МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
Кафедра теоретических и публично-правовых дисциплин

Заведующий кафедрой
доктор юридических наук, профессор
О.Ю.Винниченко

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
магистерская диссертация

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИЙСКОЙ ФЕДЕРАЦИИ

40.04.01 Юриспруденция
Магистерская программа «Защита прав человека и бизнеса»

Выполнила работу
студентка 3 курса
заочной формы обучения
Шевченко Дарья Витальевна

Научный руководитель
доктор юридических наук,
профессор
Винниченко Олег Юрьевич

Рецензент
ведущий юрисконсульт,
ООО «ТННЦ»
Гаязов Марат Наилевич

Тюмень
2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования обусловлена тем, что в современной юридической литературе справедливо отмечается, что именно информационными ресурсами охватывается познавательная деятельность людей, нам дается возможность узнать обширный перечень знаний о разного рода научных открытиях, исследованиях, получить обновленную информацию. Поэтому информационные ресурсы, становясь основой не только для взаимодействия между людьми, но и в то же время средством воздействия на них, должны гарантироваться их защита и безопасность. С целью создания безопасных условий для разумного управления распространением, а также получением информации, носящей данные персонального характера, необходимо постоянно актуализировать правовое обеспечение защиты ПД.

У самых истоков процесса своего формирования законодательство Российской Федерации в области защиты ПД развивалось, следуя по пути уже пройденному европейским правом. Первым, что сделала Россия на пути формирования данного законодательства, была ратификация ею Конвенции о защите физических лиц при автоматизированной обработке персональных данных.

Вторым шагом на этом пути стало принятие в 2006 году Федерального закона «О персональных данных», закрепившем широкое понимание персональных данных, как и в праве законодательства большинства европейских государств.

Развитие цифровых технологий обусловило необходимость принятия широких мер по защите ПД, что и стали делать многие государства мира, в том числе и Российская Федерация. Российская Федерация является одним из первых государств, которое законодательно закрепило право на забытость. Другими словами, право забвения, которое имеет ввиду под собой право быть забытым. Из чего следует, что такая привилегия дается каждому, но лишь при соблюдении определенных условий. Представляет собой возможность требования удаления своих данных из общего доступа.

Следует также сказать, что Российская Федерация в настоящее время принимает серьезные меры по защите персональных данных путем регулирования своего сегмента Интернета.

Таким образом, законодательство Российской Федерации в области защиты персональных данных в большей степени соответствует европейским образцам. При этом следует сказать, что европейские государства в настоящее время считают, что такие европейские стандарты пора обновить. Причиной этому является цифровизация общественной жизни, имеющееся стойкое противоречие между требованиями о защите персональных данных и тем, что ее практически невозможно обеспечить, когда такие данные вводятся в Интернет.

Таким образом, значимость данного исследования в современном обществе обуславливается непрерывным развитием информационной среды и информационного пространства, которое распространяется на все сферы жизнедеятельности, общества, государства, личности и человека, что в свою очередь требует заблаговременного обеспечения мер защиты информации, носящей конфиденциально-персональный характер.

Объектом исследования настоящей работы являются общественные отношения, складывающиеся в сфере правового регулирования защиты ПД в Российской Федерации, выявление существующих проблем и перспектив развития.

Предметом – нормативно-правовые акты, научная и учебная литература, акты судебных органов, статистика, отражающие различные аспекты правового регулирования защиты ПД в Российской Федерации, выявление существующих проблем и перспектив развития.

Целью выпускной квалификационной работы является анализ правового регулирования защиты ПД в Российской Федерации, выявление существующих проблем и перспектив развития.

Для достижения поставленной цели необходимо решить следующие задачи:

- рассмотреть историю зарождения института защиты ПД в Российской

Федерации,

- изучить понятие и сущность ПД , виды ПД,

- провести анализ правового обеспечения защиты ПД в Российской Федерации и зарубежных странах,

- представить общую характеристику субъекта ПД,

- изучить отличительные черты, хранения, передачи и защиты ПД различных категорий граждан,

- исследовать юридическую ответственность за отступление от буквы закона регламентирующего защиту ПД,

- выделить проблемы и возможность актуализации правового регулирования защиты ПД в Российской Федерации.

Для достижения указанной цели и решения поставленных задач исследование основывалось на положениях материалистической диалектики с использованием частно-научных методов.

Для более детального изучения правового регулирования защиты ПД в Российской Федерации был применен метод синтеза и абстрагирования.

Методы классификации и индукции позволили систематизировать и проанализировать значительный объем информации.

Теоретическую основу составляют научные работы отечественных юристов Ф.А. Абаева, И.Л. Бачило, Э.Н. Бондаренко, А.В. Дворецкого, В.Л. Гейхмана, В.Н. Лопатина, А.М. Лушникова, А.С. Маркевич, У.М. Станскової, А.А. Фатьянова и других.

Теоретические проблемы правового обеспечения информационной безопасности и защиты информации нашли отражение во многих трудах учёных-правоведов.

Так В.П. Иванский, описывал проблемы защиты информации содержащей сведения конфиденциального характера, через сопоставление понятий, явлений, процессов исследуется понятийный аппарат законодательства о защите ПД в европейских государствах.

В трудах А.А. Фатьянова анализируются все существующие в системе российского права институты тайн. Также ученый рассматривает систему

управления обеспечения информационной безопасности в области правового регулирования общественных отношений в Российской Федерации.

В работе А.И. Сотова, особое внимание автор уделяет правовому регулированию статуса компьютерной информации и информационных сетей.

