

ИНСТИТУТ ПРАВА

Кафедра «Конституционное и административное право»

Правовое обеспечение государственного управления и местного самоуправления

на тему «**Конституционно-правовые основы защиты персональных данных**»

Тольятти 2017

СОДЕРЖАНИЕ

Введение.....	3
Глава 1. Понятие персональных данных и их защита.....	8
1.1 Понятие персональных данных и гарантии их защиты.....	8
1.2 Исторический аспект защиты персональных данных.....	15
1.3 Нормативно-правовое обеспечение защиты персональных данных в зарубежных странах.....	23
1.4 Нормативно-правовое обеспечение защиты персональных данных в Российской Федерации.....	36
Глава 2. Особенности получения, передачи и защиты персональных данных отдельных категорий субъектов.....	41
2.1 Особенности получения, передачи и защиты персональных данных работников организаций.....	41
2.2 Особенности получения, передачи и защиты персональных данных несовершеннолетних.....	48
2.3 Ответственность за нарушение законодательства в области защиты персональных данных.....	50
Глава 3. Практический анализ конституционно-правовых основ защиты персональных данных.....	56
3.1 Статистические данные правовых вопросов защиты персональных данных.....	56
3.2 Анализ судебно-правовой практики при нарушении защиты персональных данных.....	62
3.3 Проблемы и перспективы развития конституционно-правовой защиты персональных данных.....	79
Заключение.....	86
Список использованных источников.....	91
Приложение.....	100

Введение

С развитием Всемирной сети Интернет у государства появились новые заботы – как обезопасить миллионы людей от несанкционированного использования их личных данных в мошеннических, либо других незаконных целях. Ежедневно в Сети совершается множество операций, предусматривающих, что человек даст доступ к определенному набору собственных данных и абсолютное большинство людей, не имеет ни малейшего понятия об элементарных правилах безопасности поведения в Интернете. Поэтому, государство старается возложить обязанности по защите персональных данных на организации, которые используют эти самые данные.

Основным законом, регулирующим обработку персональных данных различными субъектами, является Федеральный закон «О персональных данных» от 27.07.2006 года №152-ФЗ (далее – закон 152-ФЗ). Под его сферу попадают субъекты, которые осуществляют действия по обработке персональных данных с применением средств автоматизации (учитывая информационно-телекоммуникационные сети), либо без использования таких средств, при условии, что подобные действия позволяют совершать поиск или предоставлять доступ к персональным данным в базах, размещенных на материальном носителе или находящихся в картотеках, либо других систематизированных собраниях данных. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» определяет:

1. Основные понятия, связанные с обработкой персональных данных;
2. Принципы и условия обработки персональных данных;
3. Обязанности оператора;
4. Права субъекта персональных данных;
5. Виды ответственности за нарушение требований, установленных Федеральным законом № 152-ФЗ;

6. Государственные органы, осуществляющие контроль и надзор за соблюдением требований, установленных Федеральным законом № 152-ФЗ.

Не попадают под сферу регулирования закона 152-ФЗ следующие действия:

- обработка чужих персональных данных физическими лицами для собственных нужд (личных и семейных), при условии, что такая обработка не нарушает права владельца персональных данных;
- действия по организации архивов, которые попадают в сферу регуляции законодательства об архивном деле в РФ;
- обработка персональных данных, которые содержат сведения, отнесенные в соответствии с действующим законодательством РФ, к государственной тайне;
- персональные данные, относящиеся к деятельности судов, предоставленные в порядке, закрепленном соответствующими законодательными актами.

Актуальность работы обосновывается также и тем, что в рамках конституционных норм нет непосредственных гарантий на защиту персональных данных. Но международно-правовые нормы все-таки оказывают соответствующее притязание на российское законодательство и изучение проблемы защиты персональных данных в конституционно-правовом аспекте становится все более популярным.

В настоящее время институт «персональных данных» в России регулируется рядом нормативных актов. При этом, как отмечают авторы, «практически во всех законах присутствуют нормы о правах граждан – субъектов персональных данных, хотя и с различной степенью разработанности. Во многих актах закреплены нормы об ответственности за нарушения в работе с персональными данными».

В первую очередь, неприкосновенность частной жизни гарантируется Конституцией Российской Федерации, а персональные данные являются важнейшей составляющей частной жизни.

Далее необходимо отметить, что действующее трудовое законодательство нацелено на обеспечение безопасности персональных данных, как в частном секторе, так и на государственной службе. Так, ТК РФ в главе 14 определяет общие положения защиты персональных данных работника: понятие, требования, особенности хранения, передачи, права работников и ответственность за нарушение норм.

Федеральный закон № 152-ФЗ «О персональных данных» описывает организационно-правовые механизмы защиты персональной информации любого физического лица. Однако в отношении данных закон не указывает, распространяются ли его нормы на персональные данные работников.

Отметим, что в отличие от работников частного сектора, в отношении защиты персональных данных государственных гражданских служащих действуют дополнительные нормативные акты. Так, п. 4. ст. 42 № 79-ФЗ «О государственной гражданской службе Российской Федерации» устанавливаются условия получения и обработки персональных данных, доступа субъекта к данным, а также их передача третьим лицам. При этом при работе с персональными данными с использованием средств автоматизации и технических средств необходимо руководствоваться Постановлением от 17.11.2007 г. № 781.

В целом, несмотря на наличие ряда основополагающих документов, в существующем нормативно-правовом поле нет единых и исчерпывающих положений, связанных с организационно-правовой защитой персональных данных работников.

Обработка персональных данных обусловлена общими требованиями, которые строятся на базе принципов добровольности, обеспечения равенства возможностей, законности, не допущения дискриминации в трудовых отношениях. Соответственно этим требованиям, содержащихся в нормативно-правовых актах трудового законодательства России, должны соответствовать и не противоречить локальные нормативные акты различных

организаций и предприятий, дабы не ущемлять и не нарушать законные интересы гражданина Российской Федерации.

Целью исследования в данном исследовании является анализ конституционно-правовых основ защиты персональных данных. Для достижения поставленной цели необходимо выполнить следующие задачи:

- дать понятие персональных данных и определить гарантии их защиты;
- рассмотреть исторический аспект защиты персональных данных;
- проанализировать нормативно-правовое обеспечение защиты персональных данных в зарубежных странах и Российской Федерации;
- изучить особенности получения, передачи и защиты персональных данных работников организаций, несовершеннолетних;
- представить данные об ответственности за нарушение законодательства в области защиты персональных данных;
- провести статистический анализ данных правовых вопросов защиты персональных данных;
- проанализировать судебно-правовую практику при нарушении защиты персональных данных;
- рассмотреть проблемы и перспективы развития конституционно-правовой защиты персональных данных.

Объектом исследования в научно-исследовательской работе является персональные данные субъекта Российской Федерации. Предметом исследования – конституционно-правовые основы защиты персональных данных.

При написании работы использовались следующие методы исследования: теоретический анализ и обобщение научной литературы, обобщение опыта практической работы.

Теоретическая значимость работы заключается в том, что результаты, полученные в ходе исследования дополняют точку зрения авторов, работающих по данной теме. Практическая значимость работы заключается в

том, что результаты исследования могут использоваться в дальнейшем развитии защиты в области персональных данных.

Теоретической и методологической базой исследования явились нормативно-правовые акты законодательства Российской Федерации, а также труды следующих авторов: Авакьян С. А., Авдеев М. Ю., Алексеев С. С., Алистархов В., Амелин Р. В., Богатырева Н. В., Волков Ю. В., Марченко Ю. А., Федосин А. С., Бадьина А., Бархатова Е. Ю., Давыдова Е. В., Егорова О. А., Беспалов Ю. Ф. Н., Кистяковский Б. А., Кротов А. В., Кузнецова Т. В., Курбатов А. Я., Лаптев В. В., Шахматов В. П., Левина М. И., Лушников А., Медведева Т. М., Панкова О. В., Новиков В. А., Савельев А. И., Серков П. П., Свирин Ю. А., Ситникова Е. Г., Сенаторова Н. В., Терещенко Л. К. Хужокова И. М., Якушев В.С.

Объем диссертационной работы – 101 страница. Структура работы: научно-исследовательская работа состоит из введения, основной части из двух глав (в первой главе дано понятие персональных данных и их защита, вторая глава содержит практический анализ конституционно-правовых основ защиты персональных данных), заключения, списка используемой литературы и приложений.

Глава 1. Понятие персональных данных и их защита

1.1 Понятие персональных данных и гарантии их защиты

Персональные данные – это любая информация, относящаяся к прямо или косвенно определённомому или определяемому физическому лицу – субъекту персональных данных. Таким образом, это могут быть любые сведения, идентифицирующие человека, в том числе: ФИО, дата рождения, место жительства, семейное положение, сведения об образовании и профессиональной деятельности, финансовое положение, факты биографии, деловые и личные качества человека и пр.

Под обработкой персональных данных понимается любое действие (операция) или их совокупность, с применением средств автоматизации или без них для их сбора, хранения, использования, предоставления, удаления.

Анализируя конституционно-правовые рамки защиты персональных данных можно отметить, что в Конституции отсутствует положение, которое напрямую бы закрепляло «право на защиту персональных данных». Вместе с тем, отдельные положения существуют, и необходимо разобраться, какие именно нормы гарантируют защиту персональных данных.

Так, статья 23 Конституции России устанавливает право на неприкосновенность частной жизни, личную и семейную тайну. Также гарантируется право на тайну переписки, телефонных переговоров. Ограничение данного права допускается только на основании судебного решения. Положения статьи 24 Конституции РФ перекликаются с ФЗ «О персональных данных» в части прямого запрета на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия¹.

¹ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ

Определенную сложность представляет соотношение между понятиями «персональные данные», установленным ФЗ «О персональных данных» и термином «частная жизнь», используемым в тексте Конституции РФ, но не имеющем нормативного закрепленного определения. По мнению автора, термин «частная жизнь» имеет более широкое определение и включает в себя и персональные данные человека.

Категория «информация о частной жизни субъекта» представляется достаточно сложной для ее определения, так как практически невозможно определить точно термин «частная жизнь» вследствие отсутствия единого подхода к этому понятию.

Для отечественной конституционно-правовой доктрины характерно такое понимание частной жизни, в соответствии с которым к ней относится «не широкий спектр отношений, а узкая сфера интимных, бытовых и семейных отношений, не Данный вывод, как представляется, находит подтверждение и в практике Конституционного Суда РФ, который рассматривает право на неприкосновенность частной жизни в качестве «фундаментального права», «в обеспечение» которого Конституция РФ закрепляет «иные личные права», в том числе право на тайну коммуникаций и право на неприкосновенность жилища»².

В настоящее время вопрос обработки персональных данных находится в секторе внимания абсолютно любой организации. В текущих реалиях трудно найти организацию, которая не обрабатывала бы персональные данные своих сотрудников.

С момента заключения трудовых отношений хотя бы с одним гражданином, организация становится оператором персональных данных и, соответственно, принимает на себя обязанности по защите указанной

от 30.12.2008 №6-ФКЗ, от 30.12.2008 №7-ФКЗ, от 21.07.2014 N 11-ФКЗ). // «Собрание законодательства РФ», 04.08.2014, №31, ст. 4398.

² Семейный кодекс Российской Федерации от 29.12.1995 №223-ФЗ (ред. от 30.12.2015). // «Российская газета», №17, 27.01.1996.

информации, становится поднадзорной контролирующим органам, т.н. «регуляторам» (которых на сегодняшний день три).

В свою очередь, любой гражданин в процессе своей жизни вступает во взаимоотношения с различными физическими и юридическими лицами. В результате данного взаимодействия накапливаются данные о конкретном индивиде, начиная с простых (фамилии, имени, отчестве) и заканчивая специфическими (сведения о здоровье, сведения о судимости, биометрические данные). При этом, гражданин может не желать, чтобы эти сведения становились известными широкому кругу лиц. В целях защиты указанной информации используется специальный правовой режим персональных данных. Для обеспечения данного правового режима в 2006 году был принят отдельный Федеральный закон «О персональных данных». Периодически, в него вносятся поправки, касающиеся обработки персональных данных и принимаются новые подзаконные нормативно-правовые акты, направленные на конкретизацию его норм, так последние поправки вступили в силу в сентябре 2015 года.

Тем не менее, по прошествии уже почти 10 лет, у сотрудников служб информационной безопасности возникают трудности в применении действующих правовых норм, регулирующих данную сферу общественных отношений, в связи с чем и представляется целесообразным рассмотрение вопросов обработки персональных данных работников и их защиты.

Система права – совокупность правовых форм, внутренне упорядоченная по отношениям, обеспечивающим относительную самостоятельность и единство этой совокупности, которое выражается в ее интегральных, обеспечительных и координационных свойствах и функциях. Это определение охватывает существенные признаки, как системы права, так и ее подсистем: отраслей, подотраслей, институтов. Структурными элементами системы права (подсистемами) являются: отрасль, подотрасль, институт, субинститут и норма права.

Вопрос о том, какое место в системе права занимает институт персональных данных, является на сегодняшний день наименее изученным. Несмотря на важность данного института с практической точки зрения, сегодняшняя юридическая наука практически не имеет научных работ, посвященных его изучению.

Возможными причинами этого является, во-первых, то, что, защита персональной информации чаще всего понимается чисто технической задачей, то есть защитой от утечки, защиты от несанкционированного доступа, покушения на имущество и так далее. В таком ракурсе образовывается смещение акцентов в чисто техническую область. Но сама защита персональных данных – безопасность персональных данных субъекта, который дает свои данные какому-либо государственному органу или частной организации, то есть защита именно его прав³.

Другой возможной причиной этого является то, что нормы регулирующие обработку персональных данных принято считать частью института неприкосновенности частной жизни.

Одна из основных идей, которая имеет место во многих исследовательских работах, такова: права субъекта персональных данных – это юридическая конструкция, производная от прав человека, сконцентрированная в источниках международного права.

Скорее всего, необходимо различать два понятия – персональные данные и тайну частной жизни. Тайна частной жизни (личная и семейная тайна) – достаточно широкое понятие, не получившее точного нормативного закрепления и, в ряде случаев, охватывающее персональные данные. Тем не менее, отдельно взятые факты о лице, такие как фамилия, имя, отчество, место работы, адрес и т.п., а также сведения о большинстве повседневных событий, связанных с этим лицом, не всегда могут считаться тайной,

³ Алексеев С. С. Структура советского права, М., «Юрид. лит.», 1975, 264 с.

поскольку по своему характеру эти сведения являются общедоступными и могут быть произвольно получены любым случайным лицом.

В понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит непротивоправный характер. В противовес этому, персональные данные, как правило, являются своего рода идентификатором субъекта в человеческом обществе.

Институт тайны частной жизни защищает от умышленного вмешательства в личную жизнь, которое, как правило, выражается в нарушении тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, о чем прямо указано в Конституции Российской Федерации (ст. 23). Термин персональные данные, в свою очередь, тесно связан с понятием обработка. Обработка персональных данных начинается тогда, когда гражданин «свободно, своей волей и в своем интересе» (на что прямо указано в ч. 1 ст. 9 Федерального закона «О персональных данных») передает свои данные оператору для выполнения каких либо функций (например, заключение трудового договора) или делает их общедоступными (например, регистрируясь в социальных сетях).

В статье 5 Федерального закона «О персональных данных» указано, что целью данного закона является предоставление защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. По такой формулировке следует, что институт частной жизни является составной частью института персональных данных, причем тоже в некоторой его части. В свете изложенного, представляется, что необходимо отграничивать институт персональных данных от института неприкосновенности частной жизни⁴.

⁴ Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 21.07.2014). // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3451.

В настоящее время институт «персональных данных» в России регулируется рядом нормативных актов. При этом, как отмечают авторы, «практически во всех законах присутствуют нормы о правах граждан – субъектов персональных данных, хотя и с различной степенью разработанности. Во многих актах закреплены нормы об ответственности за нарушения в работе с персональными данными».

В первую очередь, неприкосновенность частной жизни гарантируется Конституцией Российской Федерации, а персональные данные являются важнейшей составляющей частной жизни.

Далее необходимо отметить, что действующее трудовое законодательство нацелено на обеспечение безопасности персональных данных, как в частном секторе, так и на государственной службе. Так, ТК РФ в главе 14 определяет общие положения защиты персональных данных работника: понятие, требования, особенности хранения, передачи, права работников и ответственность за нарушение норм.

Федеральный закон № 152-ФЗ «О персональных данных» описывает организационно-правовые механизмы защиты персональной информации любого физического лица. Однако в отношении данных закон не указывает, распространяются ли его нормы на персональные данные работников.

Отметим, что в отличие от работников частного сектора, в отношении защиты персональных данных государственных гражданских служащих действуют дополнительные нормативные акты. Так, п. 4. ст. 42 № 79-ФЗ «О государственной гражданской службе Российской Федерации» устанавливаются условия получения и обработки персональных данных, доступа субъекта к данным, а также их передача третьим лицам. При этом при работе с персональными данными с использованием средств автоматизации и технических средств необходимо руководствоваться Постановлением от 17.11.2007 г. № 781.

В целом, несмотря на наличие ряда основополагающих документов, в существующем нормативно-правовом поле нет единых и исчерпывающих

положений, связанных с организационно-правовой защитой персональных данных работников.

Персональные данные работника подлежат обработке руководителем с учетом действующего законодательства и локальных нормативных правовых актов. Под такой обработкой следует рассматривать деятельность, представляющую собой совокупность правоотношений, возникающих в процессе формирования информационных ресурсов, основанных на получении, хранении, комбинировании и документировании информации о работнике в рамках действующего трудового законодательства. Субъектами рассматриваемых правоотношений являются работник, представитель работника, работодатель, должностные лица работодателя, уполномоченные им на обработку персональных данных работника, а также иные лица, имеющие право получать и предоставлять информацию о работнике.

Правовое регулирование процедур, связанных с обработкой персональных данных работника, осуществляется в том числе и через так называемое локальное нормотворчество – «локальные нормативные акты», разрабатываемые и утверждаемые работодателем, которые распространяются на сотрудников конкретных организаций. В таких нормативных документах могут содержаться как конкретные рекомендации относительно порядка обработки персональных данных работника, так и вопросы, связанные с предоставлением персональных данных, их объемах, формах и т.д.

Среди целей, стоящих перед работодателем, осуществляющим обработку персональных данных работника, следует выделить: определение профессиональной пригодности работника; содействие в трудоустройстве на наиболее подходящую для него должность; обучение работника; обеспечение соблюдения законодательства, прав и законных интересов работника в течение всего периода трудовых отношений; обеспечение безопасности работника при выполнении им служебных обязанностей; обеспечение эффективности использования имущества предприятия и его сохранности; контроль за качеством выполняемой работы.

