношении их обработки при осуществлении на нем сбора данных.

Полагаем необходимым ввести обязанность разработки локальных актов для всех операторов персональных данных независимо от их организационно-правовой формы. На наш взгляд, эта мера повысит прозрачность процессов обработки персональных данных индивидуальными предпринимателями.

Одной из установленных обязанностей юридических лиц является назначение лица, ответственного за организацию обработки персональных данных. На данное лицо возложены весомые обязанности, включая обучение сотрудников правильной обработке персональных данных и проведение аудита внутренних процессов, связанных с этой обработкой, взаимодействие с субъектами персональных данных.

Все эти обязанности требуют определенных знаний, навыков и умений, особенно, если оператором обрабатывается большой массив персональных данных. При этом закон не предъявляет каких-либо требований к квалификации ответственных лиц.

На практике ответственным лицом назначается, как правило, работник кадровой службы, ведь нередко руководство организации – оператора полагает, что обработка персональных данных ограничивается ведением личных дел и решением иных кадровых вопросов. Однако это далеко не всегда так. Ведь даже если оператор обрабатывает исключительно фамилию, инициалы своих клиентов, или же адреса их электронных почтовых ящиков, это говорит об обработке личных данных.

В современных условиях постоянного роста количества утечек персональных данных считаем, что необходимо внедрение законодательных требований к квалификации лиц, ответственных за организацию обработки этих данных. Это важно для предотвращения незаконного оборота персональной информации. Для крупных операторов полагаем целесообразным ввести обязательную аккредитацию их деятельности по обработке персональных данных.

На сегодняшний день размеры административных штрафов за так называемую «утечку» персональных данных остаются слишком низкими. Так, минимальный штраф для юридического лица составляет шестьдесят тысяч рублей, а максимальный – сто тысяч рублей. Они не соответствуют тому ущербу, который владельцы персональных данных испытывают в результате их компрометации. Доступ к паспортным данным, фамилии, имени и отчеству дает мошенникам шансы оформить кредитный договор на третье лицо, чьи сведения оказались в их распоряжении.

Нередки утечки баз данных, содержащих и иные объемы сведения. В их числе адреса электронных почтовых ящиков с паролями к ним. Получив доступ к чужой электронной почте, мошенник использует сведения, содержащиеся в ней, в противоправных целях. Такие сведения, в том числе нередко содержат копии документов, справки из банковских организаций, содержащие, в том числе, большой объём персональных данных.

Встречались случаи наличия в скомпрометированных базах данных сведений, содержащихся в личном кабинете портала государственных услуг. Этот объем данных более чем достаточен для причинения субъекту

персональных данных колоссального вреда, нередко делая его стороной уголовного дела.

Некоторые базы данных, находящиеся в свободном доступе, содержат пароли субъектов персональных данных к их личным кабинетам в различных организациях и сервисах.

Размеры скомпрометированных баз данных весьма внушительны. Тем не менее, размеры штрафов за неправомерную обработку персональных данных, в частности, в случае утечки базы данных, непозволительно малы и составляют от шестидесяти тысяч до ста тысяч рублей для юридических лиц. Полагаем, что такие суммы штрафов несопоставимы с причиняемым вредом субъектам персональных данных. А размер присуждаемой компенсации морального вреда, причинённого утечкой персональных данных, несоизмерим объёму самого вреда. Кроме того, законодательно не установлены четкие критерии определения размера такой компенсации.

Обеспечение должного уровня информационной безопасности, защищённости информационных систем персональных данных, обеспечения наличия в организации квалифицированных специалистов в данной сфере требует больших финансовых вложений. И эти вложения гораздо выше тех штрафов, которые могут быть наложены судом на нарушителя в случае признания его таковым.

Считаем целесообразным ввести отдельный состав в статью 13.11 Кодекса об административных правонарушениях РФ, предполагающий ответственность за «неправомерную обработку персональных данных, выразившуюся в случайной передаче (предоставлении, распространении, доступе) персональных данных» [16].

Размеры административных штрафов, по нашему мнению, должны быть значительно увеличены и зависеть от количества субъектов, чьи персональных данных оказались доступны третьим лицам. Также полагаем важным определить в законодательстве более четкие критерии определения размера компенсации морального вреда, взыскиваемого с операторов персональных данных в случае нарушения ими прав субъектов.

Вопросы, связанные с проведением внутреннего контроля соответствия процессов обработки персональных данных требованиям законодательства также не урегулированы на сегодняшний день. Право решать, как именно проводись контрольные мероприятия, с какой периодичностью и что именно проверять дано оператору. Оператор самостоятельно определяет перечень вопросов, которые нужно проверить в рамках внутреннего аудита.