Общие требования при обработке персональных данных работника сформулированы в статьях Т.В. Кузнецовой, Д.Е. Ерохина и других.

Проблемы правового регулирования персональных данных нашли отражение в статьях М.В. Бундина, О.С. Соколовой, Н.Е. Циулиной. Авторы не только раскрывают сущность проблемы защиты персональных данных, но и предлагают пути решения возникающих проблем.

Таким образом, несмотря на то, что огромное количество учёных занимаются проблемой защиты персональных данных работника, тема правового регулирования оборота и защиты ПД работника остается недостаточно изученной и требует дальнейшей научной разработки.

Научная новизна исследования определяется комплексностью предпринятого анализа правового регулирования защиты ПД в Российской Федерации, выявлением существующих проблем и выработкой предложений по совершенствованию действующего законодательства.

Положения, выносимые на защиту:

«1. При наличии достаточных данных полагать, что лицо, в отношении которого ведется производство по делу об административном правонарушении и (или) иное заинтересованное лицо может угрожать свидетелю, иным участникам уголовного судопроизводства или иным путем воспрепятствовать производству по делу об административном правонарушении, механизмом противодействия может являться применение административного задержания на срок до 48 часов, что требует внесения изменений в ст.27.3 КоАП РФ.

2. Целесообразным будет также дополнение КоАП РФ нормами, устанавливающими ответственность за угрозы и (или) подкупы: с целью изменения показаний потерпевшими или свидетелями, по аналогии со ст.309 УК РФ, например, дополнить статью 17.9 КоАП РФ абзацем вторым следующего содержания:

«Подкуп свидетеля, потерпевшего в целях дачи ими ложных показаний либо эксперта, специалиста в целях дачи ими ложного заключения или ложных показаний, а равно переводчика с целью осуществления им неправильного перевода – наказывается штрафом в размере от 30 000 до 50 000 руб.».

3. На наш взгляд, необходимо статью 14 «Права учреждений, исполняющих наказания» Закона РФ от 21 июля 1993 г. № 5473-I «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы» дополнить пунктом 7.1) «осуществлять сбор, хранение и обработку персональных данных, в том числе специальных персональных данных, осужденных, подозреваемых и обвиняемых, в отношении которых в качестве меры пресечения применено заключение под стражу, полученных при осуществлении функций по исполнению наказаний, а также персональных данных иных лиц, полученных в результате обработки персональных данных осужденных, подозреваемых и обвиняемых, в отношении которых в качестве меры пресечения применено заключение под стражу».

Структура выпускной квалификационной работы определяется целью, задачами исследования, а также необходимостью логического распределения материала.

Работа включает введение, две главы, состоящие из семи параграфов, заключение и список использованных источников.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА ИНСТИТУТА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1. ИСТОРИЯ СТАНОВЛЕНИЯ ИНСТИТУТА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Институт ПД зародился в Соединенных Штатах Америки в конце XIX века. Родоначальниками данного института считаются американские юристы Самюэль Уоррен и Луи Брэндайсем. С. Уоррен и Л. Брэндайсем раскрыли значение английского слова «privacy» как «право быть оставленными в покое» (therighttobealone), которое стало начальным этапом становления во всем мире права человека на неприкосновенность частной жизни.

Данная концепция представляет собой в некоторой степени революционный шаг. Это связано с переходом в период постиндустриального общества. Только сейчас становится заметна необходимость в защите прав неприкосновенности частной жизни. На традиционном и индустриальном этапе такие права переходили на второй план.

Причиной возникновения необходимости для урегулирования вопросов связанных с ПД в Соединенных Штатах Америки стало развитие предпринимательской деятельности, а также появление иных способов ведения бизнеса, которые создали определенную возможность посягать на неотъемлемые права граждан, связанные с обработкой ПД [38, С. 487].

Концепция, созданная американскими юристами, оказала на специалистов и законодателей европейских стран очень большое влияние, что стало причиной подписания на Международном уровне следующих нормативных-правовых актов: Всеобщая декларация прав человека [2], принята в 1948 году после окончания Второй мировой войны; Конвенция о защите физических лиц при автоматизированной обработке ПД [4], заключенна 28.01.1981 года в Страсбурге; Директива № 95/46/ЕС Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» [7], принята

24.10.1995 года в Люксембурге; Хартия Европейского Союза об основных правах от 12 декабря 2007 года. Все перечисленные акты защищают права на неприкосновенность частной жизни человека на всеобщем уровне.

На территории современной России предпосылки для создания условий реализации права на неприкосновенность частной жизни были созданы уже давно.

Во времена правления Александра II был принят «Почтовый устав», затем «Телеграфный устав», которые в совокупности представляли первые документы, ограничивающие доступ к информации, которая представляется тайной.

Нарушивших охраняемую этими уставами корреспонденцию наказывали по всей строгости Уголовного уложения. В Уголовном уложении 1903 года были положения, устанавливающие ответственность должностных лиц, которые в ходе осуществления своих обязанностей нарушали неприкосновенность частной жизни людей.

Вскоре после произошедших в 1917 году событий политический вектор развития прав человека кардинальным образом сменил курс.

Так, в 1918 году вступила в силу Конституция РСФСР, которая не содержала даже минимума политических, экономических, социальных и др. прав человека, а лишь имела раздел под названием «Декларация прав трудящегося и эксплуатируемого народа». Весьма примечательным является тот факт, что данный раздел давал исчерпывающий перечень прав, которыми обладал человек:

- право на защиту от эксплуататоров;
- право на участие в управлении;
- право на свободное землепользование.