Перечисленные выше общие требования к обработке персональных данных работника базируются на соблюдении принципов добровольности, законности, обеспечения равенства возможностей, исключения дискриминации в сфере трудовых отношений. Аналогичные требования, не противоречащие трудовому законодательству Российской Федерации, должны содержаться и в локальных нормативных правовых актах предприятий и организаций с учетом специфики трудовой деятельности. Априори локальные нормы не могут противоречить трудовому и иному законодательству Российской Федерации и каким-либо образом ущемлять права и нарушать законные интересы работника.

В соответствии с положениями закона обеспечение защиты персональных данных является прямой обязанностью операторов персональных данных, а это практически все предприятия Российской Федерации.

За неисполнение требований законом предусмотрена юридическая ответственность. Санкции применяются как к руководителям индивидуально, так и к предприятиям в целом, вплоть до прекращения обработки персональных данных или аннулирования лицензии на основной вид деятельности компании.

В целом защита персональных данных представляет собой сложный технологический процесс, предупреждающий нарушение конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности компании. А обязанность по организации такого комплексного процесса всецело возложена на работодателя (оператора). За нарушение положений законодательства о персональных данных при обработке персональных данных работников виновные лица привлекаются к дисциплинарной, материальной, гражданско-правовой, административной⁴⁰ и уголовной ответственности.

1.2 Исторический аспект защиты персональных данных

Все цивилизованные государства современности уделяют особое внимание защите прав граждан, что является одним из основных проявлений демократии. Обеспечение безопасности личности, в том числе безопасности информационной, является одной из приоритетных задач любого демократического государства, строящегося на основах уважения принципов правового государства, а равно прав и основных свобод человека.

Таким образом, обеспечение конфиденциальности персональных данных как неотъемлемой части безопасности личности требует особого внимания государства и специального законодательного урегулирования.

В ходе активного формирования Глобального информационного общества планеты Земля одну из ключевых позиций занимает функция свободного обмена информацией между народами. Вместе с тем, не вызывает сомнений существующая необходимость обеспечения такой фундаментальной ценности как уважение неприкосновенности личной сферы.

Защита частной жизни имеет давнюю историю. Еще в дореволюционный период этот вопрос привлекал внимание ученых-юристов. Правовые нормы, являющиеся составной частью неприкосновенности частной жизни, относящиеся к неприкосновенности корреспонденции, уже имели место в Почтовом уставе 1857 г. и в Уставе о телеграфах 1876 г.⁵

В период Советского Союза конституционно были закреплена неприкосновенность личности, жилья, тайны переписки. Также в 1977 году появились нормы телефонных и телеграфных переговоров. Но при этом гражданам давалось недостаточно правовых гарантий на

⁵ Федеральный закон от 03.04.1995 №40-ФЗ «О Федеральной службе безопасности» (от 06.07.2016 N 374-ФЗ). // «Российская газета», N 72, 12.04.1995.

неприкосновенность тайны личной жизни, существовало определенное ограничение данных прав⁶.

В целях совмещения этих двух фундаментальных ценностей 28 января 1981 г. в Страсбурге была принята Конвенция Совета Европы о защите личности в связи с автоматической обработкой персональных данных⁷. Данный документ, регламентирующий вопросы защиты персональных данных, является основополагающим в этом направлении.

Целью Конвенции является обеспечение на территории ратифицировавших данный документ стран уважения прав и основных свобод каждого человека независимо от его гражданства или места жительства и в особенности его права на неприкосновенность личной сферы в связи с автоматической обработкой, касающихся его персональных данных⁸.

Конвенция вступила в силу 1 октября 1985 г. В настоящее время в ней участвуют практически все европейские государства. Зарубежный опыт защиты персональных данных имеет уже более чем вековую историю. Так, во Франции публикации фактов о частной жизни были запрещены и установлены штрафы для нарушителей ещё в 1858 г. А норвежский уголовный кодекс запретил публикацию информации, касающейся «персональных и частных дел» в 1889 г.

8 ноября 2001 г. Конвенция подписана от имени Российской Федерации (см. сообщение МИД России от 8 ноября 2001 г.), а ратифицирована Федеральным законом от 19.12.2005 № 160-ФЗ.

⁶ Терещенко Л. К. Отдельные вопросы применения законодательства о персональных данных // Комментарий судебной практики / под ред. К. Б. Ярошенко. М.: КОНТРАКТ, 2014. Вып. 19. С. 3 – 13.

⁷ Конвенции Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных (ETS N 108) (заключена в г. Страсбурге, 28 января 1981 г.). // «Бюллетень трудового и социального законодательства РФ», №4, 2014.

⁸ Новиков В. А. Неприкосновенность частной жизни как конституционное право и объект уголовно-правовой охраны // Юридический мир. 2014. N 7. С. 18 – 21.

Ратификация этого документа Российской Федерацией стала большим шагом на пути к обеспечению в РФ неприкосновенности личной сферы.

Далее, 22 ноября 1991 года начался следующий этап развития института неприкосновенности персональной жизни граждан. Ознаменовался этот принятием Декларации прав и свобод человека, которая в статье 9 дала гарантии на неприкосновенность личной жизни, переписки, сообщений и переговоров. При этом прослеживался один принципиальный момент – наличие определенного судебного порядка при ограничении анализируемых прав.

Обозначенная линия неприкосновенности частной жизни прослеживается и в Конституции Российской Федерации 1993 г. (ст. ст. 23, 24). Статья 23 Конституции гарантирует каждому «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». Статья 24 установила запрет на «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия»⁹.

Таким образом, следующим уровнем обеспечения конфиденциальности персональных данных является конституционное закрепление этих прав. В частности в статье 23 говорится, что «каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени», а также «право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения». Статья же 24 устанавливает норму, в соответствии с которой «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются», а «органы

⁹ Федеральный закон от 20.02.1995 №24-ФЗ «Об информации, информатизации и защите информации» (от 06.07.2016 N 374-ФЗ). // «Российская газета», №39, 22.02.1995.

государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом»¹⁰.

Непосредственный термин «персональные данные» в законодательстве Российской Федерации сформировался в середине 1990-х годов, при этом определяя правые черты данного понятия.

В ныне утратившем силу ФЗ от 20.02.1995 №24 «Об информации, информатизации и защите информации» существовала категория конфиденциальной информации, куда были отнесены персональные данные, также в федеральном законе был прописан текст статьи 24 Конституции РФ, дававший право на разглашение тайны личной жизни только с согласия гражданина, либо на основании судебного решения. Но само определение термина «персональные данные» было раскрыто не достаточно, если не полностью. Указ Президента РФ №188 от 06.03.1997 года исправил этот недостаток созданием перечня конфиденциальных сведений, по которому персональные данные это «сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность»¹¹.

Характер правового режима ФЗ от 20.02.1995 №24 «Об информации, информатизации и защите информации» был схож с европейской моделью законодательства о защите персональных данных. Но существовало принципиальное различие, которое имеет место и в настоящее время в федеральном законе №152 от 27.07.2006 «О персональных данных» и его

¹⁰ Конвенции Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных (ETS N 108) (заключена в г. Страсбурге, 28 января 1981 г.). // «Бюллетень трудового и социального законодательства РФ», №4, 2014.

¹¹ Терещенко Л. К. Отдельные вопросы применения законодательства о персональных данных // Комментарий судебной практики / под ред. К. Б. Ярошенко. М.: КОНТРАКТ, 2014. Вып. 19. С. 3 – 13.

подзаконных актах: акцентирование за защиту персональной информации в отрыве от защиты прав гражданина на неприкосновенность личных данных.

В 2005 году Российская Федерация взяла на себя обязательства привести законодательство о персональных данных в соответствии с Конвенцией Совета Европы (от 28 января 1981 г.) о защите физических лиц при автоматизированной обработке персональных данных. Таким образом, ФЗ №152 от 27.07.2006 «О персональных данных» вписывался в рамки данных обязательств, практически не отличаясь от норм Конвенции Совета Европы. Страны Европейского Союза не остановились на достигнутом, и в настоящее время там работают положения Директив 95/46/ЕС и 97/66/ЕС, которые регламентируют четкую сбалансированность юридических и технических требований при защите и обработке персональных данных, в ряде случаев именно соразмерности, обоснованности и выполнимости не хватает российскому законодательству для полноценного развития рынка.

Статья 85 Трудового Кодекса РФ содержала в себе понятие о персональных данных работника, которое вносило конкретику в общее понятие персональных данных, но принятие ФЗ №99 от 07.05.2013 «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», отменило действие данной статьи.

Действующая ныне редакция ФЗ №152 от 27.07.2006 «О персональных данных» под персональными данными подразумевает информацию, которая относится прямо или косвенно к физическому лицу. Данное определение сформировалось из-за изменений от 25.07.2011 года в данный законодательный акт. Ранее это определение помимо любой информации,

относящейся к физическому лицу относило и его ФИО, дату рождения, положение, образование, доходы и т.п.¹²

Получается из определения исчезло лишь перечисление той информации, которая относится к персональным данным. Поскольку конструкция данной нормы представляла собой открытый перечень, то исключение этого перечня не повлекло особых изменений в существе понятия «персональные данные». Основным критерий остался прежним: относимость информации к конкретному лицу и возможность его идентификации.

Соответственно, судебная практика имеет претенденты споров о том, какие категории данных относить к персональным. Работники спорят о законности попытки работодателей получить сведения о них по месту учебы, по месту исполнения должностных обязанностей. При этом замечены споры об отнесении фамилии работника к персональным данным, которая в любом случае фигурирует в любом запросе, часто доводя ситуацию с ограничениями использования персональных данных до абсурда.

Вместе с тем, по мнению Л. К. Терещенко, наличие такого перечня в первоначальной редакции Закона сыграло важную роль, поскольку давало представление о характере информации, отнесенной законодателем к персональным данным. Несмотря на то, что Федеральный закон «О персональных данных» содержит максимально широкое определение персональных данных, в практической деятельности нередко возникают проблемы с определением того, какая информация относится к персональным данным. Отсутствие перечня в отдельных случаях, в том числе и в судебной практике, позволяет по-разному толковать отнесение тех или иных категорий данных к персональным¹³.

¹² Якушев В.С. О понятии правового института // Правоведение. 1970. №6. С. 62–63.

¹³ Федеральный закон от 20.02.1995 №24-ФЗ «Об информации, информатизации и защите информации» (от 06.07.2016 N 374-ФЗ). // «Российская газета», №39, 22.02.1995.

Широкое толкование и отсутствие перечня информации относящейся к персональным данным, порождают следующие два негативных момента: во-первых, непонимание операторов (организаций обрабатывающих персональные данные), что необходимо относить к персональным данным и, во-вторых, широкие возможности контролирующих органов по привлечению операторов к ответственности за непредоставление сведений об обработке персональных данных. Так в судебной практике имеются решения судов по спору между территориальными органами Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций и операторами персональных данных, в которых последним вменялось отсутствие в уведомлениях об обработке определенных категорий персональных данных. Представляется, что наличие умысла организаций на совершение указанных действий маловероятно.

Изложенное даёт основания сделать вывод, что в последнее время в России широкое распространение получила порочная практика распространения и незаконного использования как самих баз персональных данных, так и различных незаконных способов их получения (в большей мере программных). Конфиденциальные базы персональных данных, причём разного уровня конфиденциальности — незаконно полученные как из коммерческих структур (охраняемые в соответствии режимом секретности коммерческой либо профессиональной тайны), так и из государственных органов, персональные данные в которых охраняются в соответствии с режимом служебной тайны — свободно продаются на рынках и в сети Интернет.

Человек не может чувствовать себя защищённым, пока существует угроза вторжения в частную жизнь посторонних лиц — как из праздного любопытства, так и с целью совершения мошеннических и других противоправных действий. А обеспечение безопасности граждан, их основных прав и свобод является главнейшей функцией государства. В связи с этим в России предпринимаются определённые шаги по

законодательному урегулированию этой области общественных отношений. Мы, в отличие от западных стран, имеющих уже более чем вековую историю государственного обеспечения и защиты неприкосновенности личной сферы, находимся только в начале этого пути и в процессе создания эффективной и работоспособной системы защиты персональных данных предстоит преодолеть не одно препятствие, однако конструктивное начало уже положено. Ратифицировав Конвенцию, Россия установила «планку», к которой теперь необходимо стремиться. И главный шаг в этом направлении уже сделан: разработана и введена в действие законодательная база — как законы (Закон РФ № 149-ФЗ от 27.07.2006, Закон РФ № 152-ФЗ от 27.07.2006) в качестве основы, регулирующей всю массу общественных отношений в этой области, так и ряд подзаконных нормативных актов, направленных на реализацию установлений законов, разъясняющих их положения и регламентирующих отдельные материальные и процессуальные вопросы.

1.3 Нормативно-правовое обеспечение защиты персональных данных в зарубежных странах

За последние 20 с небольшим лет были приняты несколько международных документов, определяющих основные принципы защиты частных интересов в области персональных данных. На основе этих принципов построены правовые системы многих национальных законодательств, касающиеся данной сферы.

Ниже перечислены эти документы в порядке их создания.

1. Рекомендации Совета Организации по экономическому сотрудничеству и развитию (ОЭСР), касающиеся основных положений о защите неприкосновенности частной жизни и международных обменов персональными данными от 23 сентября 1980 года;

2. Конвенция Совета Европы о защите личности в связи с автоматической обработкой персональных данных от 28 января 1981 года;

3. Рекомендации относительно компьютерных файлов персональных данных, принятые Генеральной ассамблеей ООН 14 декабря 1990 года;

4. Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных.

Основные принципы защиты частных интересов, содержащиеся в том или ином объеме во всех перечисленных документах следующие:

— персональные данные должны собираться и обрабатываться (храниться, использоваться, раскрываться, стираться и т.д.) корректно и законно;

— персональные данные должны быть адекватными заранее определенным целям и распоряжение ими должно ограничиваться по срокам, соответствующим указанным целям;

— персональные данные должны быть точны;

— персональные данные должны обрабатываться только с согласия субъектов данных;

— персональные данные должны быть доступны субъектам этих данных, в том числе и для внесения уточнения в эти данные;

— персональные данные должны быть должным образом защищены.

Все перечисленные принципы относятся ко всем структурам (государственным, частным, общественным), работающим с персональными данными.

Нет необходимости раскрывать конкретные положения каждого из перечисленных принципов. Следует только отметить, что во всех указанных международных документах содержатся исключения. При этом главным критерием для возможности ограничения прав субъектов персональных данных и симметричного расширения прав распорядителей этими данными

является безопасность гражданина, общества, государства при соблюдении фундаментальных прав и свобод граждан-субъектов персональных данных.

Следует отметить также, что все международные документы предписывают создание соответствующей властной структуры, которая должна обеспечивать гарантии субъектов персональных данных и регулировать оборот этих данных. Эта структура должна иметь полномочия и обязанности:

- принимать и рассматривать жалобы, связанные с нарушением законных интересов всех сторон;
- проводить расследования, связанные с надзором за соблюдением законодательства в области персональных данных;
- вмешиваться в процесс обработки персональных данных;
- обращаться в суды для возбуждения дел по факту нарушения соответствующего законодательства;
- отчитываться перед обществом о своей деятельности.

Важность данной структуры определяется тем обстоятельством, что она должна быть главным механизмом, позволяющим контролировать и управлять всем оборотом персональных данных во всех секторах — государственном, частном, общественном.

Как было сказано выше, одним из важнейших ресурсов информации, носящей персональный характер, являются регистры данных, поддерживаемые государственными (властными) органами на всех уровнях.

Для примера можно привести Соединенные Штаты, где различные ведомства, как на федеральном уровне, так и на уровне штатов и местном уровне поддерживают огромное число баз данных, содержащих персональную информацию. Вот только ничтожная часть таких специализированных баз данных:

- лицензия на управление транспортным средством;
- право на владение землей;

- сведения о налогах на собственность;
- лицензия на вид деятельности;
- лицензия на огнестрельное оружие;
- участие в судебных процессах;
- сведения о банкротстве;
- привлечение к гражданской или к уголовной ответственности;
- вклады в политические кампании;
- материалы Комиссии по ценным бумагам и биржам;
- информация о финансовом положении;
- лицензии на охоту и рыболовство;
- владение судами, самолетами и другими средствами передвижения;

На основании данных, которыми обладают американские государственные учреждения, можно составить детальное представление о любом индивидууме, пользуясь исключительно доступными документами (в скобках приведены соответствующие публичные регистры):

- жилая собственность, займы под жилье, оценочная стоимость жилья (право на владение землей, сведения о налогах на собственность);
- родители (акты гражданского состояния);
- номер в системе социального страхования (лицензия на управление транспортным средством);
- рост и вес (лицензия на управление транспортным средством);
- имя, адрес, пол, дата рождения (лицензия на управление транспортным средством, акты гражданского состояния);
- коррекция зрения, некоторые медицинские данные (лицензия на управление транспортным средством);
- некоторые профессии (лицензия на вид деятельности);
- данные автомобиля и ссуда на автомобиль (регистрационные документы транспортного средства);

- членство в партии и частота участия в выборах (регистрация избирателя);
- некоторые увлечения (лицензии на охоту/рыболовство);
- суда/самолеты в собственности (соответствующие лицензии);

Это только небольшая часть информации, которая может быть извлечена из данных, находящихся в распоряжении американских властей. Информация может быть гораздо обширнее, если данное лицо участвовало в судебных процессах в качестве ответчика или истца, исполняло обязанности члена суда присяжных, разводилось, участвовало в процедурах банкротства, было указано в завещаниях. Информация расширяется еще больше, если данное лицо зафиксировано Комиссией по ценным бумагам и биржам в качестве обладателя акций, если оно получало студенческие стипендии, государственные ссуды на жилье, ссуды на ведение малого бизнеса и т.д.

Если государство в целом рассматривается как некая корпорация, «акционерами» которой являются все члены общества (в том числе буквальными акционерами по праву налогоплательщика), то вся информация, которой распоряжается государство, должна служить интересам как всего общества, так и отдельных его членов, а, значит, быть доступной. Если этот тезис можно считать безусловным по отношению к правовой, коммерческой (госзакупки), научной и другой неперсонифицированной информации, то в случае с персональными данными право каждого гражданина на получение информации (знать то, что ему необходимо, о другом гражданине), сталкивается с конституционным правом любого на защиту своих частных интересов, в том числе на защиту своей персональной информации. Это столкновение интересов не имеет тривиального решения, как, например, полный запрет на доступ к любой персональной информации, находящейся в распоряжении государства. Такой подход может привести к прямо противоположному результату, такому, например, как появление на российском рынке баз данных МВД.

Поэтому очевидно, что правила, на основании которых существуют государственные (публичные) регистры и по которым происходит доступ к информации, содержащейся в этих регистрах, должны учитывать два обстоятельства.