Как показывает практика, формальное исполнение требования о проведении внутреннего контроля - частый случай, особенно в небольших организациях. Не проведение внутреннего контроля не влечет за собой наступление административной ответственности, нет риска получения штрафа по результатам проверок контролирующим органом.

Кроме того, отсутствие четких стандартов проведения оператором внутренних проверок не способствует их качественному проведению. Как правило, внутренний аудит в лучшем случае проводят программисты, однако их проверки в большей степени касаются безопасности при эксплуатации компьютерной техники, информационных систем. Вопросы соблюдения требований закона о персональных данных в части проверки правомерности обработки персональных данных оператором, актуальности локальных нормативных актов, уведомления об обработке персональных данных, исключения фактов избыточной обработки персональных данных такими специалистами не рассматриваются и остаются вне рамок проведенного внутреннего контроля. В иных случаях внутренний аудит проводят работники кадровых служб, которые в свою очередь проводят проверку в основном в рамках деятельности своего отдела.

Причиной такой практики проведения аудита процессов, связанных с обработкой персональных данных, как правило, служит отсутствие должного уровня знаний уполномоченных работников оператора в области требований действующего законодательства. К сожалению, отсутствие у оператора понимания, какие моменты необходимо проверять в приоритетном порядке, либо низкий уровень ответственности оператора в данном вопросе приводит к формальному исполнению указанной нормы.

По нашему мнению, введение обязательного списка контрольных вопросов для проведения внутреннего контроля оператором способствовало бы повышению уровня осознанности при проведении мероприятия, что в свою очередь привело бы к более качественному результату его осуществления. На сегодняшний день такой список контрольных вопросов разработан только для контролирующего органа.

Также полагаем, что содержание списка контрольных вопросов, их перечень должны ставиться в зависимость от объема и содержания обрабатываемой оператором базы персональных данных.

Кроме того полагаем, что за не проведение внутреннего контроля за обработкой персональных данных в соответствии с требованиями утверждённого списка вопросов, равно как и не соответствующие действительности результаты проведения такого мероприятия, должны повлечь для оператора ответственность.

В связи с вышеизложенным предлагаем ввести новый состав в статью 13.11 Кодекса об административных правонарушениях РФ, предполагающий наступление административной ответственности за неисполнение оператором персональных данных обязанности по проведению внутреннего контроля соответствия обработки персональных данных требованиям законодательства в указанной сфере, либо фальсификации результатов его проведения.

Полагаем, что важным направлением совершенствования законодательства в области персональных данных является создание регламента анонимизации (обезличивания) персональных данных. К сожалению, всегда существует риск неправомерного использования базы персональных данных. Это может быть выражено в неправомерном доступе к ней сторонних лиц, в том числе, в мошеннических целях.

Также бывают случаи, когда у оператора существует необходимость в ограничении объема предоставляемого своим работникам доступа к обрабатываемым персональным данным. Одним из способов такого ограничения может стать обезличивание. Оно, как мы полагаем, способно защитить данные граждан в случае их обработки оператором или компрометации.

На сегодняшний день методы и требования к обезличиванию персональных данных определены приказом Роскомнадзора от 5 сентября 2013 года № 996. Однако данный приказ регулирует обезличивание данных исключительно государственными и муниципальными органами власти. Деятельность других операторов в данном направлении не регламентирована.

По нашему мнению, установление требований к процессу обезличивания персональных данных для операторов, не относящихся к государственным или муниципальным органам власти, могло бы уменьшить риск возможных негативных последствий при обработке персональных данных, включая потенциальный несанкционированный доступ к ним.

Заключение

Вопросы, касающиеся обработки персональных данных, регулируются Федеральным законом № 152-ФЗ «О персональных данных», а также другими нормативно-правовыми актами, которые регламентируют определенные аспекты этой обработки.

В то же время, несмотря на постоянное усовершенствование законодательной базы в указанной сфере существуют вопросы применения закона на практике. Сложности его применения, в первую очередь, связаны с неопределенностью понятийного аппарата. Неясность терминов в законодательстве, таких как «хранение персональных данных», «общедоступные источники персональных данных», «категории персональных данных», «избыточная обработка персональных данных» приводит к несоответствию требованиям по обработке этих данных, нарушению прав граждан. Также, по нашему мнению, определение само «персональные данные» остается открытым.