В этот период не могло быть даже намека на такое право человека, как неприкосновенность частной жизни, потому что политика коммунизма делала невозможным любые проявления не социалистического поведения.

В дальнейшем правам и свободам в СССР не уделялось должного внимания, подтверждением этому является отсутствие в Конституции СССР

1924 года норм, защищающих или признающих права граждан на неприкосновенность частной жизни и тайны переписки.

Наоборот, эта Конституция стала предвестником создания карательного органа под названием «Объединенное государственное политическое управление» истинным назначением, которого, было ликвидация лиц, неприемлемых для власти.

Дальнейшая редакция Конституции СССР произошла 5 декабря 1936 года уже под руководством И.В. Сталина, в которой появился раздел, посвящённый правам и свободам человека и гражданина.

Провозглашённые в данной Конституции права и свободы касались широкого спектра правомочий граждан. Примерами таких прав и свобод являются: статья 124, провозгласившая свободу слова, статья 127, обеспечившая неприкосновенность личности, статья 128, гарантирующая право на неприкосновенность жилища, а также тайну переписки.

Однако, известным фактом остаются события, имевшие место быть в период с 1937 по 1939 год, которые вошли в историю России, как период сталинских репрессий, когда провозглашенные Конституцией СССР права и свободы носили лишь формальный характер.

Впервые за весь советский период на территории России стали говорить о правах человека в 1950-1960-х годах XX столетия, когда произошла смена лидера государства.

В данный период стали появляться различные научные исследования, отмечающие необходимость предоставления гражданам политических, экономических и других прав.

Значимым событием в аспекте реализации защиты ПД человека в мире стало принятие «Международного пакта о гражданских и политических правах» [3].

Данный пакт был ратифицирован на территории СССР и положен в основу новой Конституции, принятой в 1977 году. Конституция СССР 1977 года была разработана по типу самых развитых европейских государств в плане обеспечения граждан различными правами и сводами.

Так статьи 54-56 гарантировали всем гражданам неприкосновенность личности, жилища, право на личную жизнь и тайну переписки. Необходимо особо отметить, что статья 57 Конституции СССР 1977 года обязывала все органы государственной власти уважать личность человека, а также обеспечивать охрану правам и свободам, приведенным в Конституции.

В последние дни своего существования Верховный Совет РСФСР разработал и принял «Декларацию прав и свобод человека и гражданина», в которой говорилось об обеспечении защиты ПД личности.

Именно в этом документе предусматривался запрет на осуществление деятельности, которая связана со сбором, хранением, использованием, а также распространением сведений личного характера без разрешения ее владельца. Нормы, приведенные в этой Директиве, касающиеся защиты ПД в дальнейшем легли в основу Конституции Российской Федерации 1993 года [1].

Следующим шагом современной России направленным на закрепление прав на неприкосновенность частной жизни, охраны информации, составляющей ПД, стало принятие Федерального Закона № 24-ФЗ от 25.01.1995 года «Об информации, информатизации и защите информации», именно в нём закреплялось понятие ПД.

Также этот закон регламентировал деятельность, направленную на сбор, использование и хранения информации о личных данных человека, отнесенные данным законом в круг конфиденциальных.

На этом законодательная деятельность Российской Федерации по обеспечению правовой защиты и регламентации ПД не закончилась.

В настоящее время вышеназванный закон является не актуальным в силу приятия в 2006 году Федерального закона №-152 - ФЗ «О персональных данных» [14], который на данный момент является основным нормативным правовым актом, регламентирующим всю деятельность, направленную на обеспечение правовой защиты ПД человека на территории Российской Федерации.

К иным правовым актам и ведомственным документам, регулирующим рассматриваемую сферу, принято относить:

- Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите ПД при их обработке в информационных системах ПД» [21].

- Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [15].

- Приказ Федеральной службы по техническому и экспортному контролю (далее ФСТЭК) № 17 от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

- Приказ ФСТЭК № 21 от 18 февраля 2013г. – «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПД при их обработке в информационных системах ПД».

- Методика определения актуальных угроз безопасности ПД при их обработке в информационных системах ПД . (ФСТЭК России, 2008 г.)

- Базовая модель угроз безопасности ПД при их обработке в информационных системах ПД (от 15 февраля 2008 г.)

- Банк данных угроз безопасности информации (ФСЭК).

- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». М.: Стандартинформ, 2008.

- ГОСТ РИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

В настоящий период времени вопрос обработки ПД находится в секторе пристального внимания специалистов по отвечающих за безопасность в каждой организации. Сейчас, практически невозможно найти компанию, которая не обрабатывала бы ПД своих сотрудников или контрагентов.

Однако, каждый гражданин вступает во взаимоотношения с различными физическими и юридическими лицами, в результате которых образуются массивы (базы данных) ПД.

Таким образом, созданная в конце XIX века концепция американских юристов к середине XX века привела к созданию нового института защиты ПД.

1.2. ПОНЯТИЕ И СУЩНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ. ВИДЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для начала стоит выяснить, что понятие персональных данных закреплено на законодательном уровне. Также особенностью данного термина является раскрытие его в источниках международного права. Если же говорить о национальном законодательстве ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», то ПД будет являться любая информация, которая относится к определенному физическому лицу. Она может относится к нему как напрямую, влияя тем самым на основные аспекты его жизни, а также и косвенно.

В Конвенции о защите физических лиц при автоматизированной обработке ПД 1981 г., которая является обязательной для нашего государства с 1 сентября 2013 года, ПД определяются как любая информация об определенном или поддающемся определению физическом лице (ст. 2).