Одним обстоятельством является необходимость доступа к этой информации для выполнения необходимых действий или функций (деятельность государственных ведомств, использование данных для выполнения действий на рынке, поиск лиц, вопросы, связанные с недвижимостью, расследование, связанное с правонарушениями или уголовными преступлениями и т.д.). Это обстоятельство является аргументом для свободного доступа к данным, содержащимся в регистрах.

С другой стороны, существуют причины, по которым следует ввести строгое ограничение, а иногда и запрет на доступ к информации в публичных регистрах. Среди этих многих причин обязательность предоставления в регистры информацию о себе (например, в случае заполнения анкеты избирателя), тотальный характер некоторых регистров (например, актов гражданского состояния), «чувствительность» многих данных, наконец, требования по обеспечению защищенности (в том числе от физического насилия) тех, чьи персональные данные находятся в этих регистрах.

Разумеется, эти два обстоятельства (конкурирующих интересов) присутствует всегда, когда речь заходит об эффективной работе публичных регистров. Однако способы достижения баланса интересов в значительной мере зависят от специфики информации, содержащейся в регистрах. Например, баланс, который должен существовать в случае регистра недвижимости, явно отличается от того, который присущ регистру избирателей.

Тем не менее, можно обозначить основные универсальные принципы, относящиеся ко всем публичным регистрам. Их можно разделить на две категории: правила доступа к информации:

— доступ может быть разрешен только к конкретной записи, содержащейся в регистре, а не ко всему массиву документов, что, в первую очередь, должно означать невозможность извлечь весь массив информации;

— доступ может быть разрешен только исходя из конкретной цели, что должно исключить также получение всей полноты информации, относящейся к субъекту данных.

— принципы контроля над деятельностью регистра:

— существование регистра должно быть обусловлено необходимыми документами (законами, распоряжениями и т.п.);

— должны быть обозначены допустимые цели использования данных, содержащихся в регистре;

— статус регистра должен содержать все необходимые правила, которым подчиняется данный регистр (правила поиска, получения информации и т.п.);

— ведомство, поддерживающее регистр, должно выполнять необходимые требования по защите информации и обеспечению логирования пользователей;

— лица, нарушающие требования по доступу к информации и ее использованию, должны нести соответствующую ответственность;

— должны существовать механизмы, позволяющие субъектам данных ограничить доступ к своей персональной информации.

Описанный подход применяется в национальных законодательствах. Примером может служить закон Новой Зеландии «О защите частных интересов» (Privacy Act 1993), содержащий главу, посвященную публичным регистрам. Закон содержит 4 основных принципа, которым должны следовать пользователи и распорядители регистра:

— поиск информации только с использованием поисковых механизмов и индексации, специально предназначенных для данного регистра;

- запрещение комбинировать информацию, полученную из данного регистра с информацией, полученной из других аналогичных регистров;
- запрещение электронной передачи данных из регистра, кроме передачи конкретной запрошенной информации;
- ограничение, накладываемое на прибыльность регистра.

В законе сформулированы также положения, дающие право Комиссару по персональным данным разрабатывать кодексы ведения конкретных публичных регистров и предписывать ведомствам исполнять требования этих кодексов. Закон поручает также Комиссару расследовать каждый случай нарушения положений данного закона и привлекать нарушителей к ответственности в установленном законодательством порядке.

Как было сказано выше, нормы, относящиеся к конкретным публичным регистрам, могут и должны отражать специфику информации, содержащейся в данном регистре. Самым известным примером в данном случае является американский закон «О защите частных интересов водителей» (The Driver's Privacy Protection Act of 1994, 18 USC Part I, Chapter 123), принятый Конгрессом после громкого скандала, связанного с убийством известной телевизионной актрисы ее обожателем-маньяком. Данные, необходимые убийце для отслеживания актрисы, он получил в калифорнийском департаменте по лицензированию водителей. Следует отметить, что важность данного закона для Соединенных Штатов была обусловлена, в первую очередь, тем известным фактом, что лицензия на управление автомобилем фактически является одним из основных гражданских документов и содержит информацию (например, о физическом состоянии владельца и текущем месте жительства), которая отсутствует в паспортных данных. Кроме этого, на уровне штатов (в отличие от федерального уровня) не существовало ограничений на раскрытие персональной информации, определяемых общенациональным законодательством.

Закон 1994 года уже распространяется на департаменты штатов, ответственные за выдачу и учет лицензий на вождение (водительских удостоверений), и запрещает раскрытие этими департаментами персональных данных, содержащихся в регистрах. Закон содержит также исключения из этого запрещения, которые распространяются на следующие категории пользователей, действующих в соответствии с положениями законодательства:

- государственные ведомства;
- автомобильные компании и их авторизованные дилеры;
- страховые компании;
- частные сыскные агентства, обладающие соответствующей лицензией;
- местные муниципальные власти в конкретных случаях (например, при отбуксировании автомобиля, препятствующего движению автотранспорта).

При этом закон жестко регламентирует предоставление так называемой «строго ограниченной информации» (фотографии владельца, его номера социального страхования, информации о здоровье или нетрудоспособности). Тем не менее, закон предоставляет субъектам данных право снимать запрет на общий доступ (в том числе с целью последующей продажи) к их персональной информации, которая может быть использована, в частности, в маркетинговых целях.

Необходимость (и неизбежность) существования рынка персональных данных (в первую очередь, услуг по предоставлению информации персонального характера) не подлежит сомнению. Этот рынок может существовать в виде хаоса, когда не существует никаких норм, определяющих оборот персональных данных, либо в виде упорядоченной системы отношений. Следует также обратить внимание на то, что наличие

законов, прямо или *de facto* запрещающих оборот персональных данных, неизбежно приведет к «теневому» обороту, что еще хуже, чем хаос.

Общие нормы, регулирующие оборот персональных данных, содержатся в принципах, перечисленных в приведенных международных документах. Большинство национальных законодательств построено с учетом этих принципов. Однако очевидно, что сами по себе эти принципы (особенно, если учесть неизбежные исключения из них, необходимые для развития самого рынка персональных данных и отраслей, где использование персональных данных критически важно) не могут полностью составить правовую базу для оборота персональных данных.

Из общих соображений следует, что регулирование рынка персональных данных может осуществляться в нескольких формах, важнейшими из которых являются:

- законодательные акты или разделы законодательных актов, имеющие прямое отношение к обороту персональных данных на рынке;
- национальные стандарты, имеющие рекомендательный характер;
- кодексы поведения, требования которых добровольно исполняются участниками корпоративных объединений.

В качестве примера закона следует отметить закон Австралии «О защите частных интересов» (Privacy Act 1988), дополненный и исправленный в 2001 году, в котором сформулированы Национальные принципы защиты частных интересов, относящиеся исключительно к рынку персональных данных.

Эти принципы, как и весь закон в целом, являются развитием Рекомендаций Организации по международному сотрудничеству и развитию и, в частности, содержат следующие регулятивные положения.

1. Сбор персональной информации (Компания должна, по возможности, собирать персональную информацию от субъекта данных);

2. Раскрытие и использование информации (Компания может использовать информацию во вторичных целях, если они имеют отношение к первичным целям, для которых информация собиралась. Закон содержит положения, относящиеся к прямому маркетингу, если он является вторичной целью);

3. Открытость (Компания должна издать и сделать общедоступным документ, описывающий ее политику в области персональных данных);

4. Доступ и изменения (Компания должна обеспечить доступ субъекта данных к своим персональным данным. Закон содержит исключение, позволяющее компании отказать в этом доступе на конкретных коммерческих основаниях. Компания должна по запросу субъекта данных предпринять шаги по исправлению или дополнению информации о нем или пояснить причины, по которым это не сделано);

5. Идентификаторы данных (Компания не имеет право использовать в качестве собственных идентификаторов (а значит, и включать их в механизм поиска информации) идентификаторы, присвоенные субъекту персональных данных государственным ведомством);

6. Оборот медицинских данных (Закон содержит положения, ограничивающие оборот подобных данных).

Примером национального стандарта, регулирующего оборот персональных данных на рынке, является канадский Модельный свод правил по защите персональной информации, утвержденный в качестве стандарта законом «О защите персональной информации и электронных документах» (The Personal Information Protection and Electronic Documents Act, 2000). Свод правил содержит, в частности, следующие положения.

1. Ответственность компании за персональную информацию, которой она обладает (Компания должна назначить лицо, ответственное за политику и практику своей деятельности в этой сфере);

2. Цели сбора (Компания должна определить цели сбора и пояснить их субъекту данных, если информация получается от него);

3. Согласие субъекта данных на сбор, использование и раскрытие персональных данных (В общем случае требуется согласие субъекта данных на использование его персональных данных. Однако свод правил содержит допустимые исключения для необходимости получения согласия. В первую очередь, это относится к сфере прямого маркетинга, к случаям сбора долгов с субъекта данных или выполнению судебного решения. Свод правил содержит также описание возможных форм получения согласия (в частности, с использованием процедур, принятых в интернете));

4. Доступ субъектов данных к информации о них (Свод правил, предписывая в общем случае обязанность компании предоставлять такой доступ, содержит ряд допустимых исключений, в частности по коммерческим соображениям и в случае использования этих данных в суде или адвокатской деятельности).

Одним из самых интересных и важных кодексов поведения, добровольно принимаемых на себя компаниями, работающими в сфере оборота персональных данных, являются Принципы индустрии, принятые американской корпоративной организацией Individual Reference Services Group — IRSG Group. Этот кодекс имеет чрезвычайно важное значение для американского рынка в первую очередь потому, что компании, входящие в данную корпоративную организацию (US Search.com Inc., Acxiom Corporation, CDB Infotek, Database Technologies, Inc. (DBT), DCS Information Systems, Dolan Media Company, First Data Solutions LLC, LEXIS-NEXIS, LOCATEPLUS.COM, OPEN, Pinkerton Services Group, United Reporting Publishing Corporation (URPC), West Group), контролируют львиную долю рынка по предоставлению (продаже «в розницу») персональных данных американских граждан.

Принципы индустрии учитывают характер предоставляемой информации и имеют положения, применяемые к конкретным типам информации:

1. Публичные документы и общедоступная информация (Информация, полученная из открытых источников, распространяется без всяких ограничений);

2. Необщедоступная информация (Не общедоступная информация может предоставляться без ограничений только компетентным подписчикам, которые прошли проверку на надежность и безукоризненное соблюдение требований Принципов. Возможно предоставление не общедоступной информации другим профессиональным или коммерческим структурам, если из нее исключены данные, отражающие кредитную и финансовую истории, медицинские данные, девичью фамилию матери, точный номер социального страхования и данные о рождении. При этом подписчики должны принять на себя обязательства по выполнению требований Принципов).

Принципы индустрии требуют от компаний-членов IRSG Group, чтобы:

- соблюдались необходимые меры безопасности при работе с персональными данными (в том числе с точки зрения лояльности сотрудников);

- соблюдался принцип открытости политики и практики компаний;

- субъекту данных по его запросу предоставлялось право ограничить доступ к его персональным данным;

- в доступных пределах субъекту данных по его запросу был предоставлен доступ к его персональным данным, если этот доступ не ограничен обязательствами компании, в частности перед правительственными ведомствами;

- не предоставлялись данные о лицах, не достигших 18 лет.

Принципы индустрии требуют также от компаний-членов IRSG Group, чтобы источники информации обладали хорошей репутацией, а данные были получены законным образом. От компаний-членов IRSG Group требуется также, чтобы были приняты меры, обеспечивающие точность используемой информации.

Ввиду важности для Соединенных Штатов существования механизмов регулирования оборота персональных данных на рынке, Принципы индустрии были проанализированы Федеральной торговой комиссией (Federal Trade Commission — ФТК), после чего ФТК представила в Конгресс в декабре 1997 года доклад, в котором отмечалась важность инициативы компаний и высокие качества Принципов. Тем не менее, ФТК отметила, что возможная неточность информации и отсутствие права субъекта данных на получение сведений о том, кому эта неточная информация была предоставлена, понижают уровень гарантии граждан. ФТК предложила компаниям-членам IRSG Group, чтобы были усилены права субъектов данных по корректировке своих персональных данных.

1.4 Нормативно-правовое обеспечение защиты персональных данных в Российской Федерации

В настоящее время институт «персональных данных» в России регулируется рядом нормативных актов. При этом, как отмечают авторы, «практически во всех законах присутствуют нормы о правах граждан — субъектов персональных данных, хотя и с различной степенью разработанности. Во многих актах закреплены нормы об ответственности за нарушения в работе с персональными данными».

В первую очередь, неприкосновенность частной жизни гарантируется Конституцией Российской Федерации, а персональные данные являются важнейшей составляющей частной жизни. Обозначенная линия неприкосновенности частной жизни прослеживается и в Конституции Российской Федерации 1993 г. (ст. ст. 23, 24). Статья 23 Конституции гарантирует каждому «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». Статья 24 установила запрет на «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия»¹⁴.

Также для развития нормы о неприкосновенности частной жизни и в связи с ратификацией Российской Федерацией ряда международных актов, в Трудовой Кодекс была включена глава 14 «Защита персональных данных». В ней определяются общие положения защиты персональных данных работника: понятие, требования, особенности хранения, передачи, права работников и ответственность за нарушение норм.

Кроме того, в качестве нормативно-правового источника защиты персональных данных, можно отметить: ФЗ №149 «Об информации, информационных технологиях и защите информации». Необходимо отметить, что действующее трудовое законодательство нацелено на обеспечение безопасности персональных данных, как в частном секторе, так и на государственной службе.

Помимо Конституции РФ, основным законом, регулирующим обработку персональных данных различными субъектами, является Федеральный закон «О персональных данных» от 27.07.2006 года №152-ФЗ (далее – закон 152-ФЗ). Под его сферу попадают субъекты, которые осуществляют действия по обработке персональных данных с применением средств автоматизации (учитывая информационно-телекоммуникационные сети), либо без использования таких средств, при условии, что подобные действия позволяют совершать поиск или предоставлять доступ к персональным данным в базах, размещенных на материальном носителе или находящихся в картотеках, либо других систематизированных собраниях данных. Не попадают под сферу регулирования закона 152-ФЗ следующие действия:

¹⁴ Федеральный закон от 20.02.1995 №24-ФЗ «Об информации, информатизации и защите информации» (от 06.07.2016 N 374-ФЗ). // «Российская газета», №39, 22.02.1995.

- обработка чужих персональных данных физическими лицами для собственных нужд (личных и семейных), при условии, что такая обработка не нарушает права владельца персональных данных;
- действия по организации архивов, которые попадают в сферу регуляции законодательства об архивном деле в РФ;
- обработка персональных данных, которые содержат сведения, отнесенные в соответствии с действующим законодательством РФ, к государственной тайне;
- персональные данные, относящиеся к деятельности судов, предоставленные в порядке, закрепленном соответствующими законодательными актами.

Федеральный закон № 152-ФЗ «О персональных данных» описывает организационно-правовые механизмы защиты персональной информации любого физического лица. Однако в отношении данных закон не указывает, распространяются ли его нормы на персональные данные работников.

Отметим, что в отличие от работников частного сектора, в отношении защиты персональных данных государственных гражданских служащих действуют дополнительные нормативные акты. Так, п. 4. ст. 42 № 79-ФЗ «О государственной гражданской службе Российской Федерации» устанавливаются условия получения и обработки персональных данных, доступа субъекта к данным, а также их передача третьим лицам. При этом при работе с персональными данными с использованием средств автоматизации и технических средств необходимо руководствоваться Постановлением от 17.11.2007 г. № 781.

Опираясь на теорию права можно провести анализ института персональных данных.

Так, предметом указанного института являются общественные отношения, связанные с обработкой персональных данных осуществляемой государственными и муниципальными органами, юридическими и физическими лицами с использованием средств. Указанный институт

содержит разветвленный понятийный аппарат. Так, в частности, статья 3 Федерального закона «О персональных данных» содержит в себе такие дефиниции как: «персональные данные», «оператор», «обработка персональных данных», «автоматизированная обработка персональных данных», «обезличивание персональных данных», «информационная система персональных данных», «трансграничная передача персональных данных» и т. п.

Кроме того, указанная сфера жизнедеятельности на сегодняшний день является относительно обособленной и имеет целый арсенал источников, содержащих в себе как нормы материального права (федеральные законы) так и нормы процессуального права (подзаконные нормативные акты) предписывающие процедуры, которые обязан провести оператор персональных данных по защите обрабатываемой им информации.

Статья 5 Федерального закона «О персональных данных» содержит принципы и условия обработки персональных данных. Анализ указанных принципов и иных норм, содержащихся в указанном Федеральном законе и изданных в соответствии с ним подзаконных нормативных актов позволяет сделать вывод о том, что для данного института характерен преимущественно императивный метод правового регулирования.

Таким образом, очевидно, что рассмотренная выше совокупность правовых норм, регулирующих общественные отношения, связанные с обработкой персональных данных и их защитой имеет все присущие самостоятельному правовому институту отличительные черты.

Для определения места данного института в системе права Российской Федерации следует обратиться к классификации. Как известно, существует деление права на частное и публичное, материальное и процессуальное.

Проведенный выше анализ показывает, что институт персональных данных относится к публичной отрасли права. В то же время, нормы данного института находят свое отражение и в такой традиционно отнесенной к частному праву отрасли как трудовое (главе 14 ТК РФ).

Таким образом, очевидно, что указанный правовой институт регулирует общественные отношения, относящиеся к нескольким отраслям права, т.е. находящиеся на стыке отраслей, поэтому, по мнению автора, указанный правовой институт следует рассматривать как межотраслевой.

В целом, несмотря на наличие ряда основополагающих документов, в существующем нормативно-правовом поле нет единых и исчерпывающих положений, связанных с организационно-правовой защитой персональных данных работников.

Обработка персональных данных обусловлена общими требованиями, которые строятся на базе принципов добровольности, обеспечения равенства возможностей, законности, не допущения дискриминации в трудовых отношениях. Соответственно этим требованиям, содержащихся в нормативно-правовых актах трудового законодательства России, должны соответствовать и не противоречить локальные нормативные акты различных организаций и предприятий, дабы не ущемлять и не нарушать законные интересы гражданина Российской Федерации.

Глава 2. Особенности получения, передачи и защиты персональных данных отдельных категорий субъектов

2.1 Особенности получения, передачи и защиты персональных данных работников организаций

Общие правила обращения с персональными данными установлены Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ), а непосредственно в трудовых отношениях – дополнительно главой 14 Трудового кодекса РФ (далее – ТК РФ).