Вторая проблема, на наш взгляд, заключается в несоответствии понятий в различных нормативно-правовых актах. Некоторые из таких актов, не претерпевали каких-либо изменений в течение длительного времени и, следовательно, их положения не соответствуют актуальной редакции Федерального закона № 152-ФЗ. Так, требования к структуре документов, определяющих политику оператора в отношении обработки персональных данных, различны для государственных или муниципальных органов и иных категорий операторов. А понятие «неавтоматизированная обработка персональных данных», определенное в Положении, утвержденном Постановлением Правительства РФ № 687 от 15 сентября 2008 года, отсутствует в Федеральном законе № 152-ФЗ, и противоречит идее, указанной в статье 22 закона.

Считаем вопросом, требующем внимания законодателя, отсутствие в законодательстве четких требований по определению операторами, не являющимися государственными или муниципальными органами власти, перечня мер, необходимых для принятия в целях соблюдения закона. Законом

не определен четкий перечень обязательных для издания локальных актов для таких операторов. Отсутствие требований законодателя по проведению внутреннего контроля за обработкой персональных данных, а также относительно невысокие штрафы за допущенные нарушения влекут недостаточно внимательное отношение операторов к исполнению законодательства, что в свою очередь может явиться причиной нарушения прав субъектов персональных данных. Также на сегодняшний день не разработаны требования к процедуре обезличивания персональных данных для вышеуказанных операторов.

Еще одним важным вопросом, который по нашему мнению, требует внимания, является разность требований нормативно-правовых актов, регулирующих вопросы обработки персональных данных. Актуальная редакция закона о персональных данных освобождает индивидуальных предпринимателей от обязанности разработки локальных актов по обработке персональных данных, что, по нашему мнению, противоречит положениям трудового кодекса, который обязывает работодателя ознакомить своих работников с такими актами [41].

Каких-либо исключений для индивидуальных предпринимателей кодекс не делает. В то же время законом о персональных данных обязанность разработать такие документы возлагается исключительно на юридических лиц. Также существует несоответствие положений пункта 2 части 1 статьи 18.1 Федерального закона № 152-ФЗ и Постановления Правительства РФ от 21 марта 2012 года № 211 в части требований к структуре определяющего политику оператора в отношении обработки персональных данных. Создание инструмента для формирования шаблона политики в отношении обработки персональных данных способствовало бы более корректному составлению такого документа и помогло бы избежать его несоответствия законодательно закрепленной структуре.

В законе о персональных данных отсутствуют четкие требования к структуре согласия на обработку персональных данных. Это влечет за собой составление согласий в нарушение критериев, указанных в части 1 статьи 9 закона, что в свою очередь усложняет их интерпретацию и дальнейшее

отстаивание субъектами своих прав в судебных органах, в том числе права на компенсацию морального вреда.

Полагаем, что закон о персональных данных предъявляет недостаточные требования к ведению интернет-сайтов, посредством которых производится обработка персональных данных. В частности, отсутствуют требования к содержанию таких сайтов. Зачастую эти сайты не содержат реквизитов оператора, что затрудняет реализацию субъектом персональных данных своих прав.

Еще одной проблемой, на наш взгляд, является недостаток надлежащего контроля со стороны операторов за соответствием обработки персональных данных обязательным требованиям. Это часто связано с низким уровнем знаний операторов в данной сфере. На законодательном уровне не закреплены требования к квалификации лиц, ответственных за организацию обработки персональных данных. Их назначение нередко производится формально. Ненадлежащее исполнение своих функций вследствие отсутствия квалификации в данном вопросе нередко приводит к нарушению прав граждан, создает угрозу их нематериальным благам и гражданским правам субъектов персональных данных.

Отсутствие административной ответственности для лиц, действующих по поручению оператора, при нарушении ими прав граждан, не способствует повышению их бдительности в вопросах сохранности персональных данных. Отдельного внимания, по нашему мнению, требуют вопросы применения положений статьи 10.1 закона о персональных данных, в том числе связанные с правовыми основаниями распространения персональных данных. Шаблон согласия на обработку персональных данных, разрешенных для распространения, не дает операторам возможности производить распространение способами, отличными от распространения на собственном интернет-ресурсе, что затрудняет исполнение указанной нормы. Кроме того полагаем, что список исключений, предусмотренных частью 15 статьи 10.1 Закона не является достаточно полным.