Ни в первом, ни во втором из названных нормативных актов понятие персональных данных не конкретизируется, поэтому данный законодательный пробел активно пытается заполнить доктрина.

Для наглядности обратимся к точки зрения Кучеренко А.В. По его мнению в отношении ПД стоит провести классификацию исходя из необходимости обработки данных. Это должно быть предусмотрено законом. Исследователь выделяет ПД, которые обрабатываются:

- с момента регистрации рождения уполномоченным органом (фамилия, имя, отчество, дата и место рождения);

- с момента внесения записи в соответствующие документы (семейное положение, образование, профессия, доходы и т. д.);

- по точному требованию закона и не требуют дополнительного оформления (нация, раса, социальное положение) [51].

По нашему мнению в данный перечень следует добавить вид данный, относящийся к информационной системе.

В тоже время, если досконально разбирать национальное законодательство, то можно увидеть закрепление данной группы ПД. Речь идет о п. 1 ст. 1 Федерального закона о персональных данных. В ней предусмотрены нормы по регулированию отношений в области обработки ПД. При этом используются средства автоматизации.

В современном мире именно защита указанных является наиболее приоритетным и актуальным вопросом так как подвергается хищениями электронных баз данных и торговлей ими.

В другом исследовании, автором которого выступает А. М. Лушников, выделяются иные виды ПД [51], в частности:

- ФИО, а также данные документа, удостоверяющего личность субъекта;

- гендерная принадлежность, количество лет, анатомические характеристики (рост, вес и т. д.) и биометрические данные лица;

- наличие у гражданина образования (специального и/или дополнительного);

- информация о здоровье гражданина и его сексуальной ориентации;

- национальность, расовая принадлежность, религиозные и политические убеждения, принадлежность к конфессии, членство в политической партии и т. п.;

- информация о месте проживания, а также о хобби гражданина, семейное положение лица, наличие детей, родственных связей с иными лицами и пр.);

- автобиография лица, в которой отражена трудовая деятельность (место работы, размер заработной платы, судимости, служба в армии, занятие выборных должностей, прохождение государственной службы и т. д.);

- финансовые активы гражданина (доходы, информация о задолженностях, наличие во владении имущества и т. п.);

- сведения оценочного характера, касающиеся личных и деловых качеств субъекта.

Классификация, предлагаемая данным автором, на наш взгляд, отражает в себе максимальный перечень данных и является самой обширной.

Все же, в условиях современной реальности даже данная классификация требует доработки, так на наш взгляд необходимо включить в вышеуказанный перечень следующую информацию: сведения отражающие кредитную историю субъекта, поскольку довольно часто информация является очень значимой при решении субъектом вопросов носящих экономический характер.

Для того, чтобы полноценно изучить институт ПД необходимо выяснить к какой отрасли права он относится. Как мы уже выяснили, это не гражданское право. Так как источники используемые нами не говорят об этом. Таким образом, наглядно прослеживается тенденция информационного права. Тем самым, можно сказать, что и информационное право представляет собой довольно молодую отрасль права. Связано это с развитием общества и становлением постиндустриализации. То есть главным фактором производства становится информация, приходит она на смену промышленности.

Информационное право появилось на рубеже веков настоящего столетия и до сих пор его нельзя назвать до конца развитой отраслью. Так как просуществовало оно до настоящего момента сравнительно недолго и ещё имеет множество нерешенных вопросов.

ПД (с лат. personal data) - это любая информация, прямо или косвенно относящаяся к определенному или определяемому физическому лицу – субъекту ПД.

Если мы обратимся к юридической литературе, то выясним, что персональные данные имеют достаточно больший спектр классификации. Они могут быть объединены по цели или сложности сбора. Наиболее популярно объединение по степени секретности. Здесь же можно провести параллель с засекреченными данными, которые используются в области информационного права. В тоже время, если мы обратимся к букве закона, то найдем исчерпывающий перечень видов ПД. К ним можно отнести общие, специальный, биометрические и др.

Для того, чтобы разобраться в этом вопросе следует рассмотреть все виды более подробно и выяснить какие данные встречаются чаще всего, а также являются объектом для преступных посягательств. В первую очередь

стоит обратиться к общим ПД. Здесь раскрывается основная информация о человеке. То есть та, которая позволит его идентифицировать на начальных этапах. Это может быть ФИО, место жительства, паспортные данные и др. Именно эта группа данных охраняется законом. И за распространение таких сведений грозит уголовная ответственность.

Общие ПД представляют собой опасность в той части, что они чаще всего легко получаемы. Их можно найти в документах об образовании, а также в паспорте.

Вышеупомянутые данные не раскрывают наши биологические особенности. Поэтому для их обозначения выделяют биометрические.

К биометрическим данным относятся:

-фотография;

-отпечаток пальца или сетчатка глаза;

-зубная карта;

-группа крови;

-запись образца голоса;

-другая генетическая информация [36, С.67].

Приведенные данные могут использоваться как при проведении лечения, так и при трудоустройстве. Например, необходимо оформление документов в государственные органы. Здесь данные могут быть задействованы при изготовлении визы или заграничного паспорта.

У каждого человека есть те сведения, о разглашении которых он чаще всего воздерживается. Это касается нации, религии, сведений о состоянии здоровья. Все это вызывает необходимость в названии их как специальных ПД.

Чаще всего подобные сведения можно найти в медицинских карточках, а также в личном деле. Если говорить о специальных данных, то они могут пригодиться в политической деятельности. Речь идет о вступлении в ряды вооружённых сил. В тоже время они обладают определенной спецификой. Так как для того, чтобы получить такие данные необходимо разрешения владельца.