Персональные данные – это любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу – субъекту персональных данных. Таким образом, это могут быть любые сведения, идентифицирующие человека, в том числе: ФИО, дата рождения, место жительства, семейное положение, сведения об образовании и профессиональной деятельности, финансовое положение, факты биографии, деловые и личные качества человека и пр.

Под обработкой персональных данных понимается любое действие (операция) или их совокупность, которые совершаются с использованием или без использования средств автоматизации, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

С незапамятных времен государство, кредиторы и работодатели запрашивали или требовали от граждан самую разную информацию — имя, адрес, дату рождения и т.п. Граждане предоставляли эту информацию, получая взамен защиту, различные услуги или приобретения. Позже, кроме того, страхователи, частные сыскные структуры, юристы и новостные

репортеры добывали подобную информацию для своих профессиональных целей.

Что, собственно, изменилось в последнее время, что вызывает к проблеме персональной информации такой повышенный интерес? С наступлением эры компьютеров и телекоммуникационных технологий, доступ к персональной информации, ее объемы, возможность быстро получать и компилировать данные из различных источников привели к тому, что технологическое количество перешло в новое качество. Снизилась затраты (времени, усилий, финансовых средств) на получение подобной информации, что сделало обработку и предоставление заказчику персональной информации, особенно на западе, не только рентабельным, но и высокодоходным бизнесом.

Итак, рынок персональной информации возник в результате следующих факторов:

- данные в подавляющем большинстве стали представляться и обрабатываться в электронном виде;
- стало легко комбинировать данные, полученные из разных баз данных (источников);
- возросшее быстродействие компьютеров позволяет производить любую необходимую обработку информации, содержащей персональные данные;
- стоимость хранения данных и доступа к их массивам резко снизилась;
- персональные компьютеры превратились в общедоступное средство;
- возникший интернет завершил формирование среды информационного обмена, связанного с персональными данными.

Работодатель вправе обрабатывать только те персональные данные, которые ему необходимы в целях обеспечения соблюдения законодательства, содействия работникам в трудоустройстве, получении образования и

продвижении по службе, обеспечения их личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Персональные данные могут содержаться, к примеру, в анкете или автобиографии; в документе, удостоверяющем личность гражданина; в личной карточке № Т-2; в трудовой книжке; в свидетельствах о заключении брака, рождении ребёнка; в документах воинского учёта; в документах об образовании; в справках о доходах с предыдущего места работы; в документах обязательного пенсионного страхования; в трудовом договоре и в других документах.

Все персональные данные следует получать у самого работника и только с его согласия, если иное не установлено законом. Если их можно получить только от третьей стороны, работника нужно уведомить об этом заранее и получить его письменное согласие. При этом ему нужно сообщить:

- о целях получения персональных данных;
- о способах их получения;
- о характере подлежащих получению персональных данных;
- о последствиях отказа дать письменное согласие на их получение.

Работодатель не вправе получать и обрабатывать:

- персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности;
- специальные категории персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, установленных законом.

Порядок получения согласия на обработку персональных данных регламентирован в ст. 9 Закона № 152-ФЗ.

Согласно разъяснениям Роскомнадзора согласие на получение персональных данных требуется и от соискателей, в том числе:

— от претендента на замещение вакантной должности на период принятия работодателем решения о приёме либо отказе в приёме на работу: при поступлении резюме по каналам электронной почты, факсимильной связи; при сборе персональных данных посредством типовой формы анкеты соискателя, утверждённой работодателем. Если же от имени соискателя действует кадровое агентство, с которым у него заключён договор, или если соискатель самостоятельно разместил своё резюме в сети Интернет, предоставив доступ к нему неограниченному кругу лиц, получать согласие не требуется;

— для включения соискателя в кадровый резерв работодателя.

Согласия на обработку персональных данных не требуется, если обработка необходима для исполнения договора, стороной которого является субъект персональных данных. По мнению ФНП России, это правило распространяется и на стороны трудового договора.

Не требуется согласия на обработку персональных данных работника (соискателя), получаемых, в частности:

— из документов (сведений), предъявляемых при заключении трудового договора в соответствии со ст. 65, ч. 4 ст. 275 ТК РФ;

— по результатам обязательного предварительного медицинского осмотра о состоянии здоровья;

— в объёме, предусмотренном унифицированной формой № Т-215, в том числе персональных данных близких родственников, и в иных случаях, установленных законодательством РФ (получение алиментов, оформление допуска к государственной тайне, социальных выплат);

В случаях, предусмотренных федеральным законодательством, не требуется получать согласие на обработку персональных данных уволенного работника. Например, в случае если обработка персональных данных осуществляется в рамках бухгалтерского и налогового учёта.

Работодатель не может сообщать третьей стороне персональные данные работника без его письменного согласия. Например, если от сторонней организации поступил запрос о предоставлении письменной характеристики в отношении вашего сотрудника. Без письменного согласия сообщить третьим лицам персональные данные можно только в случае, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных ТК РФ или иными федеральными законами. Например, когда необходимо представить сведения в ПФР РФ, ФСС РФ или по запросу правоохранительных органов, а также органов безопасности, государственных инспекторов труда при осуществлении ими государственного контроля и надзора за соблюдением трудового законодательства по их мотивированным запросам. Мотивированный запрос должен содержать:

- указание цели запроса;
- ссылку на правовые основания запроса, в том числе подтверждающие полномочия органа, направившего запрос;
- перечень запрашиваемой информации.

По этой же самой причине направление персональных данных работников в орган ЦЗН при проведении процедуры сокращения численности или штата не будет противоречить действующему законодательству о защите персональных данных. Ведь это обязанность работодателя.

А вот если запрос поступил из организации, не обладающей соответствующими полномочиями, согласие получить нужно.

Например, в случае если организация планирует провести аудит бухгалтерской (финансовой) отчетности, в том числе в целях подтверждения правильности расчётов по заработной плате с работниками. Проводится ли аудит в обязательном или добровольном порядке, правового значения не имеет. Кроме того, работодатель обязан предупредить лиц, получающих

персональные данные работника, о том, что эти данные могут быть использованы только в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило будет (было) соблюдено.

Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя, базируются на главном принципе свободы доступа работника к своим персональным данным, в том числе на праве получения копии любой записи, содержащей такие данные.

Это право корреспондируется с обязанностью работодателя на основании письменного заявления работника не позднее 3 рабочих дней выдать ему безвозмездно надлежащим образом заверенные копии документов, связанных с работой (приказ о приёме на работу, приказ об увольнении, выписку из трудовой книжки, справку о заработной плате и т. п.). На дистанционных работников это положение тоже распространяется, но с учётом особенностей, установленных гл. 49.1 ТК РФ.

Работники также имеют право:

- на полную информацию о своих персональных данных и их обработке;
- на доступ к медицинской документации, отражающей состояние его здоровья, с помощью медицинского специалиста по его выбору;
- обжаловать в суд любые неправомерные действия или бездействие работодателя при обработке и защите их персональных данных. Защищать свои персональные данные они могут самостоятельно либо через представителя. Таким представителем может выступать профсоюз либо иное лицо (как физическое, так и юридическое).
- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства. Если работодатель отказывается выполнять это требование, работник может заявить ему о своём несогласии в письменной форме с соответствующим обоснованием. Если речь идёт о персональных данных оценочного характера, работник вправе дополнить их заявлением, выражающим его собственную точку зрения.

Обязанности работодателя по защите персональных данных

Защиту персональных данных работника от неправомерного их использования или утраты работодатель обеспечивает за счёт своих средств. Работодателю необходимо:

- установить порядок хранения и использования персональных данных работников в локальном нормативном акте – Положении о персональных данных. Здесь должен быть закреплён, в частности, перечень персональных данных, обрабатываемых в организации, порядок доступа работника к своим персональным данным и вопросы защиты последних от неправомерного использования или утраты. Работников организации нужно ознакомить с этим документом, а также с их правами и обязанностями в этой области. Его отсутствие может быть квалифицировано государственной инспекцией труда как нарушение трудового законодательства;

- назначить ответственное за организацию обработки персональных данных лицо;

- установить конкретный перечень работников, которые имеют доступ к персональным данным других работников (например, руководитель, бухгалтер, кадровик). А с такими работниками работодателю необходимо оформить письменное обязательство о неразглашении конфиденциальных сведений;

- вести журналы учёта персональных данных, в которых будет чётко отражено, кто, когда имел доступ, к каким персональным данным, каких работников и с какой целью;

- при использовании электронных систем хранения и обработки персональных данных обеспечить их защиту в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных;

- по требованию работника работодатель обязан известить всех лиц, которым ранее были сообщены неверные или неполные персональные

данные этого работника, обо всех произведённых в них исключениях, исправлениях или дополнениях.

В целом защита персональных данных представляет собой сложный технологический процесс, предупреждающий нарушение конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности компании. А обязанность по организации такого комплексного процесса всецело возложена на работодателя (оператора). За нарушение положений законодательства о персональных данных при обработке персональных данных работников виновные лица привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности.

2.2 Особенности получения, передачи и защиты персональных данных несовершеннолетних

Персональные данные детей, которые еще не достигли совершеннолетия, теперь находятся под защитой официального законодательства России. Официальное ведомство Российской Федерации Роскомнадзор в ходе запланированной проверки обнаружило ряд грубых нарушений законодательства, касающихся размещения персональных данных детей на сайтах.

Прежде всего, под прицелом оказались такие данные детей, как их адреса, телефоны, а также места работы родителей. Кроме того, некоторые сайты имели в открытом доступе информацию о том, к какой социальной группе относятся семьи учеников. Что касается фотографий, существует закон «О защите персональных данных», согласно которому без разрешения человека публиковать его фото запрещено. В случае фотографий детей разрешение необходимо со стороны его родителей или законных представителей. Такая же ситуация и с фамилией и именем ребенка.

Однако законодатели признают, что единой формы решения этой проблемы пока нет. В частности, недоразумения в этом плане могут случаться в детском саду или школе. В общем виде формулировки закона сводятся к тому, что без разрешения публиковать фотографии и персональные данные (Ф.И.О., номер телефона, адрес) нельзя, а значит, имея разрешение — можно.

Соответственно, все, что нужно сделать педагогам, это взять письменное разрешение родителей или законных представителей о возможности использования персональных данных детей с уточнением, каких именно персональных данных. Такое разрешение можно спросить у родителей сразу при поступлении в образовательное учреждение либо каждый год, либо для каждого мероприятия.

Впрочем, о мероприятиях разговор отдельный. Статья 152.1 Гражданского кодекса РФ говорит, что согласие не требуется в случаях, если:

- использование изображения осуществляется в государственных, общественных или иных публичных интересах;

- изображение гражданина (в том числе несовершеннолетнего гражданина) получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и тому подобном), за исключением случаев, когда такое изображение является основным объектом использования;

- гражданин (в этом случае, безусловно, речь уже идет о совершеннолетнем) позировал за плату.

Вывод: руководствуясь Гражданским кодексом РФ, фотографии детей с публичных мероприятий можно публиковать без проблем и опасений, а фотографии, где отдельно взятый ребенок, например, сидит за партой и решает задачу, — нельзя.

Подобные проблемы говорят в пользу того, что в любом случае лучше взять разрешение на публикацию фотографий и персональных данных

(Ф.И.О.) и уведомлять родителей о публикации тех или иных информации в сети. Ведь, публикуя что-либо в Интернете, вы публикуете это навсегда. И ребенок даже через много лет может иметь последствия от публикации, сделанной, когда он был в детском саду. Без крайней необходимости не публикуйте в сети ФИО детей, сведения о них (а это — персональные данные) и их фотографии.

Надо знать, что за публикацию фотографий детей в Интернете без согласия их родителей предусмотрена ответственность по статье 137 Уголовного кодекса РФ. В случае, если суд признает вину, лицо, опубликовавшее фотографию, будет наказано штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода за период до 18 месяцев, либо обязательными работами на срок от 120 до 180 часов, либо исправительными работами на срок до 1 года, либо арестом на срок до 4 месяцев.

2.3 Ответственность за нарушение законодательства в области защиты персональных данных

Глубокое проникновение информационных технологий в частную жизнь, возрастающая роль использования интеллектуальных мобильных устройств, становление человека частью интернет-пространства привели к новому этапу в обработке персональных данных. Возможности для сбора, хранения и обработки информации расширяются и становятся повсеместно доступными для широкого круга лиц.

В информационном обществе личность напрямую или опосредованно находится под постоянным влиянием со стороны других участников информационного взаимодействия. Очевидно, что в многочисленных интернет-предложениях персональная информация выступает в качестве своего рода незаменимой валюты, используемой для оплаты таких услуг. Это означает, что растущие рынки, помимо их преимуществ, несут определенные

риски для благосостояния пользователя, его права на конфиденциальность и защиту данных.

В этом отношении технологические и социальные изменения, с одной стороны, безусловно, положительно повлияли на граждан: для профессиональной деятельности, отдыха, безопасности, развития личности или социального взаимодействия, но с другой – представляют дополнительный риск, обусловленный противоправным или некомпетентным использованием информации и технологий ее обработки и распространения. В этой связи в современных условиях человек зачастую теряет личный контроль над распространением информацией о себе, о своей личной жизни.

Таким образом, новые риски требуют решений, адаптированных к текущим обстоятельствам, обеспечивающих высокий уровень защиты.

Одним из знаковых событий 2015 года в области персональных данных стало вступление в силу с 1 сентября 2015 года Федерального закона от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» (далее – Закон № 242-ФЗ, Закон о локализации персональных данных).

Данным законом была установлена обязанность операторов обеспечить при сборе персональных данных российских граждан их хранение на территории Российской Федерации, внесены изменения в содержание уведомления о начале обработки персональных данных, а также введен порядок ограничения доступа к информации в сети Интернет, обрабатываемой с нарушением законодательства в области персональных данных.

Дополнительно в целях обеспечения принципа прозрачности реализации возложенных полномочий по контролю за соблюдением Закона № 242-ФЗ на официальном сайте Роскомнадзора была размещена схема взаимодействия

Роскомнадзора с операторами персональных данных иностранной юрисдикции по проверке исполнения Закона № 242-ФЗ (Приложение 1).

Вступление указанного закона в силу также было ознаменовано возложением на Уполномоченный орган новых полномочий в части ведения реестра нарушителей прав субъектов персональных данных. На первоначальном этапе реализации этих полномочий стояла задача по обеспечению соответствующей нормативной правовой базы.

Постановлением Правительства Российской Федерации от 19 августа 2015 № 857 были утверждены Правила создания, формирования и ведения автоматизированной информационной системы «Реестр нарушителей прав субъектов персональных данных». Приказами Роскомнадзора утверждены Порядок взаимодействия оператора реестра с провайдером хостинга, Порядок получения доступа к информации, содержащейся в реестре нарушителей прав субъектов персональных данных, оператором связи, а также форма заявления субъекта персональных данных о принятии мер по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных.

Этот инструмент блокировки интернет-страниц, уникальный в международном правовом регулировании, позволяет защитить права субъектов на неприкосновенность их частной жизни, личную, семейную тайну путем ограничения доступа к интернет-ресурсам, обрабатывающим их персональные данные в отсутствие соответствующих правовых оснований.

Изменения коснулись и содержания уведомления о начале обработке персональных данных, которое оператор персональных данных обязан подать в Роскомнадзор. С момента вступления в силу Закона № 242-ФЗ оператор персональных данных должен указывать в уведомлении информацию о месте нахождения базы данных, в которой обрабатываются персональные данные российских граждан.

Глобальная модификация затронула и порядок контроля в области персональных данных. Законом № 242-ФЗ из сферы регулирования Закона №

294-ФЗ были выведены вопросы государственного контроля за обработкой персональных данных.

Выведение с 1 сентября 2015 года государственного контроля и надзора в области персональных данных из сферы действия Закона № 294-ФЗ изменило отдельные аспекты организации и проведения контрольно-надзорных мероприятий.

Так, были внесены изменения в программы проверок, касающиеся соблюдения требований по локализации баз данных на территории Российской Федерации.

Кроме того, с 1 сентября 2015 года Роскомнадзор и его территориальные органы при организации и проведении проверок стали руководствоваться исключительно Административным регламентом исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, утвержденным приказом Минкомсвязи России от 14 ноября 2011 года № 312.

Рассмотрим ответственность за нарушение законодательства в области защиты персональных данных (таблица 2.1).

Таблица 2.1 - Ответственность за нарушение законодательства в области защиты персональных данных

Статья	Кодекс	Содержание статьи	Ответственность за нарушение
13.11	КоАП РФ	Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)	Предупреждение или административный штраф: на должностных лиц - от 500 до 1000 руб.; на юридических лиц - от 5 000 до 10 000 руб.
13.14	КоАП РФ	Разглашение информации, доступ к которой ограничен федеральным законом, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей	Административный штраф: на должностных лиц - от 4 000 до 5 000 руб.

19.7	КоАП РФ	Непредставление или несвоевременное представление сведений (информации), представление которых предусмотрено законом, либо предоставление таких сведений в неполном объеме или в искаженном виде	Предупреждение или административный штраф: на должностных лиц - от 300 до 500 руб.; на юридических лиц - от 3000 до 5000 руб.
137	УК РФ	Нарушение неприкосновенности частной жизни	Штраф от 100 000 до 350 000 руб.; лишение права занимать определенные должности или заниматься определенной деятельностью; обязательные, исправительные или принудительные работы; арест; лишение свободы
272	УК РФ	Неправомерный доступ к компьютерной информации	Штраф от 100 000 до 500 000 руб.; исправительные или принудительные работы; ограничение свободы; лишение свободы
81, п.6, пп. «в»	ТК РФ	Разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника	Расторжение трудового договора работодателем, увольнение.
24 п.2	152-ФЗ	Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом	Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом

Итак, ответственность за нарушение закона о персональных данных может быть: административной (ст. 5.39, 13.11, 13.14, 19.5 и 19.7 КоАП РФ), уголовной (ст. 137, 140 и 272 УК РФ), дисциплинарной (пп. «в» п. 6 ст. 81 ТК РФ), материальной (ст. 238 ТК РФ), гражданско-правовой. Но успешное функционирование контрольно-надзорной деятельности является залогом

защищенности прав и свобод человека и гражданина при обработке его персональных данных, способствует повышению степени свободы граждан, укреплению правовой защищенности и безопасности личности.

Глава 3. Практический анализ конституционно-правовых основ защиты персональных данных

3.1 Статистические данные правовых вопросов защиты персональных данных

За 2015 г. зафиксирован 21 случай крупной утечки данных, было скомпрометировано около 814,5 млн записей. Рассмотрим статистику нарушений защиты персональных данных по государственным органам (рисунок 3.1).