Для устранения указанных проблем полагаем целесообразным внести изменения в понятийный аппарат Федерального закона № 152-ФЗ «О

персональных данных», а также привести в соответствие положения различных нормативно-правовых актов в сфере обработки персональных данных профильному закону. Также считаем необходимым внести изменения в статьи 9, 10.1 закона, конкретизировать перечень мер, предусмотренных статьей 18.1.

Повышение административных штрафов за нарушение закона, а также введение таких штрафов за неисполнение обязанностей оператора, предусмотренных статьей 18.1 закона, и отдельного состава за так называемые «утечки» персональных данных способствовало бы более внимательному отношению операторов к вопросам обработки личных данных, и, возможно повышению интереса к изучению требований законодательства.

Закон о персональных данных неразрывно связан с гражданским законодательством, базируясь на единой цели – защите прав человека, гарантированной Конституцией РФ. Совершенствование законодательства в сфере персональных данных должно привести к усилению защиты нематериальных благ человека и гражданина, неприкосновенности его частной жизни, защите чести и достоинства, личной и семейной тайн.

Список литературы и используемых источников

1. Аверченков В.И. Защита персональных данных в организации: [сайт]. — URL: <https://www.iprbookshop.ru/6993.html> (дата обращения: 25.11.2024)
2. Апелляционное определение Курганского областного суда от 07.09.2017 № 33-2984/2017: [сайт]. - URL: https://oblsud--krg.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=30042948&case_uid=d95487b3-046d-44c1-b4b7-3632573e00ff&result=1&delo_id=5&new=5 (дата обращения 18.12.2023).
3. Апелляционное определение Московского городского суда от 24.07.2017 № 33-28957/2017: [сайт]. - URL: <https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/217b1629-f96d-4e60-986f-978017689292> (дата обращения 18.12.2023).
4. Апелляционное определение Свердловского областного суда от 19.09.2019 № 33-15137/2019: [сайт]. - URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=SOUR&n=248543&dst=100002&ysclid=lgjszbi4gx860160458#bhcYcbTkDAVGpA3e1> (дата обращения: 16.05.2023).
5. Бабелюк Е. Г. Механизм правового регулирования персональных данных: [сайт]. - URL: <https://cyberleninka.ru/article/n/mehanizm-pravovogo-regulirovaniya-personalnyh-dannyh/viewer> (дата обращения 19.11.2024).
6. Голембиовская О. М. Формализация подходов к обеспечению защиты персональных данных: монография // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/81851.html> (дата обращения: 27.04.2024).
7. Гражданский кодекс Российской Федерации (ред. от 08.08.2024): [сайт]. — URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102033239> (дата обращения: 16.05.2023).
8. Из-за чего чаще случаются утечки информации: итоги опроса. Аналитический центр Infowatch: [сайт]. - URL:

<https://www.infowatch.ru/analytics/analitika/iz-za-chego-chasche-sluchayutsya-utechki-informatsii-itogi-oprosa> (дата обращения: 16.12.2024)

9. Касаткин А. А. Защита персональных данных: обзор судебной практики: [сайт]. - URL: <https://moluch.ru/archive/284/63963/> (дата обращения: 16.12.2023)

10. Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 30.12.2001 № 195-ФЗ (ред. от 12.11.2024): [сайт]. — URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 13.02.2024).

11. Кокурина М. А. Оптимизируем работу с личными данными сотрудников / М. А. Кокурина: [сайт]. — URL: <https://glavkniga.ru/elver/2019/21/4432> (дата обращения: 13.02.2023).

12. Комаров С.А., Мицкая Е.В. Правовое регулирование обеспечения информационной безопасности и защиты персональных данных: монография: [сайт]. — URL: <https://artsakhlib.am/wp-content/uploads/2019/11/Сергей-Комаров-Мицкая-Елена-Мицкая-Информационная-безопасность.pdf> (дата обращения: 13.03.2024).

13. Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020): [сайт]. — URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102027595> (дата обращения: 13.02.2024).

14. Новиков Р. В. Правовое регулирование защиты информации, относящейся к сфере частной жизни граждан, в гражданском законодательстве и законодательстве о персональных данных: [сайт]. - URL: <https://cyberleninka.ru/article/n/pravovoe-regulirovanie-zaschity-informatsii-otnosyascheysya-k-sfere-chastnoy-zhizni-grazhdan-v-grazhdanskom-zakonodatelstve-i/viewer> (дата обращения: 16.12.2024).

15. Новицкая И. Н. Правовая защита персональных данных в Российской Федерации // Молодой ученый. — 2024. — № 18 (517). — С. 244-246. — URL: <https://moluch.ru/archive/517/113510> (дата обращения: 18.08.2024).

16. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024): [сайт]. — URL: <http://pravo.gov.ru/proxy/ips/?docbody&nd=102108261> (дата обращения: 13.09.2023).

17. О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных: Федеральный закон от 19 декабря 2005 г. №160-ФЗ: [сайт]. — URL: <https://base.garant.ru/12143756/> (дата обращения: 13.09.2024).

18. О связи: Федеральный закон № 126-ФЗ от 07.07.2003 (ред. от 01.12.2023): [сайт]. — URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102082548> (дата обращения: 13.09.2023).

19. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022): [сайт]. — URL: https://www.consultant.ru/document/cons_doc_LAW_61798/c3b53a3601408c50895476568264472cfd0a83bc/ (дата обращения: 19.09.2023).

20. Об основах охраны здоровья граждан в Российской Федерации: Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 26.09.2024): [сайт]. — URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102152259> (дата обращения: 25.09.2024).

21. 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: постановление Правительства Российской Федерации от 21 марта 2012 г. № 211: [сайт]. — URL: http://pravo.gov.ru/proxy/ips/?doc_itself=&nd=102154754&page=1&rdk=3#I0 (дата обращения: 28.09.2023).

22. Об утверждении перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 № 188: ред. от 13.07.2015: [сайт]. — URL:

http://pravo.gov.ru/proxy/ips/?docbody=&link_id=0&nd=102046005&intelsearch=&firstDoc=1 (дата обращения: 28.04.2024).

23. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119: [сайт]. — URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102160483> (дата обращения: 28.02.2023).

24. Об утверждении требований к подтверждению уничтожения персональных данных: приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 г. № 179: официальный интернет-портал правовой информации: [сайт]. — URL: <http://publication.pravo.gov.ru/Document/View/0001202211290008?ysclid=lgkdhm4cwm460091589> (дата обращения: 13.05.2023).

25. Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных к распространению: приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 года № 18 // Официальный интернет-портал правовой информации: [сайт]. — URL: <http://publication.pravo.gov.ru/document/0001202104210039> (дата обращения: 17.08.2024).

26. Определение Верховного Суда РФ от 05.03.2018 г. № 307-КГ18-101 Об отказе в передаче жалобы в Судебную коллегия Верховного Суда Российской Федерации: [сайт]. — URL: <https://www.garant.ru/products/ipo/prime/doc/71793774/?ysclid=lgjtkp7amv583450820> (дата обращения: 13.05.2023).

27. Определение Московского городского суда от 10.11.2016 № 33-38783/2016: [сайт]. — URL: <https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/19d661b0-6b14-48eb-b753-9adbf19fe32a> (дата обращения 12.10.2023)

28. Определение Пятого кассационного суда общей юрисдикции от 28.09.2021 № 88–7100/2021: [сайт]. — URL: https://5kas.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&cas

e_id=5299996&case_uid=afde134a-632f-4e02-9b8e-

edb573eef771&new=2800001&delo_id=2800001 (дата обращения: 19.12.2023).

29. Платонова Н. И. Современные правовые подходы к пониманию биометрических данных: [сайт]. - URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=114228> (дата обращения 24.05.2024).

30. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. Постановлением Правительства РФ от 15 сентября 2008 г. № 687): [сайт]. — URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102124251> (дата обращения: 15.09.2024).

31. Постановление мирового судьи судебного участка № 2 Апатитского судебного района Мурманской области от 05 февраля 2020 года № 5-17/2020: [сайт]. - URL: https://2ap.mrm.msudrf.ru/modules.php?name=sud_delo&op=cs&case_id=7820164&delo_id=1500001 (дата обращения 24.06.2024).

32. Постановление мирового судьи судебного участка ЗАТО г. Заозерска Кольского судебного района Мурманской области от 31.07.2023 года № 5-84/2023: [сайт]. - URL: https://zzk.mrm.msudrf.ru/modules.php?name=sud_delo&op=cs&case_id=42400153&delo_id=1500001 (дата обращения 10.12.2023).

33. Постановление Тринадцатого арбитражного апелляционного суда от 01.07.2016 № А56-6698/2016: [сайт]. - URL: <https://sudact.ru/arbitral/doc/J8ihyq5cYyo1/?ysclid=lgjsc8zp1z312118129> (дата обращения: 16.08.2024).