К числу обезличенных «ПД» относят данные, имеющие всеобщую доступность.

Подобную информацию, помимо средств массовой информации, можно найти в справочниках или других подобных реестрах. Для наглядности можно обратиться к доходам служащих, являющимися персональными данными. Их специфика состоит в их открытости.

В тоже время нельзя сказать о том, что проблем в области персональных данных не существует. Они имеют место быть, и помимо прочего, демонстрируются во всех странах. В тоже время, если рассматривать проблему конфиденциальности персональных данных, то граждане в какой-то степени сами виноваты в их утечке. Речь идет о социальных сетях, благодаря которым можно получить доступ к нежелательным личным данным. В тоже время и эта ситуация имеет свои нюансы.

В тоже время лицо находится в не очень выгодном положении. С той позиции, что гражданин не дает согласия на использование и обработку своих данных согласия. Специфика лишь в том, что это может быть формальная галочка, а не письменный документ. И то это случается не всегда.

Для восполнения данного пробела в социальных сетях должны использоваться «средства управления конфиденциальностью данных, доступные каждому» [44, С.32]. Это позволило бы иметь равные возможности. Тут же следует отметить, что необходимо наличие новых систем, которые бы регулировали и фиксировали использование ПД.

Как мы видим, вопрос защиты ПД очень глубокий и может развиваться в довольно разных направлениях. Задействуется область межгосударственных отношений, что в свою очередь осложняет решение проблем. В тоже время появляется больший набор средств для борьбы с преступными посягательствами в отношении персональных данных.

В настоящий момент информационное общество претерпевает условия новшества. По этому случаю следует искать варианты и компромиссы в области ПД. Речь идет об интересах частных и публичных. Они взаимосвязаны, в тоже время и зависят друг от друга. В тоже время они имеют ряд различий, благодаря которым и происходит конфликт [43, С. 49].

Лишь небольшая часть проблем, которая была рассмотрена в области цифровых технологий в социальной сфере, уже на практике может вызвать немало вопросов. Для их разрешения необходимо усиление нравственных аспектов в законодательстве.

Здесь стоит отметить, что речь идет о внедрении в действие таких НПА, которые регулировали бы основы информационного права. Что касается положений данных законов, то они бы имели нравственные аспекты, препятствующие дегуманизации общественных отношений в сфере цифровых технологий. Другие положения могли бы касаться закреплению гуманистических основ, касающихся конституционного строя.

Таким образом, если рассматривать принятие цифровых технологий и электронных документов как право, принадлежащее гражданину от рождения, то оно не должно являться обязательным в реализации такого вида прав.

На основе вышеприведенных классификаций возможно разделение ПД на:

- данные находящиеся во всеобщем доступе, содержащиеся в «анкетах» (ФИО, место и дата рождения, паспортные реквизиты, информация о полученном образовании, профессиональных навыках, месте работы и трудовом стаже др.). Как уже отмечалось, такие данные легко получить в открытом доступе. Могут быть отражены в справочниках.

В тоже время может быть предъявлено требование об исключении сведений. Этим правом наделяется субъект при существовании определенных условий. Его данные должны не появляться в свободном доступе.

- специальные ПД, охарактеризованы в ст. 10 Федерального закона о персональных данных, законодателем отнесена расовая и национальная принадлежности, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимная жизнь.

Что касается специальных данных, то они должны использоваться лишь в соответствии с законодательством.

- биометрические данные, законодателем отнесены следующие сведения: характеристики физиологических особенностей человека биологических

особенностей позволяющих установить личность субъекта ПД п. 1 ст. 11 Федерального закона о персональных данных.

Обработка данных относящихся к категории биометрических исключительно с согласия их субъекта, отступление от данного правила предусмотренны ст. 11 Федерального закона о персональных данных.

1.3. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИЙСКОЙ ФЕДЕРАЦИИ И ЗАРУБЕЖНЫХ СТРАНАХ

К базовым правам человека первого поколения относится защита неприкосновенности частной жизни. Это право содержит в себе тот момент, который отражает жизнь гражданина тайную от внешних вмешательств, даже со стороны государства. Другими словами, это такие сведения, которые мы бережем от глаз других людей. В тоже время они дают нам свободу выражения своих действий, желаний и возможностей.

Официальное толкование права на частную жизнь на региональном уровне было дано в Декларации Парламентской Ассамблеи Совета Европы (далее - ПАСЕ) «О СМИ и правах человека» 1970 года [6].

Согласно данному толкованию право на частную жизнь представляет собой «право на ведение собственной жизни по собственному усмотрению при минимальном постороннем вмешательстве».

В настоящее время насущным является процесс развития науки. Неразрывно он связан с хранением личной информации, а также её обработкой. Для разъяснение подобных ситуаций и уточнения мотивов сбора данных, необходимо внести коррективы в уже существующее толкование.

Так, в 1998 году ПАСЕ была принята Резолюция № 1165 «О праве на неприкосновенность личной жизни» [9], которая ввела «право на контроль за персональными сведениями».

Согласно позиции ПАСЕ, закреплённое в ст. 8 Европейской конвенции о защите прав человека и основных свобод 1950г. [5], право на неприкосновенность личной жизни должно давать людям защиту от

незаконного вмешательства государственных органов, частных организаций, в том числе СМИ и физических лиц в их жизнь.