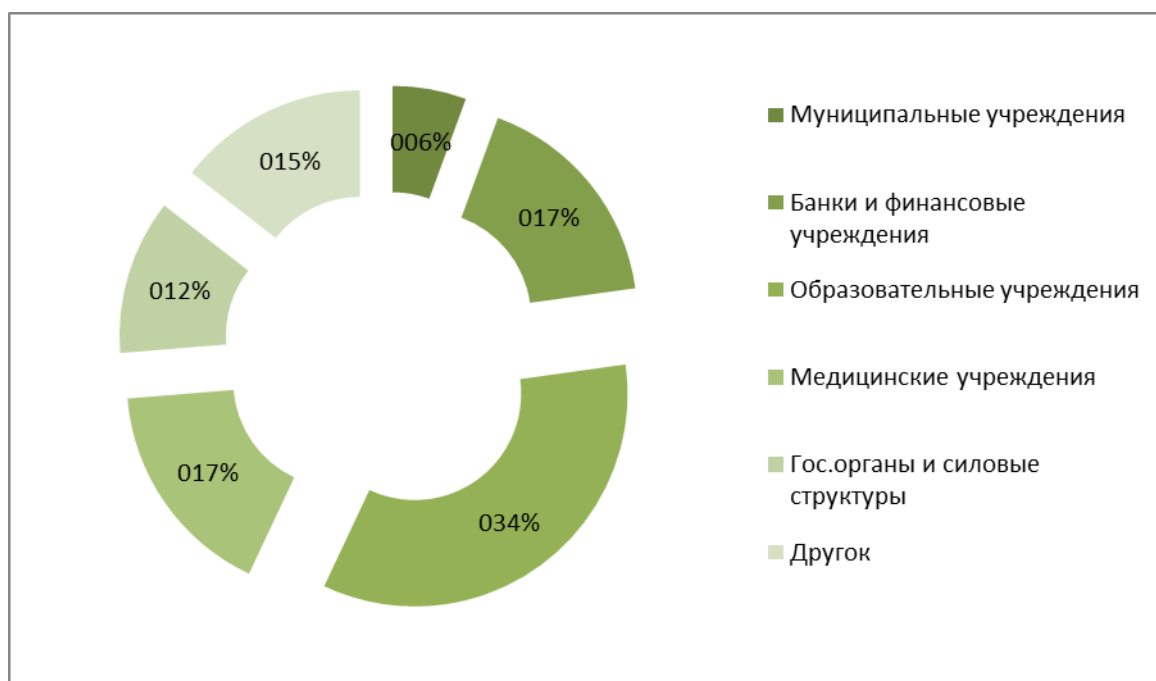


Рисунок 3.1 - Статистика нарушений защиты персональных данных по
государственным органам¹⁵

Итак, согласно диаграмме на рисунке 3.1 видно, что основной процент утечки информации происходит из образовательных структур. Наименьший процент утечки происходит из муниципальных учреждений.

¹⁵ Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2015 год // [Электронный ресурс] <https://rkn.gov.ru>

Рассмотрим статистику нарушения учета информации и данных по их типам (рисунок 3.2).

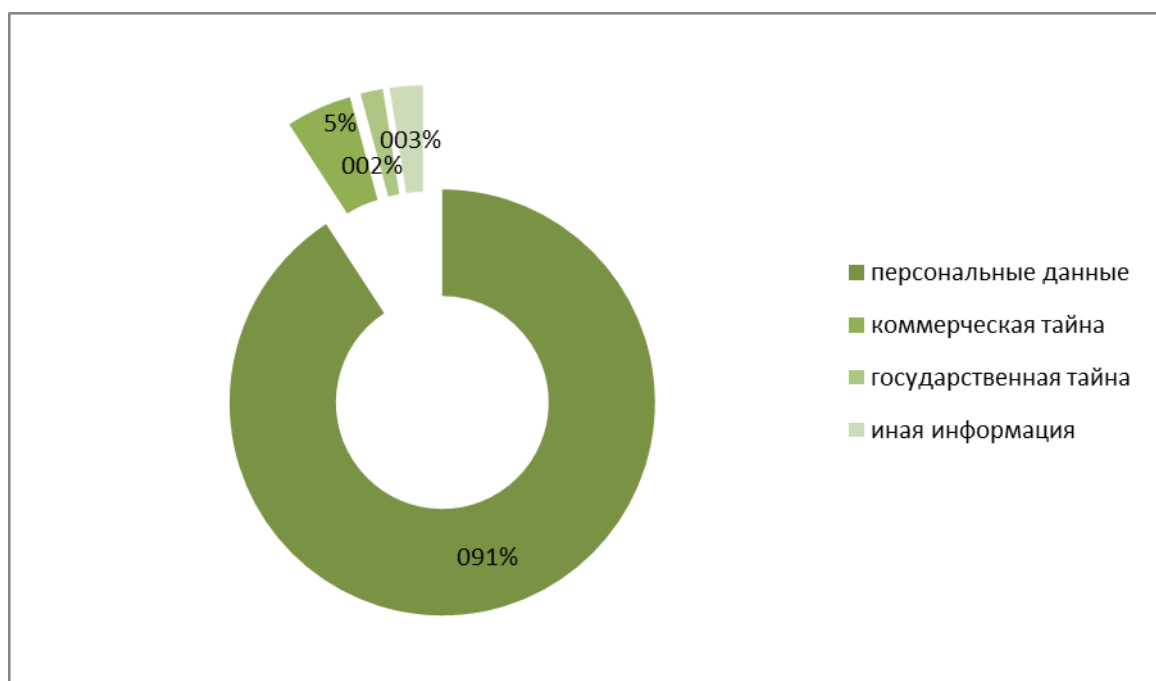


Рисунок 3.2 - Статистика нарушения учета информации и данных по их типам¹⁶

В 2014 г. выявлено 2027 сайтов, распространявших личную информацию о детях и их родителях в открытом доступе. Сайты принадлежали школам, детским садам, интернатам, муниципальным образованиям и администрациям субъектов РФ. В 2012 г. около г. Казань обнаружена несанкционированная свалка, среди которой оказались личные дела военнослужащих воинской части МВД специального назначения. В Брянской области при проверке одной из больниц, сотрудники Роскомнадзора выявили выброшенные в ближайший мусорный бак старые личные дела, карточки пациентов. В 2012 г. на сайте Следственного комитета России в открытом доступе появились данные обращений граждан через интернет-приемную. Всего 30 тыс. сообщений за 2,5 года оказались в разделе

¹⁶ Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2015 год // [Электронный ресурс] <https://rkn.gov.ru>

«Новости». В 2015 г. среди компаний, пострадавших от утечек за последние полгода, числятся МТС, ВТБ 24, РЖД, СОГАЗ.

Во исполнение государственной функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных территориальными органами Роскомнадзора в 2015 году были проведены 1 292 контрольно-надзорных мероприятия, из них 883 проверки в целях выполнения плана деятельности территориальных органов Роскомнадзора, что составляет 91% от количества запланированных проверок, и 99 внеплановых проверок, что составляет 10% от количества проведенных мероприятий.

В процессе проведения данных проверок предметом исследования являлась деятельность по обработке персональных данных, изучались информационные системы персональных данных, а также проводился анализ документов, характер информации в которых предполагает включение в них персональных данных.

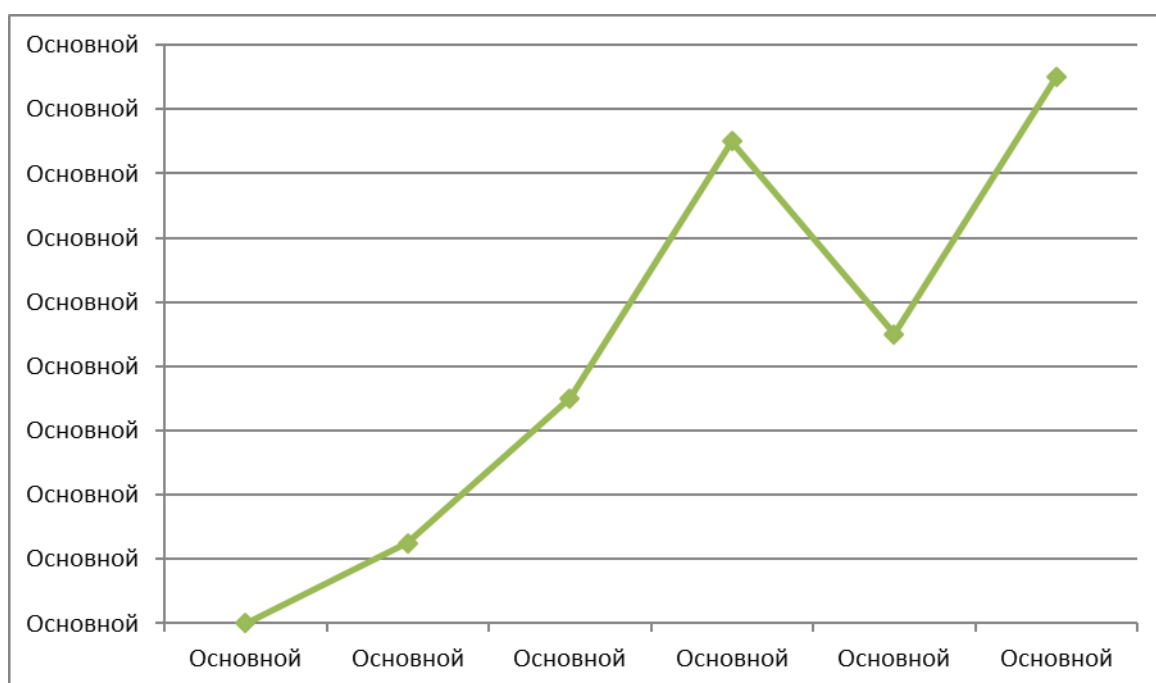


Рисунок 3.3 – Динамика проведенных плановых проверок с 2008 года

В рамках реализации функции по осуществлению государственного контроля и надзора в 2015 году проведено 1 160 плановых и 104 внеплановых проверки, а также 132 плановые проверки в отношении государственных органов, муниципальных органов, организующих и (или) осуществляющих обработку персональных данных.

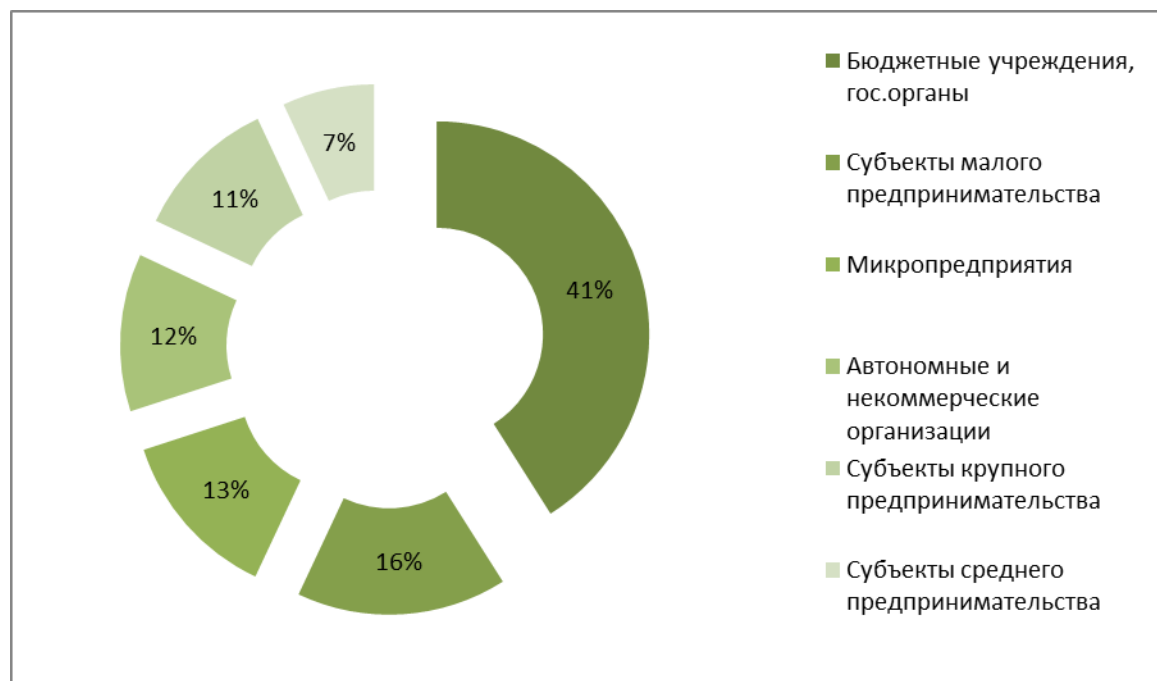


Рисунок 3.4 – Проверки, проведенные в 2015 году¹⁷

В 89 случаях, что составляет 9% от количества запланированных мероприятий, проверки не проведены по предусмотренным законодательством причинам, а именно:

- в связи реорганизацией юридического лица были отменены 11 проверок;
- в связи с ликвидацией юридического лица – 6 проверок;
- по распоряжению органов прокуратуры – 36 проверок;
- в связи с наступлением обстоятельств непреодолимой силы – 2 проверки;

¹⁷ Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2015 год // [Электронный ресурс] <https://rkn.gov.ru>

— по причине отсутствия объекта надзора по месту фактического осуществления деятельности – 35 проверок;

— в связи с отсутствием при проведении плановой проверки руководителя, иного должностного лица или уполномоченного представителя юридического лица, индивидуального предпринимателя, его уполномоченного представителя – 5 проверок;

— по причине непредоставления проверяемым лицом документов, необходимых для проведения и завершения, – 1 проверка.

Анализ результатов проведенных контрольно-надзорных мероприятий территориальными органами Роскомнадзора в 2015 году показывает, что каждая вторая проверка оператора выявляет нарушения. Так, при проведении 461 плановой проверки, что составляет 52% от проведенных плановых проверок, было выявлено 1 397 нарушений.

Количество выявленных нарушений при проведении плановых проверок в 2015 году на 37% больше числа выявленных нарушений в 2014 году.

Одним из наиболее частых нарушений, выявляемых при проведении плановых проверок, является представление в уполномоченный орган уведомления об обработке персональных данных, содержащего неполные и (или) недостоверные сведения, что показывают результаты 197 контрольно-надзорных мероприятий. По результатам проведения 195 мероприятий выявлено отсутствие в поручении лицу, которому оператором доверяется обработка персональных данных, обязанности соблюдения конфиденциальности персональных данных и обеспечения их безопасности.

Кроме того, по результатам проведения плановых проверок были выявлены такие нарушения, как отсутствие у оператора места (мест) хранения персональных данных (материальных носителей), перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ; обработка персональных данных в случаях, не предусмотренных Федеральным законом «О персональных данных»; несоответствие

содержания письменного согласия субъекта персональных данных на обработку персональных данных требованиям законодательства Российской Федерации.

В 2015 году территориальными органами Роскомнадзора в целях проверки исполнения ранее выданного предписания по итогам проведения плановых проверок было проведено 54 внеплановых проверки, что составляет 55% от общего количества внеплановых. В результате в 35% случаев (11 проверок) было установлено невыполнение в установленный срок законного предписания органа (должностного лица) Уполномоченного органа по защите прав субъектов персональных данных, осуществляющего государственный надзор (контроль), об устранении нарушений законодательства Российской Федерации в области персональных данных.

По итогам выявленных нарушений при проведении контрольно-надзорных мероприятий территориальными органами Роскомнадзора выдано 731 предписание об устранении установленных нарушений.

За отчетный период территориальными органами Роскомнадзора составлен и направлен на рассмотрение в суды 7 721 протокол об административных правонарушениях, по результатам рассмотрения которых наложено 10 454 600 рублей штрафов, из них взыскано 4 818 615 рублей.

Подчеркивая значимость контрольных функций, закон выделяет среди направлений государственной контрольной деятельности не только предупреждение, выявление и пресечение правонарушений, но также систематическое наблюдение за исполнением обязательных требований, анализ и прогнозирование состояния исполнения обязательных требований при осуществлении деятельности операторов.

На 2015 год территориальными органами Роскомнадзора было запланировано проведение 1 929 мероприятий систематического наблюдения. Проведено 2 086 мероприятий систематического наблюдения, из них 1 970 плановых мероприятий, что составляет 99% от запланированных

мероприятий, и 116 внеплановых мероприятий, что составляет 5% от общего количества проведенных мероприятий. По итогам 654 плановых мероприятий систематического наблюдения, что составляет 33% от проведенных плановых проверок, выявлено 1 229 нарушений.

3.2 Анализ судебно-правовой практики при нарушении защиты персональных данных работников организаций

Обработка, хранение и использование персональных данных зачастую являются головной болью организаций. Работодатели нередко считают, что на проблему использования персональных данных работника можно не обращать внимания.

В ст. 86 ТК РФ определяется исчерпывающий перечень требований, предъявляемых к обработке персональных данных работника, которые в целях обеспечения прав и свобод человека и гражданина обязан соблюдать работодатель и его представители. Но часто при обработке и хранении персональных данных работников возникают спорные ситуации. В этом случае работники вынуждены обращаться в суд за защитой персональных данных. Нарушения при обработке и хранении данных работников также могут быть выявлены при проверке деятельности организации прокуратурой, другими государственными органами по жалобам работников.

Так как для принятия на работу достаточно подтвердить свое ФИО предъявлением документа удостоверяющего личность. Суды руководствуются именно этим фактом. При этом работодатель обязан представить работникам документы, устанавливающие порядок обработки персональных данных работников, под роспись.

Анализ судебной практики показывает, что работодатели часто нарушают требования Закона по обработке персональных данных.

Рассмотрим два распространенных примера привлечения судом к административной ответственности юридических лиц (работодателей) за нарушение правил обработки и хранения персональных данных.

В соответствии со ст. 6, п. 1 ст. 11 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных. Вместе с тем в результате проверки установлено, что в ООО "Мираж" согласие работников на обработку их персональных данных не получено.

Таким образом, в действиях ООО «Мираж» был выявлен состав административного правонарушения, предусмотренного ст. 13.11 КоАП РФ, то есть нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных). Судом ООО «Мираж» был признан виновным в совершении административного правонарушения, предусмотренного ст. 13.11 КоАП РФ, и было назначено административное наказание в виде предупреждения¹⁸.

Следующий пример из судебной практики. ООО АНО ДПО «Учебный Центр Газ-Нефть» было привлечено к административной ответственности по ст. 13.11 КоАП РФ за отсутствие письменного согласия Тряскиной Н.Г. и Зотовой Ю.С. на передачу их персональных данных третьим лицам и их обработку. Таким образом, нарушен порядок сбора персональных данных Тряскиной Н.Г. и Зотовой Ю.С, которые в обязательном порядке должны быть ознакомлены под роспись с Положением «О разграничении прав доступа к обрабатываемым персональным данным в АНО «Учебный центр Газ-Нефть», а также дать свое согласие на обработку своих персональных данных¹⁹.