34. Правила оказания услуг телефонной связи (утв. постановлением Правительства Российской Федерации от 24.01.2024 № 59 «О порядке оказания услуг телефонной связи»: [сайт]. — URL: https://www.consultant.ru/document/cons_doc_LAW_468098/466d42f281ea110e3eda3c7bc023787675b533d (дата обращения: 10.09.2024).

35. Решение Московского районного суда города Твери Тверской области от 18.02.2016 № 12-24/2016: [сайт]. - URL: <https://moskovsky-->

twr.sudrf.ru/modules.php?name=sud_delo&name_op=case&_uid=2ecf9caf-7be9-4b6c-9878-74a99d713729&deloId=1502001&caseType=0&new=0&srv_num=3&hideJudge=0 (дата обращения 25.03.2023).

36. Решение Обоянского районного суда Курской области от 10.08.2017 № 2-318/2017: [сайт]. - URL: <https://sudact.ru/regular/doc/qHAaFCDKoflt> (дата обращения: 16.04.2023).

37. Решение Первомайского районного суда города Мурманска от 27.05.2022 № 2-1877/2022: [сайт]. - URL: https://perv--mrm.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=170672290&case_uid=95fe355e-ff05-411e-ae6b-29b10f206f4f&delo_id=1540005 (дата обращения: 12.12.2024).

38. Решение Подпорожского городского суда Ленинградской области от 14.12.2020 № 2-335/2020: [сайт]. - URL: https://podporozhsky--lo.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=213910044&case_uid=b15f9045-0e4e-46c5-b1f4-d7f47389c568&delo_id=1540005 (дата обращения: 17.12.2023).

39. Решение Таганского районного суда города Москвы от 19.12.2018 № 02-4261/2018: [сайт]. - URL: <https://mos-gorsud.ru/rs/taganskij/services/cases/civil/details/c5e2b24f-3000-4eb3-babb-27718caf62e4> (дата обращения 13.11.2024).

40. Рожкова М. А. Характеристики больших данных, значимые для целей гражданского права: [сайт]. - URL: <https://rozhkova.com/pdf/2019-06.pdf> (дата обращения: 07.11.2024).

41. Рузанова В. Д. Персональные данные как гражданско-правовая категория: [сайт]. - URL: <https://cyberleninka.ru/article/n/personalnye-dannye-kak-grazhdansko-pravovaya-kategoriya> (дата обращения: 16.12.2024)

42. Савин М. П. Анализ судебных решений в области защиты права на изображение и имя в отношении физических лиц: [сайт]. — URL: <https://moluch.ru/archive/189/47982> (дата обращения: 11.08.2023).

43. Скрипник Д. А. Обеспечение безопасности персональных данных : учебное пособие // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/89449.html> (дата обращения: 12.02.2024).

44. Стриганова Т.М. Защита чести, достоинства и деловой репутации граждан: [сайт]. — URL: <https://cyberleninka.ru/article/n/zaschita-chesti-dostoinstva-i-delovoy-reputatsii-grazhdan/viewer> (дата обращения: 12.05.2024).

45. Трудовой кодекс Российской Федерации: Федеральный Закон Российской Федерации от 30.12.2001 № 197-ФЗ ред. от 19.12.2022, с изм. от 11.04.2023: [сайт]. - URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102074279> (дата обращения: 15.09.2024).

46. Шаблинский И. Г. Правовое регулирование информационных отношений в сфере обработки персональных данных: учебное пособие для вузов: [сайт]. - URL: <https://urait.ru/book/pravovoe-regulirovanie-informacionnyh-otnosheniy-v-sfere-obrabotki-personalnyh-dannyh-544886> (дата обращения: 17.12.2024)

47. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981: [сайт]. - URL: <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm> (дата обращения: 17.10.2024).

48. Gruber S., Neumayr B., Schuetz C.G., Schrefl M., Fabianek C., Gringinger E. Towards informed watermarking of personal health sensor data for data leakage detection //Lecture Notes in Computer Science. 2021. Т. 12617 LNCS. С. 109-124.

49. Newman N., Fletcher R., Schulz A., Andi S., Robertson C. T., Nielsen R. K. Reuters Institute digital news report 2021: [сайт]. - URL: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital_News_Report_2021_FINAL.pdf (дата обращения: 17.12.2022).

50. The Personal Information Protection and Electronic Documents Act (PIPEDA) 13.04.2000: [сайт]. -URL: <https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf> (дата обращения: 18.05.2023).

51. What is Personal Data? 09.03.2023: [сайт]. -URL: <https://www.privacypolicies.com/blog/personal-data> (дата обращения: 15.09.2024).