Что объединяет государства ПАСЕ? Тот факт, что все они обязаны были принять такие законы, которые бы регулировали и защищала права человека, которые относятся к его личной жизни. Прежде всего, речь идет о главных законах страны. Например, Конституция РФ. Они могут быть нарушены лишь в случаях крайней необходимости, что позволяет гражданам чувствовать себя в безопасности. Следовательно, национальное законодательство должно включать положения:

-в случае имеющихся в публикации посягательств на личную жизнь журналисты и редакторы должны нести ответственность в той же степени, как если бы это была клевета;

-потерпевший должен обладать возможностью требовать возмещение ущерба, понесённого в результате посягательств на его личную жизнь путём предъявления соответствующего гражданского иска;

-при публикации в СМИ сведений впоследствии оказавшихся недостоверными, соответствующий редактор обязан опубликовать опровержение после получения требований заинтересованных лиц;

-осуществление фото-, видеосъёмки и аудиозаписи, потенциально способных нарушить право на частную жизнь или нанести физический ущерб людям должны быть запрещены;

-к издательским группам, которые на регулярной основе нарушают право на частную жизнь, должны быть применены соответствующие экономические санкции в виде штрафа;

-потерпевшему должно гарантироваться право на подачу гражданского иска против фотографа или того лица, вовлечённого в оспариваемое действие, когда «папарацци» осуществили вторжение в его частную собственность либо использовали специальную аппаратуру для увеличения/усиления записи (съёмки), осуществление которой невозможно было бы без вторжения в частную собственность;

-СМИ обязаны разрабатывать внутренние правила, касающиеся публикации материалов, которые могут затрагивать право на частную жизнь и иметь специальное подразделение, предназначенное для работы с жалобами организаций и физических лиц на нарушение их частной жизни и требований об опубликовании соответствующих опровержений;

- должны быть предусмотрены положения, согласно которым частное лицо, обладающее сведениями о том, что кто-то намерен осуществить распространение фото-видео-съёмки/аудиозаписи либо информации касающейся его личной жизни могло воспользоваться правом на ходатайство о возбуждении чрезвычайного судебного процесса, к примеру ускоренного судопроизводства о принятии временных мер по отсрочке публикации подобной информации до принятия судом постановления об имеющемся либо отсутствующем факте вторжения в частную жизнь.

Исходя из практики Европейского суда по правам человека (далее - ЕСПЧ) - понятие «личная жизнь», которое охватывает моральные и физические аспекты жизни лица является достаточно широким и не может поддаваться исчерпывающему определению.

При этом, осуществляя толкование данного понятия, ЕСПЧ рассматривает личную жизнь не столько относительно внутреннего мира индивида, который не может быть полностью контролирован и ограничен по объективным причинам, сколько через призму взаимоотношения индивида и внешней среды.

Представляется очевидным, что понятие «ПД» существенно уже понятия «информация о частной жизни».

По мнению английского учёного-правоведа Рэймонда Уэйкса, под персональной информацией индивида следует понимать те сведения, которые находятся во взаимосвязи с данным лицом, а также относительно которых можно ожидать, что он относит их к конфиденциальным или интимным и соответственно хочет ограничить или даже остановить их обращение [45, С. 31].

Нами были рассмотрены некоторые международные документы, которые имели одну общую черту. Каждое государство заинтересовано в обеспечении прав гражданина в области защиты личной информации. Тем самым государство выступает гарантом защиты данных прав и оно вправе устанавливать санкции за нарушение законодательных положений.

Некоторые персональные данные обрабатывается автоматически. Актуальным было бы установление определенных требований для такого вида информации. Что они должны в себя включать:

-они должны собираться исключительно для законных целей и применяться в полном соответствии с ними;

-при получении, сборе и автоматической обработке должны применяться только законные и добросовестные методы;

- при сборе следует ограничиваться исключительно требуемыми сведениями, не выходя за адекватные пределы необходимых целей;

-сведения должны быть сохранены в форме, позволяющей произвести идентификацию субъекта ПД только до предела заявленной цели, для которой они собраны;

-собираемые сведения должны быть точными и при хранении обновляться на регулярной основе.

Национальное законодательство должно содержать положения, касающиеся вопросов предоставления соответствующих надлежащих гарантий по сбору ПД.

ПД, затрагивающие национальную принадлежность лица, политические взгляды, религиозные убеждения, а также информация затрагивающая сексуальную ориентацию и здоровье, может подвергаться автоматической обработке только в исключительных случаях.

Генеральной Ассамблеей ООН в 2013 году были принята Резолюция 68/167 «Право на неприкосновенность личной жизни в цифровой век» [8], которая касалась влияния процессов цифровизации на правовое регулирование неприкосновенности частной жизни.

В соответствии с данным актом прослеживается тенденция, которая представляет собой негативные последствия. Речь идет о том, что любое использование различных сообщений через электронные технологии негативно скажется на реализации прав.

Вместе с тем Генеральной Ассамблеей ООН был подтверждён тезис о том, что права человека, которые имеются в реальности, должны быть соблюдены и защищены и в виртуальном пространстве. В условиях глобальной и поступательной цифровизации государствам следует и дальше уважать и защищать право на неприкосновенность частной жизни.

Рассматриваемый орган ООО выполняет в некотором роде контролирующую функцию. С чем она связана? Прежде всего, все члены ООО должны периодически проводить обзор внутреннего законодательства. Также следует учитывать автоматический сбор данных на предмет соответствия целям защиты неприкосновенности личной жизни и по обеспечению всеобъемлющего и эффективного выполнения обязательств касающихся соблюдения прав человека добровольно на себя взятых.