¹⁸ Постановление мирового судьи судебного участка N 12 Зуевского судебного района Кировской области от 8 апреля 2015 г. по делу N 5-199/15.

¹⁹ Постановление мирового судьи судебного участка N 8 судебного района г. Уфы Республики Башкортостан по делу N 5-203/2015.

В соответствии со ст. 86 ТК РФ обработка персональных данных может осуществляться работодателем лишь с целью обеспечения соблюдения нормативных правовых актов, содействия работникам в трудоустройстве, обучения и продвижения по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Нарушения могут быть и при назначении ответственного лица, которое осуществляет обработку данных в организации.

Согласно ч. 1 ст. 22.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных. Так, в нарушение п. 1 ч. 1 ст. 18.1, ч. 1 ст. 22.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» в ООО «Ясмин» не назначен ответственный за организацию обработки персональных данных. Согласно п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных законом и принятыми в соответствии с ним нормативными правовыми актами²⁰.

В некоторых случаях суд может признать законность действий работодателя при обработке и защите персональных данных работника.

Так, в исковом заявлении Б.П. ссылался на то обстоятельство, что в период его работы у ответчика при разработке конструкторской документации на ряде документов, которые он не видел и не подписывал или с содержанием которых не был согласен, представители работодателя указали его фамилию.

В связи с чем, он в докладной записке потребовал от работодателя удалить свою фамилию из всех конструкторских документов, которые он не

²⁰ Постановление мирового судьи Вологодской области по судебному участку N 9 по делу N 5-1303/2015г.

подписывал или с содержанием которых не был согласен, однако работодатель никаких действий по защите персональных данных Б.П. не предпринял, чем нанес ему моральный вред.

Отказывая в удовлетворении исковых требований Б.П., суд указал, что использование работодателем персональных данных Б.П. в виде указания его фамилии в конструкторской документации было обусловлено выполнением им трудовых обязанностей и было осуществлено в соответствии с должностной инструкцией Б.П. и действующими нормами трудового права.

Суд при этом отметил, что каких-либо доказательств того, что документы, в которых была указана фамилия истца, не относились к области его трудовых обязанностей, в материалах дела не имеется²¹.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Исходя из толкования ст. 90 ТК РФ в совокупности со ст. 237 ТК РФ следует, что в результате незаконного распространения информации о персональных данных работника последнему может быть причинен моральный вред, подлежащий возмещению работодателем.

Так, Апелляционным определением Верховного Суда Республики Саха (Якутия) от 23 октября 2013 г. по делу N 33-4172/13 было установлено незаконное бездействие акционерной компании «АЛРОСА», выразившееся в нарушении норм защиты персональных данных работника Д. при их получении и обработке, содержащихся в дополнительном соглашении б/н от 30 апреля 2008 г. к трудовому договору. При таких обстоятельствах, вопреки выводам суда первой инстанции, распечатка с интернет-сайта и протокол осмотра с участием нотариуса указывают на неправомерное использование третьими лицами персональных данных работника, находившихся, кроме истца, только у работодателя. Таким образом, акционерная компания

²¹ Решение судебной коллегии по гражданским делам Санкт-Петербургского городского суда от 26 января 2012 г. по делу N 33-712/2012.

«АЛРОСА» (ОАО) нарушила действующее законодательство по защите персональных данных работника.

В соответствии с п. 4 ст. 86 ТК РФ работодатель не имеет права получать и обрабатывать данные работника о его политических, религиозных и иных убеждениях и частной жизни без его письменного согласия, если это не связано с трудовыми отношениями.

Судебная практика подтверждает необходимость и обязанность работодателя предоставлять защиту персональных данных работника. К примеру, суд указал, что работодатель правомерно не представил акционерам общества копию трудового договора с генеральным директором, поскольку ст. 88 ТК РФ установлен запрет на передачу персональных данных работника третьей стороне, а в соответствии со ст. 90 ТК РФ лица, виновные в нарушении норм, регулирующих защиту персональных данных, несут административную, гражданско-правовую или уголовную ответственность²².

Суды и другие правоохранительные органы могут беспрепятственно получать от организаций персональные данные работников, клиентов или контрагентов без согласия последних. Данную правовую позицию поддерживают и суды высших инстанций.

В частности, Иркутский областной суд в Апелляционном определении от 9 сентября 2014 г. по делу N 33-7441-14 указал, что суд первой инстанции сделал правильные выводы о том, что запрос сведений, касающихся лица, состоящего в трудовых отношениях с администрацией муниципального образования, является правомерным, произведен прокурором в пределах его полномочий, предусмотренных законом, и не требует согласия указанного гражданина на обработку его персональных данных. Как следует из содержания запроса и материалов дела, обращаясь к главе администрации АМО, прокурор конкретизировал запрашиваемые сведения, ограничив их документами, предшествующими заключению трудового договора, включая

²² Постановление ФАС Московского округа от 14.01.2010 по делу N А40-38438/09-17-269.

конкурсную документацию, что воспринимается однозначно и не вызывает сомнений в составе и объеме запрашиваемых документов.

В соответствии с п. 6 ст. 3 Федерального закона «О персональных данных» действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц, являются предоставлением, а не распространением информации.

Рассмотрим следующий пример из судебной практики. Так, в Апелляционном определении от 4 марта 2015 г. по делу N 33-7084 Московский городской суд правильно исходил из того, что обработка персональных данных заявителя по его письменному заявлению осуществляется не в рамках уголовно-правовых отношений, определяющих основания аннулирования всех последствий, связанных с судимостью, а в связи с его профессиональной деятельностью и в соответствии с целями обработки, определенными Трудовым кодексом РФ, которые допускают включение в данную справку сведений как об имеющейся, так и об имевшейся у лица судимости. Данное правовое регулирование обеспечивает защиту общественных интересов и обязывает ФКУ ГИАЦ МВД России и ИЦ предоставлять информацию обо всех судимостях заявителя, включая погашенные²³.

Федеральными законами могут быть предусмотрены иные случаи передачи персональных данных без согласия работника. Запрашивать сведения о персональных данных работника могут также адвокаты, нотариусы, должностные лица государственных органов.

В соответствии с п. 1 ч. 3 ст. 6 Федерального закона от 31.05.2002 N 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» адвокат имеет право осуществлять сбор сведений, которые необходимы для оказания юридической помощи, при этом также осуществлять запрос справок, характеристик и иных документов от различных органов

²³ Апелляционное определение Московского городского суда от 4 марта 2015 г. по делу N 33-7084.

государственной власти, местного самоуправления, общественных объединений и иных организаций. Перечисленные представители государственной власти в порядке, установленном законодательством, имеют обязанность выдать адвокату запрошиваемые им документы или их заверенные копии не позднее чем в месячный срок со дня получения запроса адвоката.

В частности, в Апелляционном определении Московского городского суда от 24 декабря 2014 г. по делу N 33-41576/2014 указано, что, отказывая истцу в удовлетворении заявленных требований, суд первой инстанции исходил из того, что предоставление ответчиком адвокату копии трудовой книжки П. и расписки в получении трудовой книжки соответствует положениям п. 1 ч. 3 ст. 6 Федерального закона «Об адвокатской деятельности и адвокатуре в Российской Федерации», п. п. 2, 3 ч. 1 ст. 6 Федерального закона «О персональных данных», поскольку обработка персональных данных истца осуществлялась ЗАО «ИНТЕРРОС ЭСТЕЙТ» в целях обеспечения права на представления доказательств по гражданскому делу. Но не все правоохранительные и контрольные органы имеют аналогичные права. Остановимся на следующей судебной практике.

Так, Девятый арбитражный апелляционный суд в своем Постановлении от 25.06.2009 по делу N А40-76345/08-122-112 указал, что сотрудник службы судебных приставов не имеет права запрашивать и получать сведения, содержащие личные данные граждан. В частности, суд отметил, что ни Федеральный закон от 21.07.1997 N 118-ФЗ «О судебных приставах», ни Федеральный закон от 02.10.2007 N 229-ФЗ «Об исполнительном производстве» не предоставляют судебным приставам-исполнителям права получать персональные данные без согласия их субъектов, не устанавливают условия получения таких данных, не определяют круг субъектов, персональные данные которых подлежат обработке, а также полномочия судебного пристава-исполнителя по их обработке.

За разглашение персональных данных устанавливается дисциплинарная ответственность. Однако в практике есть случаи признания недействительным применение дисциплинарной ответственности к работнику за разглашение сведений о персональных данных, если работник не был ознакомлен с внутренними документами об обработке и хранении персональных данных, а также в случае недоказанности работодателем факта обоснованности привлечения к дисциплинарной ответственности.

Разрешая спор по существу и признавая незаконным и подлежащим отмене приказ Дальневосточного банка ОАО «Сбербанк России» о применении дисциплинарного взыскания о наложении на Д. дисциплинарного взыскания в виде замечания, суд первой инстанции пришел к обоснованному выводу о том, что ответчиком в судебном заседании не доказан тот факт, что Д. получила копии приказов, содержащие персональные данные работников Дальневосточного банка ОАО «Сбербанк России». Незаконность получения персональных данных и факт распространения также не доказаны.

Судебная коллегия также соглашается с выводом суда первой инстанции о пропуске срока привлечения истца к дисциплинарной ответственности, поскольку датой обнаружения проступка является подача директором юридического управления служебной записки на имя заместителя председателя Дальневосточного банка «Сбербанк России» о необходимости проведения служебного расследования. Об этом прямо указано в п. 2.3 акта служебного расследования. Приказ о применении дисциплинарного взыскания издан после истечения срока для применения наказания, когда с момента обнаружения проступка до применения дисциплинарного взыскания прошло более двух месяцев²⁴.

Рассмотрим дело, рассмотренное в Сызранском городском суде от 18.11.2016 году. Яшагин В.В. обратился в Сызранский городской суд с иском

²⁴ Апелляционное определение Хабаровского краевого суда от 30 мая 2014 г. по делу N 33-3334.

к АО «Производственная компания Автокомпонент Сызрань» о понуждении предоставить документы, связанные с работой, и взыскании компенсации морального вреда, мотивируя тем, что он работает в АО «Производственная компания Автокомпонент Сызрань» (далее по тексту АО «ПК Автокомпонент Сызрань») в должности главного энергетика.

Истец неоднократно обращался в отдел кадров предприятия и к исполнительному директору с заявлением о предоставлении ему копий документов, связанных с работой. Однако, заявление у него не принимали, регистрировать данное заявление в отделе кадров и канцелярии отказывались. В связи с этим, Яшагин В.В. был вынужден направить заявление о выдаче ему копий документов, связанных с работой, в адрес АО «ПК Автокомпонент Сызрань» почтовым отправлением. Ответ на данное заявление истцом до настоящего времени не получен, копии документов, связанных с работой, Яшагину В.В. ответчиком до настоящего времени не выданы. В результате нарушения трудовых прав истцу причинен моральный вред. На основании изложенного, Яшагин В.В. просит суд:

- обязать АО «ПК Автокомпонент Сызрань» в трехдневный срок предоставить истцу надлежаще заверенные копии документов, связанных с работой: трудовой договор и все дополнительные соглашения к трудовому договору; приказ о приеме на работу; Правила внутреннего трудового распорядка; локальные нормативные акты работодателя (выписки из них), затрагивающие права и обязанности истца, как работника акционерного общества (положение о структурном подразделении, о работе с персональными данными, о коммерческой тайне, об оплате труда, о премировании и другие); карточку формы Т-2; приказы о применении дисциплинарных взысканий за весь период работы; приказы об объявлении простоя, изменении условий труда, о переводах и перемещении за весь период работы; коллективный договор; должностную инструкцию главного энергетика; о проведении специальной оценки условий труда (аттестации рабочего места) главного энергетика; справки о доходах физического лица по

форме 2-НДФЛ за 2013-2016 годы; расчетные листки за весь период работы; документы, подтверждающие суммы и сроки выплаты заработной платы за весь период работы; предоставить полную информацию о наличии в АО «ПК Автокомпонент Сызрань» персональных данных истца и обработке этих данных, а также выдать копий всех записей, содержащих персональные данные истца;

- взыскать с АО «ПК Автокомпонент Сызрань» в его пользу: компенсацию морально вреда – 10 000 рублей, и почтовые расходы – 141 рубль 55 копеек;

- обратиться с решением суда в части требований о предоставлении копий документов к немедленному исполнению.

В процессе рассмотрения судом настоящего гражданского дела Яшагин В.В. уменьшил и уточнил свои исковые требования, в связи с тем, что его исковые требования в части предоставления перечисленных выше документов были исполнены ответчиком после обращения его в суд с данным иском. Просит суд взыскать с АО «ПК Автокомпонент Сызрань» в его пользу: компенсацию морально вреда – 10 000 рублей, почтовые расходы – 141 рубль 55 копеек, а всего – 10 141 рубль 55 копеек.

Представитель АО «ПК Автокомпонент Сызрань» Шестакова Л.А. в судебном заседании иск не признала, пояснила, что в адрес ответчика поступило заявление Яшагина В.В. о предоставлении ему документов. Почтовым отправлением с описью вложений работодатель направил в адрес истца документы в запрошенном им объеме. При этом, Яшагиным В.В. кроме документов, связанных с его работой, были запрошены локальные нормативные акты АО «ПК Автокомпонент Сызрань», которые также были ему предоставлены. Однако, анализ ст. 62 ТК РФ позволяет сделать вывод о том, что на работодателе лежит обязанность безвозмездно предоставить работнику по его письменному заявлению копии документов, связанных с работой, т.е. документов, содержащих персональную информацию о работнике, но не копии локальных нормативных актов, содержащих нормы

трудового права, с которыми работодатель обязан только ознакомить работника под роспись (абз. 17 ст. 22, ч. 3 ст. 68 ТК РФ). Кроме того, названная выше норма закона не обязывает работодателя предоставить работнику по его письменному заявлению копии коллективных договоров, соглашений и локальных нормативных актов, содержащих нормы трудового права (штатного расписания, правил внутреннего трудового распорядка, должностной инструкции, положения об оплате труда, положения о премировании, положения об отпусках и т.п.), которые регулируют трудовые отношения и иные непосредственно связанные с ними отношения (ч. 2 ст. 5 ТК РФ). Таким образом, работодатель не обязан предоставлять работнику копии локальных нормативных актов. В связи с этим требование истца обязать АО «ПК Автокомпонент Сызрань» предоставить ему копии локальных нормативных актов (положение о структурном подразделении, о работе с персональными данными, и премировании и другие) является необоснованным.

Также необоснованными являются требования истца в части предоставления имеющейся в АО «ПК Автокомпонент Сызрань» полной информации о персональных данных Яшагина В.В. и обработке этих данных, а также в части обязания ответчика выдать копии всех записей, содержащих его персональные данные. Согласно ст. 14 ФЗ «О персональных данных» от 27 июля 2006 года № 152-ФЗ, субъект персональных данных имеет право на получение сведений, указанных в части 7 настоящей статьи. В силу ст. 20 названного выше Федерального закона оператор обязан сообщит в порядке, предусмотренном статьей 14 настоящего Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

Все персональные данные истца, которые имеются у работодателя, содержатся в карточке формы Т-2. Иных персональных данных Яшагина В.В. в АО «ПК Автокомпонент Сызрань» не имеется. При этом, копия карточки формы Т-2 была предоставлена истцу вместе со всем пакетом документов.

Для получения копий иных записей, содержащих его персональные данные, Яшагину В.В. необходимо конкретизировать наименование документов, в которых содержатся его персональные данные. Таким образом, требования истца возложить на ответчика обязанность предоставить копии документов, перечисленных в исковом заявлении, и информации о наличии персональных данных истца, являются необоснованными, поскольку все документы и сведения о наличии персональных данных, в том числе копии записей, содержащих персональные данные, предоставлены Яшагину В.В. в полном объеме.

Исковые требования Яшагина В.В. в части взыскания с АО «ПК Автокомпонент Сызрань» компенсации морального вреда также являются необоснованными, поскольку, согласно ст. 237 ТК РФ, моральный вред, причиненный работнику неправомерными действиями или бездействием работодателя, возмещается работнику в денежной форме в размерах, определяемых соглашением сторон трудового договора. В случае возникновения спора факт причинения работнику морального вреда и размеры его возмещения определяются судом независимо от подлежащего возмещению имущественного ущерба. В силу ст. 1101 ГК РФ, размер компенсации морального вреда определяется судом в зависимости от характера причиненных потерпевшему физических и нравственных страданий, а также степени вины причинителя вреда в случаях, когда вина является основанием возмещения вреда.

При определении размера компенсации вреда должны учитываться требования разумности и справедливости. Характер физических и нравственных страданий оценивается судом с учетом фактических обстоятельств, при которых был причинен моральный вред, и

индивидуальных особенностей потерпевшего. Однако, истец не привел доводов о том, какие именно нравственные и физические страдания ему были причинены, что свидетельствует об отсутствии как таковых нравственных и, тем более, физических страданий. Компенсация морального вреда подлежит возмещению работнику при нарушении работодателем каких-либо трудовых прав работника. Однако, АО «ПК Автокомпонент Сызрань» полагает, что никаких прав истца в данной ситуации им не нарушено.

Заявление Яшагина В.В. о предоставлении документов содержало значительный перечень документов. Работодатель, стремясь избежать конфликтных ситуаций с работником, предоставил истцу даже больше того, что предусмотрено законом. При этом, часть запрошенных документов по трудовой деятельности Яшагина В.В. находится на хранении в архиве предприятия. Создание архива организации предусмотрено ФЗ «Об архивном деле в Российской Федерации» № 125-ФЗ. Документы по личному составу работодатель обязан хранить установленное законом время и в случае ликвидации организации передавать документы в госархив.

В АО «ПК Автокомпонент Сызрань» утвержден стандарт предприятия СтП 10-4.2-2015, а также номенклатура дел на предприятии, подлежащих ведению и передаче в архив. Сводная номенклатура дел согласована с Управлением государственной архивной службы Самарской области. Таким образом, хранение и обработка документов по личному составу осуществляется в порядке, предусмотрен законодательством об архивной деятельности. Согласно п. 8.2.1. Основных правил работы архивов организации, утвержденных решением коллегии Росархива (Основные правила работы архивов организаций являются нормативно-методическим документом, определяющим их деятельность), срок исполнения запросов социально-правового характера граждан и организаций по материалам архива не должен превышать 30 дней со дня регистрации обращения. При сложных запросах срок может быть продлен, но не более чем на 30 дней с обязательным уведомлением об этом заявителя.

Таким образом, работодатель при исполнении заявления истца действовал в рамках, установленных действующим законодательством, и не нарушал прав и законных интересов истца. Соответственно, требования истца о взыскании морального вреда являются необоснованными.

Судом установлено, что Яшагин В.В. работает в АО «ПК Автокомпонент Сызрань» в должности главного энергетика.

Истец направил в адрес АО «ПК Автокомпонент Сызрань» посредством почтовой связи заявление о выдаче ему копий документов, связанных с работой, а именно: трудового договора и всех дополнительных соглашений к трудовому договору; приказа о приеме на работу; Правилами внутреннего трудового распорядка; локальных нормативных актов работодателя (выписки из них), затрагивающих права и обязанности истца, как работника акционерного общества (положений о структурном подразделении, о работе с персональными данными, о коммерческой тайне, об оплате труда, о премировании и другие); карточки формы Т-2; приказов о применении дисциплинарных взысканий за весь период работы (при наличии); приказов об объявлении простоя, изменении условий труда, о переводах и перемещении за весь период работы (при наличии); коллективного договора (при наличии); должностной инструкции главного энергетика; документов о проведении специальной оценки условий труда (аттестации рабочего места) главного энергетика; справок о доходах физического лица по форме 2-НДФЛ за 2013-2016 годы; расчетных листков за весь период работы; документов, подтверждающих суммы и сроки выплаты заработной платы за весь период работы; о предоставлении ему полной информации о наличии в АО «ПК Автокомпонент Сызрань» персональных данных истца и обработке этих данных, а также о выдаче копий всех записей, содержащих персональные данные истца.

Названное выше заявление было получено ответчиком. Однако, в установленный законом трехдневный срок документы, связанные с работой, а также иные запрашиваемые истцом документы, Яшагину В.В. выданы не

были, в связи с чем он обратился в Сызранский городской суд с иском к АО «ПК Автокомпонент Сызрань» о понуждении предоставить документы, связанные с работой, и взыскании компенсации морального вреда.

После обращения Яшагина В.В. в суд с указанным выше исковым заявлением, АО «ПК Автокомпонент Сызрань» направило в адрес истца посредством почтовой связи документы, связанные с его работой, а также иные запрашиваемые им документы. Указанные выше обстоятельства подтверждаются заявлением Яшагина В.В. об истребовании документов, описью вложений в ценное письмо, кассовыми чеками ФГУП «Почта России», отчетом об отслеживании почтового отправления, описью вложений в ценную бандероль, а также объяснениями представителя ответчика в судебном заседании.

При таких обстоятельствах, суд полагает необходимым иски требования Яшагина В.В. удовлетворить в части, взыскать с АО «ПК Автокомпонент Сызрань» в пользу истца компенсацию морального вреда в размере 1 000 рублей, поскольку в судебном заседании установлено, что в результате нарушения ответчиком прав Яшагина В.В., являющегося работником АО «ПК Автокомпонент Сызрань», выразившегося в невыполнении его законных требований и в непредоставлении в установленный законом срок копий документов, связанных с работой, истец был вынужден обратиться в Сызранский городской суд с иском о понуждении предоставить документы, связанные с работой, испытывал переживания в связи с незаконностью действий ответчика, обиду. Таким образом, в результате названных выше незаконных действий АО «ПК Автокомпонент Сызрань» истцу был причинен моральный вред, выразившийся в нравственных страданиях, который, в силу приведенных выше положений закона, подлежит компенсации ответчиком.

При определении размера компенсации морального вреда судом учтены обстоятельства настоящего гражданского дела, степень нравственных страданий истца, степень вины ответчика в причинении вреда, требования

разумности и справедливости, а также иные, заслуживающие внимания обстоятельства. Заявленный Яшагиным В.В. размер компенсации морального вреда (10 000 рублей) суд полагает явно завышенным и неразумным.

Доводы представителя АО «ПК Автокомпонент Сызрань» Шестаковой Л.А. о том, что при исполнении заявления истца работодатель действовал в рамках, установленных действующим законодательством, и не нарушал прав и законных интересов Яшагина В.В., т.к. запрашиваемые им документы находятся на хранении в архиве предприятия, а срок выдачи их из архива составляет 30 дней, суд полагает несостоятельными, поскольку они противоречат приведенным выше положениям закона, согласно которым по письменному заявлению работника работодатель обязан не позднее трех рабочих дней со дня подачи этого заявления выдать работнику копии документов, связанных с работой. Факт сдачи документов, связанных с работой истца, в архив предприятия, не освобождает работодателя от возложенной на него законом обязанности выдать работнику копии названных выше документов в срок, установленный Трудовым кодексом РФ.

Ссылка представителя АО «ПК Автокомпонент Сызрань» Шестаковой Л.А. на стандарт предприятия СтП 10-4.2-2015 и на Основные правила работы архивов организации, утвержденные решением коллегии Росархива (Основные правила работы архивов организаций являются нормативно-методическим документом, определяющим их деятельность), устанавливающие 30-дневный срок исполнения запросов социально-правового характера граждан со дня регистрации обращения, неосновательна и не может быть принята судом во внимание, поскольку статьей 62 ТК РФ установлен срок выдачи работнику копий документов, связанных с работой, который составляет не позднее трех рабочих дней со дня подачи соответствующего заявления. Данный срок не может быть изменен на основании названных выше актов, имеющих меньшую юридическую силу.

В соответствии со ст. 98 ГПК РФ с ответчика следует взыскать с пользу истца почтовые расходы в размере 141 рубль 55 копеек. Согласно ст. 103

ГПК РФ с АО «ПК Автокомпонент Сызрань» следует взыскать госпошлину в доход государства в размере 300 рублей.

На основании изложенного, руководствуясь ст.ст. 194-199 ГПК РФ суд решил иск Яшагина ВВ к АО «Производственная компания Автокомпонент Сызрань» о возмещении морального вреда удовлетворить в части. Взыскать с АО «Производственная компания Автокомпонент Сызрань» в пользу Яшагина ВВ: компенсацию морального вреда – 1 000 рублей, почтовые расходы – 141 рубль 55 копеек, а всего – 1 141 рубль 55 копеек. В остальной части исковые требования Яшагина ВВ оставить без удовлетворения.

Взыскать с АО «Производственная компания Автокомпонент Сызрань» госпошлину в доход государства в размере 300 рублей. Решение может быть обжаловано в Самарский областной суд через Сызранский городской суд в течение месяца со дня принятия решения суда в окончательной форме²⁵.

Таким образом, можно сделать вывод о том, что судебная практика по вопросам обработки и хранения персональных данных является одним из наиболее распространенных категорий трудовых споров. В основном в судах рассматриваются нарушения правил обработки и хранения персональных данных различными организациями. Большинство споров удалось бы избежать, если бы работодатели соблюдали требования федерального законодательства об обработке и хранении персональных данных.

В основном суды апелляционной и кассационной инстанции соглашались с выводами судов первой инстанции и оставляют решения без изменений.

²⁵ Решение по делу 2-4158/2016 ~ М-4370/2016 // [Электронный ресурс] <https://rospravosudie.com>.

3.3 Проблемы и перспективы развития конституционно-правовой защиты персональных данных

Компании, работающие на рынке персональной информации, собирают эту информацию из нескольких категорий источников. Первой категорией являются базы данных, находящиеся в распоряжении государства и доступные на определенных законных основаниях.

Второй категорией являются источники общедоступной информации, к которой можно отнести статьи и скрытую рекламу в газетах и журналах, а также другую информацию из печатных источников. Мощные поисковые механизмы, работающие в интернете, позволяют просеивать сетевые ресурсы (например, персональные сайты) и находить информацию, которую можно ассоциировать с конкретными личностями. Источником информации являются также различные электронные справочные издания, наподобие «желтых страниц». Кроме этого, различные специализированные ресурсы, такие как сайты корпоративных организаций или общественных структур, помещают в интернете списки своих членов с необходимой информацией или объявления желающих участвовать в каких-либо инициативах.

Третьей основной категорией источников персональной информации являются находящиеся в частной собственности базы данных, содержащие, как правило, информацию, относящуюся к материальной сфере. Так, например, три американские кредитные организации поддерживают и продают информацию, относящуюся к финансовой сфере. Источником этой информации являются кредиторы, суды, а также сами граждане.

В частном секторе потребителями персональной информации, предоставляемой специализированными компаниями, является множество компаний и лиц. К их числу относятся банки, страховые компании, торговые компании и в целом все, кто работают в режиме кредитования, а также юристы, частные сыщики, некоммерческие структуры и журналисты. Целями использования информации могут быть пресечение мошенничества,

исполнение судебных решений, поиск должников и имущества несостоятельных должников, совместная с государственными органами деятельность в расследовании правонарушений, поиск получателей наследства и т.п.

Кроме очевидной пользы от возможности получить необходимую персональную информацию, существуют многочисленные риски, связанные с оборотом персональных данных.

Самое главное — это возможность вторжения в частную жизнь, проникновение в личную тайну, получение и распространение так называемой «чувствительной» информации, которая защищается международным правом и законодательством цивилизованных стран.

Можно обозначить массу рисков, связанных с ошибками или неточностями в персональных данных. Врач, информация о наличии лицензии на деятельность которого случайно стерта из баз данных, потратит много времени на поиск новых клиентов. Предприниматель, чье имя оказалось случайно ассоциировано с криминальным фактом, с трудом будет находить деловых партнеров. Неточная информация, содержащаяся в базах, может повлиять на решение работодателя о найме на работу, а компании о предоставлении товарного или денежного кредита.

Нет нужды пояснять, что существуют также риски, связанные с возможными правонарушениями или преступлениями в отношении субъектов персональных данных (от мошенничества до нанесения физического ущерба).

Можно обозначить несколько направлений работ, которые могут помочь снижению издержек, связанных с оборотом персональных данных:

Снижение доступности информации, которая может быть отнесена к разряду «чувствительной». Это должно включать:

— избирательную политику по отношению к потребителям (покупателям), что включает в себя разделение информации и ее

потребителей (покупателей) на соответствующие разряды с дифференцированными правами доступа к соответствующим разрядам информации;

— снижение объема «чувствительной» персональной информации, которая может быть свободно получена из публичных регистров данных;

— дополнительные меры по аппаратно-программной защите данной категории информации.

Контроль использования данных. Это может включать в себя:

— проверку использования данных конкретными получателями (покупателями) информации;

— ведение учета доступа к персональным данным.

Обеспечение доступа субъектов данных к информации о них и способами контроля над их персональными данными. Это может включать в себя две основные возможности, предоставляемые субъекту данных:

— обязанность получить согласие субъекта данных на раскрытие информации о нем, что может обеспечить осведомленность субъекта данных о существовании его персональной информации;

— право субъекта данных запретить распространение его персональных данных, что может стать по-настоящему эффективным, если существует универсальная среда, охватывающая все структуры, осуществляющие распространение персональных данных.

Обучение всех участников оборота персональных данных законным методам работы с целью снижения существующих рисков.

Заложить основы российской модели конституционно-правовой защиты персональных данных позволяет выявление и последующее раскрытие содержания конституционных оснований защиты персональных данных. Причем в качестве центрального элемента представляется разумным рассматривать право на неприкосновенность частной жизни, конституционно закрепленное в ч. 1 ст. 23 в совокупности с ч. 1 ст. 24. Помимо

неприкосновенности личной жизни субъекта в качестве других элементов российской модели конституционно-правовой защиты персональных данных могут выступать такие составляющие, как: тайна переписки и переговоров, сообщений, неприкосновенность жилья.

Следует отметить, что в содержании иных гарантированных Конституцией РФ прав тоже могут быть выявлены отдельные гарантии защиты персональных данных (например, в праве на свободное использование своих способностей и имущества для предпринимательской и иной не запрещенной законом экономической деятельности). Вместе с тем центральное значение для определения основных принципов обработки и защиты персональных данных в конституционно-правовом аспекте имеют три проанализированных в настоящей статье права.

Понимая под моделью «упрощенную и символическую схему, предназначенную для объяснения какой-либо реальности», считается возможным отказаться от причисления других прав к числу элементов модели конституционно-правовой защиты персональных данных как не содержащих таких конституционных гарантий защиты указанной категории информации, которые могли бы оказать значительное влияние на формирование соответствующей модели.

Представляется, что в качестве элемента права на неприкосновенность частной жизни может быть выделено притязание на защиту персональных данных.

Такое понимание права на неприкосновенность частной жизни сопряжено с пересмотром получившего распространение в отечественной доктрине и конституционно-судебной практике узкого истолкования частной жизни, ограничивающего содержание последней сферой жизнедеятельности, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства. Граница, которая позволяла бы обособить частную жизнь в ее узком понимании от иных сфер жизнедеятельности, может быть проведена лишь весьма условно и то далеко

не всегда. Зачастую грань между данными сферами жизнедеятельности оказывается размыта, и это обуславливает необходимость расширительного толкования частной жизни. Возможность включения в содержание частной жизни иных сфер, в процессе которых происходит становление личности (в частности, образовательной, профессиональной), будет иметь своим следствием повышение объема конституционных гарантий свободного развития личности.

Учитывая, что человек, его права и свободы провозглашаются ст. 2 Конституции РФ высшей ценностью, расширение содержания частной жизни представляется обоснованным.

Несмотря на почти 10-летний срок действия Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (далее – закон о персональных данных) установленные им требования к обработке сведений по-прежнему систематически нарушаются операторами, а многие лица, являющиеся субъектами персональных данных, не знают ни объема своих прав, гарантированных законом (гл. 3 закона о персональных данных), ни способов их защиты.

Результаты проводимых Роскомнадзором как уполномоченным органом по защите прав субъектов персональных данных контрольно-надзорных мероприятий показывают, что основными проблемами в этой области являются:

— сбор операторами избыточных сведений персонального характера, запрашиваемых у субъектов персональных данных, необходимость получения которых не обусловлена целями обработки;

— практика "сознательного правонарушения", когда операторы осознанно идут на нарушение требований законодательства, считая, что проще уплатить незначительный штраф (ст. 13.11 КоАП РФ), чем действовать по закону;

— наличие у ряда операторов внутренних документов, определяющих порядок обработки персональных данных, положения которых противоречат нормам закона о персональных данных;

— отсутствие у субъектов персональных данных возможности удалить свои данные, ранее предоставленные операторам, в том числе при использовании интерактивных сервисов (при осуществлении покупок в интернет-магазинах, пользовании социальными сетями и т. д.).

В целях обеспечения защиты прав граждан на неприкосновенность частной жизни, личную и семейную тайну и создания условий для соблюдения закона о персональных данных операторами Роскомнадзор разработал Стратегию институционального развития и информационно-публичной деятельности в области защиты прав субъектов персональных данных на период до 2020 года (далее – Стратегия). Вчера (31 марта) Стратегия была презентована ведомством на специально организованной информационным агентством России "ТАСС" пресс-конференции.

В качестве мер по повышению правовой грамотности населения Стратегия предусматривает, в частности, оптимизацию деятельности существующего Портала персональных данных (pd.rkn.gov.ru), проведение дважды в год дней открытых дверей для консультирования субъектов персональных данных и операторов, занимающихся обработкой данных, по вопросам применения соответствующего законодательства, создание тематических рекламных роликов и их трансляцию на рекламных билбордах, а также перед началом показа фильмов в кинотеатрах и на интернет-сайтах, предоставляющих доступ к легальному кинематографическому контенту.

Особое внимание уделено вопросу защиты персональных данных несовершеннолетних граждан, в том числе в Интернете. Предлагается, например, ввести в школах факультативные занятия по информационной грамотности, на которых детям будут объяснять, как максимально защитить свои персональные данные в сети, избежать взлома аккаунта и

распространения личных данных, и обеспечить информирование несовершеннолетних популярными среди них интернет-сайтами о необходимости ответственно относиться к своим личным данным. Ответственное отношение к личным данным определяется Стратегией как понимание необходимости бережной обработки персональных данных, осознание последствий, которые информационные технологии могут оказать на личную жизнь, репутацию и психологическое состояние субъекта персональных данных.

Информация о ходе реализации Стратегии будет отражаться в ежегодном отчете Роскомнадзора, который он направляет Президенту РФ, Федеральному Собранию РФ и в Правительство РФ. Во многих случаях граждане могут сами предотвратить незаконную обработку своих персональных данных, соизмеряя объем запрашиваемых операторами сведений и цели обработки данных.

Необходимость определения конституционно-правовых рамок защиты персональных данных в России назрела давно. Приходится, однако, признать, что уровень разработанности вопросов конституционно-правовой защиты персональных данных в отечественной доктрине, а также в практике Конституционного Суда РФ не отвечает современным реалиям. Перспективными представляются исследование соответствующих вопросов с использованием метода моделирования и разработка российской модели конституционно-правовой защиты персональных данных, в основу которой может быть положен предложенный подход.

Заключение

Институт персональных данных в настоящее время является относительно новым. Исторически произошедший из института тайны частной жизни, данный правовой институт представляет собой новое обособленное образование.

Но необходимость определения конституционно-правовых рамок защиты персональных данных в России назрела давно. Приходится, однако, признать, что уровень разработанности вопросов конституционно-правовой защиты персональных данных в отечественной доктрине, а также в практике Конституционного Суда РФ не отвечает современным реалиям. Перспективными представляются исследование соответствующих вопросов с использованием метода моделирования и разработка российской модели конституционно-правовой защиты персональных данных.

Итак, защита персональных данных представляет собой сложный технологический процесс, предупреждающий нарушение конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности компании. А обязанность по организации такого комплексного процесса всецело возложена на работодателя (оператора). За нарушение положений законодательства о персональных данных при обработке персональных данных работников виновные лица привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности.

Институт персональных данных относится к публичной отрасли права. В то же время, нормы данного института находят свое отражение и в такой традиционно отнесенной к частному праву отрасли как трудовое (главе 14 ТК РФ). Очевидно, что указанный правовой институт регулирует

общественные отношения, относящиеся к нескольким отраслям права, т.е. находящиеся на стыке отраслей, поэтому, по мнению автора, указанный правовой институт следует рассматривать как межотраслевой.

С практической точки зрения, важность института персональных данных заключается в том, что:

Во-первых, любое физическое лицо является носителем (субъектом) персональных данных, интересы которого связаны с тем, что «принадлежащие» ему персональные данные не должны распространяться произвольным образом и должна обеспечиваться их защита.

Во-вторых, любое юридическое лицо с момента вступления в трудовые отношения хотя бы с одним работником становится оператором персональных данных, на которого возлагается обязанность по обеспечению конфиденциальности, целостности и доступности указанных данных, а также ответственность за нарушения законодательства о персональных данных.

Судебная практика по вопросам обработки и хранения персональных данных является одним из наиболее распространенных категорий трудовых споров. В основном в судах рассматриваются нарушения правил обработки и хранения персональных данных различными организациями. Большинство споров удалось бы избежать, если бы работодатели соблюдали требования федерального законодательства об обработке и хранении персональных данных. В основном суды апелляционной и кассационной инстанции соглашались с выводами судов первой инстанции и оставляют решения без изменений.