В тоже время следует учесть тот факт, что неприкосновенность частной жизни не носит под собой абсолютный и полный характер. В другой ситуации, если все же произошло вмешательство, то следует определить его соразмерность.

Как мы выяснили, информация в эпоху постиндустриального общества является главным фактором производства. Цифровые технологии лишь продлевают жизнь этой информации или же наоборот – делают её быстро устаревшей. Исходя из этого, актуальность защиты частной жизни является неотъемлемой частью современного человека.

В вышеупомянутой резолюции 68/167 был сформулирован призыв к Верховному комиссару ООН по правам человека подготовить специальный доклад о соотношении права на частную жизнь и цифровой трансформации.

В июле 2014 года, Верховный комиссар ООН по правам человека выступила с таким докладом [50].

В данном докладе, в частности, было отмечено, что при малой кристальности государств в отношении принимаемых ими мер, позволяющих воздействовать на реализацию права на неприкосновенность частной жизни попытки по предотвращению пробелов и обеспечению точной ответственности требуют особых усилий.

Чрезвычайное внимание в сообщении акцентировалось на существующей необходимости проведения всеобщего диалога на постоянной основе и выполнения детального анализа по мере того, как информация, касающаяся соответствующих мер, переходит в достояние общественности.

В Организации по экономическому сотрудничеству и развитию (далее - ОЭСР) одними из первых обратились к вопросам необходимости правового регулирования автоматического сбора данных и их перемещений на трансграничном уровне.

Так, в 1980 году в рамках ОЭСР были приняты Фундаментальные положения, регламентирующие защиту неприкосновенности частной жизни и международных обменах ПД. В данном документе содержались рекомендации, которые стали инструментом по унификации и гармонизации национальных законодательств государств-членов ОЭСР по вопросам международного обмена ПД.

В 1981 году, через год после принятия вышеупомянутых Основных положений, Советом Европы принимается Конвенция о защите физических лиц при автоматизированной обработке ПД, которая вступила в силу в 1985 году.

Уже в самом начале документа мы видим указание на то, что необходимо принятие мер по защите прав в области частной жизни. Это связано как с автоматической обработкой наших данных, так и получение их преступным путем и неправомерным вмешательством.

В рамках Европейского союза (далее - ЕС), принцип соразмерной защиты ПД при перемещении через государственные границы был закреплён в 1995 году Директивой Европейского парламента № 95/46 в виде правила, согласно которому государства-члены ЕС не будут вводить меры по запрету или ограничению свободных потоков данных внутри союза.

В тоже время следует учесть, особенности отдельно взятого национального законодательства. Несмотря на попытки его систематизации, не должны исчезать или сокращаться нормы о защите основных прав и свобод. В том числе и право на частную жизнь не должно занимать второстепенную роль. Следовательно, необходимо создание или дополнение национального законодательства таким образом, чтобы были соблюдены принципы ЕС.

Несмотря на то, что де-юре европейская директива представляет собой региональный стандарт, обязательный для государств-членов ЕС, де-факто она стала международным стандартом глобального уровня, который реализуется в государствах, не являющихся членами ЕС.

Подобную особенность может объяснить не столько универсальность норм, сколько тот факт, что данная директива основана на анализе правоприменительной практики государств-членов ЕС по имплементации в национальное законодательство международных принципов.

Проведем анализ правового регулирования рассматриваемых вопросов в России и Германии.

Для подробного изучения стоит обратить внимание на то, что ПД как понятие выступает одним из основных в области информационного права. Теперь же следует изучить нормы закона, в которых данный термин находит свою регламентацию.

Помимо Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных», понятие ПД содержится в Указе Президента РФ № 188 от 6 марта 1997 г. «Об утверждении Перечня сведений конфиденциального характера» [20], таким образом ПД могут также считаться: «данные об известном событии и обстоятельствах частной жизни гражданина, позволяющие провести идентификацию личности за исключением сведений доступных для распространения в средствах массовой информации и в случаях строго запрещенных законодательством».

Также терминология ПД содержится в Конвенции о защите физических лиц при автоматизированной обработке персональных данных [4], принятая в 1999г. в Страсбурге. Рассматриваемая Конвенция раскрывает понятие той

информации, которая преобладает в области ПД. Здесь она представляет собой любую важную информации о конкретном человеке.

Если рассматривать историю разивития ПД, то стоит разделить на два периода. Первый до 2011 года, который отражал содержание ПД в виде той информации, по которой можно определить конкретное лицо. Например, фамилия, дата рождения др.

Впоследствии термин информационное право было изменено, на обработку ПД.

Взяв за основу предлагаемое определение ПД появляется возможность раскрыть некоторые признаки ПД, к примеру: ПД – это информация не имеющая зависимость по способу передачи и фиксации; информация, содержащаяся в ПД, имеет строго определенное отношение к конкретному физическому лицу.

Нами было рассмотрено содержание данных о физическом лице, но что делать с данными умерших? На этот вопрос имеется ответ, который раскрывает тот факт, что информация об умершем не может считаться персональными данными. Таким образом, на практике не возникает с этим сложностей [41, С.86].

К примеру, если сравнивать Россию и Норвегию, Францию разница в субъектах ПД колоссальная. Законодатель данных иностранных государств считает информацию содержащую ПД, случае если такая информация не относится к конкретно-определенному лицу, кроме этого, законодателем отдельно выделяется терминология ПД юридического лица.

Более детально остановимся на законодательстве Германии. Оно совсем не похоже на французское. В чем же его схожесть с отечественным? Прежде всего, стоит начать с терминологии. Она аналогичная российской. ПД представляют собой информацию о конкретном человеке. Сюда же по германскому законодательству включается информация, связанная с профессией того лица, кому поручена обработка данных. Чаще всего – банковская или врачебная тайна.