С учетом изложенного, представляется, что особенности обработки персональных данных необходимо рассматривать в разрезе обработки персональных данных работников и их защиты. Обработка персональных данных обусловлена общими требованиями, которые строятся на базе принципов добровольности, обеспечения равенства возможностей, законности, не допущения дискриминации в трудовых отношениях. Соответственно этим требованиям, содержащихся в нормативно-правовых

актах трудового законодательства России, должны соответствовать и не противоречить локальные нормативные акты различных организаций и предприятий, дабы не ущемлять и не нарушать законные интересы гражданина Российской Федерации.

В целом, несмотря на наличие ряда основополагающих документов, в существующем нормативно-правовом поле нет единых и исчерпывающих положений, связанных с организационно-правовой защитой персональных данных работников.

Действующее законодательство предусматривает широкий перечень обязанностей операторов возлагаемых на них в связи с обработкой персональных данных работников. Обязанности отражены как в Федеральном законе «О персональных данных», так и в Трудовом кодексе Российской Федерации. Конкретный порядок реализации материальных норм указанных выше нормативно-правовых актов находит свое отражение в процессуальных нормах подзаконных нормативных актов: Указы Президента РФ, Постановления Правительства РФ, приказы ФСТЭК России, ФСБ России. Следует отметить, что на практике указанные выше нормы подзаконных нормативных актов, не в полной мере реализуются операторами. Как правило, это связано с наличием спорных вопросов возникающих в процессе их правоприменения, недостаточным пониманием и не желанием нести финансовые затраты на мероприятия по защите информации.

Помимо обязанностей, действующее трудовое, административное и уголовное законодательство содержит широкий перечень норм, предусматривающих ответственность различных субъектов за нарушение законодательства о персональных данных. Так в нормах трудового, административного и уголовного права предусмотрена ответственность сотрудников за разглашение законно, либо незаконно полученных персональных данных. Ряд норм административного права предусматривает

ответственность операторов персональных данных за нарушение правил обработки и нарушение конфиденциальности информации.

В последнее время в России широкое распространение получила порочная практика распространения и незаконного использования как самих баз персональных данных, так и различных незаконных способов их получения (в большей мере программных). Конфиденциальные базы персональных данных, причём разного уровня конфиденциальности — незаконно полученные как из коммерческих структур (охраняемые в соответствии режимом секретности коммерческой либо профессиональной тайны), так и из государственных органов, персональные данные в которых охраняются в соответствии с режимом служебной тайны — свободно продаются на рынках и в сети Интернет.

Человек не может чувствовать себя защищённым, пока существует угроза вторжения в частную жизнь посторонних лиц — как из праздного любопытства, так и с целью совершения мошеннических и других противоправных действий. А обеспечение безопасности граждан, их основных прав и свобод является главнейшей функцией государства. В связи с этим в России предпринимаются определённые шаги по законодательному урегулированию этой области общественных отношений. Мы, в отличие от западных стран, имеющих уже более чем вековую историю государственного обеспечения и защиты неприкосновенности личной сферы, находимся только в начале этого пути и в процессе создания эффективной и работоспособной системы защиты персональных данных предстоит преодолеть не одно препятствие, однако конструктивное начало уже положено. Ратифицировав Конвенцию, Россия установила «планку», к которой теперь необходимо стремиться. И главный шаг в этом направлении уже сделан: разработана и введена в действие законодательная база — как законы (Закон РФ № 149-ФЗ от 27.07.2006, Закон РФ № 152-ФЗ от 27.07.2006) в качестве основы, регулирующей всю массу общественных отношений в этой области, так и ряд подзаконных

нормативных актов, направленных на реализацию установлений законов, разъясняющих их положения и регламентирующих отдельные материальные и процессуальные вопросы.

Указанное многообразие правового регулирования в то же время, отсутствие практики толкования нормативных актов регулирующих данную сферу, ее слабая изученность, а также невозможность рассмотреть весь спектр проблемных вопросов связанных с защитой персональных данных позволяют считать, что указанное пособие лишь раскрывает проблематику вопроса, которая находится в постоянном развитии.

Список использованных источников

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 №6-ФКЗ, от 30.12.2008 №7-ФКЗ, от 21.07.2014 N 11-ФКЗ). // «Собрание законодательства РФ», 04.08.2014, №31, ст. 4398.

2. «Всеобщая декларация прав человека» (принята Генеральной Ассамблеей ООН 10.12.1948). // «Российская газета», №67, 05.04.1995.

3. Международный Пакт от 16.12.1966 «О гражданских и политических правах». // «Бюллетень Верховного Суда РФ», №12, 1994.

4. Конвенции Совета Европы о защите физических лиц в отношении автоматизированной обработки персональных данных (ETS N 108) (заключена в г. Страсбурге, 28 января 1981 г.). // «Бюллетень трудового и социального законодательства РФ», №4, 2014.

5. Конвенция о защите прав человека и основных свобод от 4 ноября 1950 г. // СЗ РФ. 2001. № 2.

6. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 №14-ФЗ (ред. от 23.05.2016 N 146-ФЗ). // «Российская газета», №23, 06.02.1996, №24, 07.02.1996, №25, 08.02.1996, №27, 10.02.1996.

7. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ (ред. от 03.07.2016 N 353-ФЗ). // «Собрание законодательства РФ», 07.01.2002, №1 (ч. 1), ст. 1.

8. Семейный кодекс Российской Федерации от 29.12.1995 №223-ФЗ (ред. от 30.12.2015). // «Российская газета», №17, 27.01.1996.

9. Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ (ред. от 03.07.2016). // «Собрание законодательства РФ», 07.01.2002, №1 (ч. 1), ст. 3.

10. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (ред. от 06.07.2016). // «Российская газета», №113, 18.06.1996, №114, 19.06.1996, №115, 20.06.1996, №118, 25.06.1996.
11. Закон РФ от 21.07.1993 №5485–1 «О государственной тайне» (ред. от 08.03.2015). // «Российские вести», №189, 30.09.1993.
12. Федеральный закон от 20.02.1995 №24-ФЗ «Об информации, информатизации и защите информации» (от 06.07.2016 N 374-ФЗ). // «Российская газета», №39, 22.02.1995.
13. Федеральный закон от 27.07.2004 N 79-ФЗ "О государственной гражданской службе Российской Федерации" (ред. от 03.07.2016 N 276-ФЗ) // «Российская газета», N 12, 07.08.2004.
14. Федеральный закон от 03.04.1995 №40-ФЗ «О Федеральной службе безопасности» (от 06.07.2016 N 374-ФЗ). // «Российская газета», N 72, 12.04.1995.
15. Федеральный закон от 15.07.1995 №101-ФЗ «О международных договорах Российской Федерации» (ред. от 12.03.2014). // «Российская газета», №140, 21.07.1995.
16. Федеральный закон от 12.08.1995 №144-ФЗ «Об оперативно-розыскной деятельности» (ред. от 06.07.2016 N 374-ФЗ). // «Российская газета», №160, 18.08.1995.
17. Федеральный закон от 25.01.2002 №8-ФЗ «О Всероссийской переписи населения» (ред. от 02.07.2013). // «Российская газета», №17, 29.01.2002.
18. Федеральный закон от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных». // «Собрание законодательства РФ», 26.12.2005, №52 (1 ч.), ст. 5573.
19. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 21.07.2014). // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3451.

20. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» (от 06.07.2016 N 374-ФЗ). // «Собрание законодательства РФ», 31.07.2006, №31 (1 ч.), ст. 3448.

21. Федеральный закон от 27.12.2002 №184-ФЗ «О техническом регулировании» (от 05.04.2016 N 104-ФЗ). // «Российская газета», №245, 31.12.2002.

22. Федеральный закон от 07.07.2003 №126-ФЗ «О связи» (от 06.07.2016 N 374-ФЗ). // «Собрание законодательства РФ», 14.07.2003, №28, ст. 2895.

23. Федеральный закон от 29.07.2004 №98-ФЗ «О коммерческой тайне» (ред. от 12.03.2014). // «Собрание законодательства РФ», 09.08.2004, №32, ст. 3283.

24. Федеральный закон от 22.10.2004 №125-ФЗ «Об архивном деле в Российской Федерации» (ред. от 02.03.2016). // «Собрание законодательства РФ», 25.10.2004, №43, ст. 4169.

25. Указ Президента РФ от 06.03.1997 №188 «Об утверждении Перечня сведений конфиденциального характера» (ред. от 23.09.2005). // «Российская газета», №51, 14.03.1997.

26. Указ Президента РФ от 30.05.2005 №609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» (ред. от 01.07.2014). // «Российская газета», №120, 07.06.2005.

27. Распоряжение Президента РФ от 10.07.2001 №366-рп «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных». // «Собрание законодательства РФ», 16.07.2001, №29, ст. 3011.

28. Постановление Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». // «Российская газета», №200, 24.09.2008.

29. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». // «Российская газета», №256, 07.11.2012.

30. Авакьян С. А. Конституционное право России. Учебный курс: Учеб. пособие: В 2 т. 5-е изд., перераб. и доп. М.: Норма, 2014. Т. 1. 864 с

31. Авдеев М. Ю. Нормативное содержание права на неприкосновенность частной жизни // Новый юридический журнал. 2013. №1. С. 49 – 54.

32. Алексеев С. С. Структура советского права, М., «Юрид. лит.», 1975, 264 с.

33. Алистархов В. Выбор вида наказания работнику за разглашение сведений с ограниченным доступом // Трудовое право. 2014. №9. С. 37 – 48.

34. Амелин Р. В., Богатырева Н. В., Волков Ю. В., Марченко Ю. А., Федосин А. С. Комментарий к Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» (постатейный) // СПС КонсультантПлюс. 2013.

35. Апелляционное определение Московского городского суда от 4 марта 2015 г. по делу N 33-7084.

36. Апелляционное определение Хабаровского краевого суда от 30 мая 2014 г. по делу N 33-3334.

37. Бадьина А. Обработка, порядок хранения и передвижения персональных данных // Кадровик. Кадровое делопроизводство. 2012. №1. С. 162 – 171.

38. Бархатова Е. Ю. Комментарий к Конституции Российской Федерации (постатейный). 2-е изд., перераб. и доп. Москва: Проспект, 2015. 272 с.

39. Давыдова Е. В. Что работодателю необходимо знать о персональных данных работников? // Отдел кадров коммерческой организации. 2015. №3. С. 33 – 42.

40. Егорова О. А., Беспалов Ю. Ф. Настольная книга судьи по трудовым делам: учебно-практическое пособие. М.: Проспект, 2013. 248 с.

41. Изменения в порядке обработки персональных данных в информационно-телекоммуникационных сетях в 2015 году // СПС КонсультантПлюс. 2015.

42. Кодекс Российской Федерации об административных правонарушениях. Главы 11 – 18. Постатейный научно-практический комментарий / И. А. Аксенов, С. Н. Антонов, О. В. Гречкина и др.; под общ. ред. Б. В. Россинского. М.: Библиотечка «Российской газеты», 2014. Вып. IX – X. 880 с.

43. Комментарий к Кодексу Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ (постатейный) (Амелин Р. В., Бевзюк Е. А., Волков Ю. В., Воробьев Н. И., Вахрушева Ю. Н., Жеребцов А. Н., Корнеева О. В., Марченко Ю. А., Степаненко О. В., Томтосов А. А.) (Подготовлен для системы КонсультантПлюс, 2014)

44. Комментарий к Трудовому кодексу Российской Федерации (постатейный) / С. Ю. Головина, А. В. Гребенщиков, Т. В. Иванкина и др.; под ред. А. М. Куренного, С. П. Маврина, В. А. Сафонова, Е. Б. Хохлова. 3-е изд., пересмотр. М.: НОРМА; ИНФРА-М, 2015. 848 с.

45. Комментарий к Трудовому кодексу Российской Федерации (постатейный) / М. А. Бочарникова, З. Д. Виноградова, А. К. Гаврилина и др.; отв. ред. Ю. П. Орловский. 6-е изд., испр., доп. и перераб. М.: КОНТРАКТ, ИНФРА-М, 2014. 1680 с.

46. Комментарий к Уголовному кодексу Российской Федерации: в 2 т. (постатейный) / А. В. Бриллиантов, Г. Д. Долженкова, Э. Н. Жевлаков и др.; под ред. А. В. Бриллиантова. 2-е изд. М.: Проспект, 2015. Т. 1. 792 с.

47. Комментарий к Конституции Российской Федерации. / под ред. В. Д. Зорькина. 2-е изд. М.: Норма, 2011. 1088 с.

48. Конституция Российской Федерации. Доктринальный комментарий (постатейный) / М. П. Авдееenkova, А. Н. Головистикова, Л. Ю. Грудцына и др.; рук. авт. кол. Ю. А. Дмитриев, науч. ред. Ю. И. Скуратов. 2-е изд., изм. и доп. М.: Статут, 2013. 688 с.
49. Кистяковский Б. А. Государственное право (общее и русское). М., 1908 – 1909; Покровский И. А. Основные проблемы гражданского права. Петроград: Право; Правда, 1917.
50. Кротов А. В. Некоторые аспекты права на неприкосновенность частной жизни при реализации информационных прав // Законодательство и экономика. 2013. №4. С. 51 – 54.
51. Кузнецова Т. В. Организация работы с персональными данными // Делопроизводство. 2011. №2. С. 3 – 8; Трудовое право. 2011. №5. С. 77 – 83.
52. Курбатов А. Я. Защита прав и законных интересов в условиях «модернизации» правовой системы России. М.: Юстицинформ, 2013. 172 с.
53. Кухаренко Т. А. Комментарий к Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» (постатейный) // СПС КонсультантПлюс. 2011.
54. Лаптев В. В., Шахматов В. П. Цели правового регулирования и система права // Правоведение. 1976. №4. С. 26–35.
55. Левина М. И. Система российского законодательства теоретическая конструкция и действующая модель. С. 42 – 51 (<http://ecsocman.hse.ru/data/165/680/1219/004.LEVINA.pdf>)
56. Лушников А. Защита персональных данных работника: сравнительно-правовой комментарий гл. 14 Трудового кодекса РФ // Трудовое право. 2014. № 9. С. 93–101; № 10. С. 77–82. СПС «КонсультантПлюс», 2014. Версия 4015.00.09, сборка 208002 (дата обращения: 13.03.2016)

57. Медведева Т. М. О работе с персональными данными работников // Актуальные вопросы бухгалтерского учета и налогообложения. 2014. №21. С. 77 – 88.
58. Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2015 год // [Электронный ресурс] <https://rkn.gov.ru>
59. Панкова О. В. Рассмотрение в судах общей юрисдикции дел об административных правонарушениях / под ред. О. А. Егоровой. М.: Статут, 2014. 440 с.
60. Постановление мирового судьи судебного участка N 8 судебного района г. Уфы Республики Башкортостан по делу N 5-203/2015.
61. Постановление мирового судьи Вологодской области по судебному участку N 9 по делу N 5-1303/2015г.
62. Постановление мирового судьи судебного участка N 12 Зуевского судебного района Кировской области от 8 апреля 2015 г. по делу N 5-199/15.
63. Постановление ФАС Московского округа от 14.01.2010 по делу N А40-38438/09-17-269.
64. Решение судебной коллегии по гражданским делам Санкт-Петербургского городского суда от 26 января 2012 г. по делу N 33-712/2012.
65. Решение по делу 2-4158/2016 ~ М-4370/2016 // [Электронный ресурс] <https://rospravosudie.com>.
66. Путеводитель по кадровым вопросам. Персональные данные работников // СПС КонсультантПлюс. 2015.
67. Новиков В. А. Неприкосновенность частной жизни как конституционное право и объект уголовно-правовой охраны // Юридический мир. 2014. N 7. С. 18 – 21.
68. Разъяснения Роскомнадзора «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве» // <http://rkn.gov.ru/>

69. Разъяснения Роскомнадзора О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки // <http://25.rsoc.ru>

70. Савельев А. И. Законодательство о локализации данных и его влияние на рынок электронной коммерции в России // Закон. 2014. №9. С. 51 – 68.

71. Серков П. П. Административная ответственность в российском праве: современное осмысление и новые подходы: монография. М.: Норма, Инфра-М, 2012. 480 с.

72. Свирин Ю. А. Дивергенция в системе права: монография. М.: Астра Полиграфия, 2012. 392 с.

73. Ситникова Е. Г., Сенаторова Н. В. Трудовой договор: некоторые основания прекращения. М.: Библиотечка «Российской газеты», 2014. Вып. №2. 192 с.

74. Ситникова Е. Г., Сенаторова Н. В. Трудовой кодекс Российской Федерации. Раздел III. Трудовой договор: постатейный научно-практический комментарий М.: Библиотечка «Российской газеты», 2013. Вып. VII – VIII. 720 с.

75. Ситникова Е. Г., Сенаторова Н. В. Расторжение трудового договора по инициативе работодателя (пункты 1 – 6 части 1 статьи 81 Трудового кодекса РФ). М.: Библиотечка «Российской газеты», 2013. Вып. 1. 192 с.

76. Терещенко Л. К. Доступ к информации: правовые гарантии // Журнал российского права. 2010. №10. С. 46 – 53.

77. Терещенко Л. К. Модернизация информационных отношений и информационного законодательства: монография. М.: Институт законодательства и сравнительного правоведения при Правительстве РФ, ИНФРА-М, 2013. 227 с.

78. Терещенко Л. К. Отдельные вопросы применения законодательства о персональных данных // Комментарий судебной практики / под ред. К. Б. Ярошенко. М.: КОНТРАКТ, 2014. Вып. 19. С. 3 – 13.
79. Терещенко Л. К., Тиунов О. И. Правовой режим персональных данных // Журнал российского права. 2014. №12. С. 42 – 49.
80. Федосин А. С. Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в РФ: автореф. дис. ... канд. юрид. наук. Саранск, 2014. 27 с.
81. Хужокова И. М. Эволюция содержания права на неприкосновенность частной жизни в России // Адвокатская практика. 2006. №4. С. 2 – 5.
82. Якушев В.С. О понятии правового института // Правоведение. 1970. №6. С. 62–63.
83. Privacy and «Public Registers» by Roger Clarke, Principal, Xamax Consultancy Pty Ltd, Canberra Individual Reference Services. A Report to Congress. Federal Trade Commission, December 1997
84. Public Records: Access, Privacy, and Public Policy. A Discussion Paper Prepared by Robert Gellman, Consultation on Public Records. April 21, 1995
85. Schiedermaier St. Der Schutz des Privaten als internationales Grundrecht. Mohr Siebeck, 2012. 460 S.