Что касается операторов, то ситуация одинаковая. определяются они в ФРГ также как и в РФ. Нами употребляется понятие – субъект ПД. Если разбираться в содержании круга лиц, то помимо оператора туда включаются и другие люди. Речь идет о помощниках операторов или о тех, на кого накладывается обязательство по выполнению функций оператора.

В законодательстве ФРГ «О персональных данных», отсутствует терминология, определяющая оператора ПД, вместо этого выделяются следующие термины: «публичное и непубличное учреждение, объединение, ассоциации, образованные применением норм гражданского уложения Германии» [30, С.16].

Изучив институт персональных данных в ФРГ мы выяснили, что область хранения и защиты данный вполне стойкая. В ней есть все инструменты для борьбы против преступных посягательств. Отличительной чертой является лишь отсутствие такого понятие как оператор ПД, что не имеет особой роли и значения. Ведь в законе перечислены те, кто могут ими быть.

Мы воспринимаем ФРГ как одну из развитых стран, наравне с ней в России довольно хорошо развит институт ПД. Возможно, оно ещё находится на самом раннем этапе развития, но благодаря динамичному росту может превратиться в мощный механизм по защите данных.

Проведенный анализ показал, что актуальность и разумность охраны персональных данных присуща практически всем государством. Также в странах прослеживается работа автоматических система обработки данных, что уменьшает процент сбоев и распространения данных в открытый доступ [42, С.39].

Критерий разумности играют важную роль в настоящее время. Именно этот критерий должен являться основополагающим в деятельности операторов ПД.

По мнению Вулкова Т. разумная защита по закону РФ невозможна. Этому лежит простое объяснение. Вспомним счета наших чиновников и прочее имущество – большинство находится за пределами государства, что

представляет собой некоторую сложность при обработке данных. Необходимо, что личные данные хранились только лишь на территории РФ.

Имея множество аналогичных положений с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Закон ФРГ «О персональных данных» тоже выделяет важное направление, которое выражается в разумной защите данных. В тоже время в законе ФРГ решен проблемный вопрос, который встречается и в нашем государстве. Это соблюдение сохранности данных лишь на территории Германии. Другими словами, при обнаружении личных данных на территории других стран необходимо их перевести и установить их факт только на территории того государства, гражданами которого являются лица, выявленных данных. По отечественному законодательству регламентируется лишь письменное согласие, которое не всегда может являться мощным инструментов для защиты персональных данных [30, С.17].

Устанавливается наличие схожих и различных моментов в области регулировании ПД в РФ и ФРГ. В тоже время стоит обратить внимание на более совершенную систему передачи ПД в страны иностранных государств у ФРГ. Законодательные нормы наиболее продуманные и более детализированы, что позволяет говорить о большей вероятности сохранения в тайне ПД. Как и во всех областях, наибольшая защита порождает больший контроль. Так и на территории ФРГ имеет место быть строгий контроль со стороны государства, выраженный в строгом порядке передачи и управлении ПД.

ГЛАВА 2. ПРАВООТНОШЕНИЯ, ВОЗНИКАЮЩИЕ В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. ОБЩАЯ ХАРАКТЕРИСТИКА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Терминология, определяющая субъект ПД раскрывается и в российском законодательстве и в законодательстве европейских стран.

В НПА Европейского союза законодатель выделяет две группы субъектов правоотношения между которыми возникают в процессе обработки, сбора, хранения использования и передачи ПД:

а) Физические или юридические лица (чаще всего физические), к которым непосредственно относят собираемые, обрабатываемые, используемые, передаваемые и хранимые данные. В теории множества стран таких лиц обременяют термином «субъект данных» «data subject»;

б) юридические и физические лица, осуществляющие деятельность связанную обработкой, использованием и передачей ПД. В список таких лиц определяют следующих субъектов.

Контролер или держатель ПД – лицо имеющее право принимать любое решение, не противоречащее закону по вопросам обработки, использования и передачи ПД. (лицо может быть как физическим, так и юридическим).

Пользователь ПД – физическое лицо или юридическое лицо, использующее собираемые и обрабатываемые ПД, при этом данное лицо не является контролером таких данных.

Обработчик ПД – физическое лицо или юридическое лицо, обладающее компьютерными технологиями, непосредственно осуществляющее обработку данных (автоматизированную или ручную), при этом данное лицо не является контролером таких данных.

Сборщик ПД - физическое или юридическое лицо, осуществляющее первичный сбор персональных данных [33, С. 270].

Субъект ПД - это основной участник таких правоотношений, имеющий законные возможности направленные на обеспечение охраны сведений о нем и

предотвращение нанесения вреда личности, доброму имени, чести и репутации. Субъектом ПД является физическое лицо, которое прямо или косвенно определено или определяемо с помощью ПД [29, С.90].

В НПА Европейских стран нет определение такого понятия.

Вместе с тем в теоретических выкладках и в нормативных акты государств - членов Европейского Союза дают возможность полагать, что субъект ПД - это лицо, которое уже идентифицировано, либо еще идентифицируется в настоящее время, или по имеющимся данным может быть идентифицировано в будущем, на основании ПД которые прямо или косвенно к нему относятся, в частности, с помощью ссылки на конкретно-определенный идентификатор, примером могут послужить: ФИО, данные о месте жительства, идентификационный номер или онлайн-идентификатор, также идентификация возможна в случае если известен один или несколько иных факторов, уникальных для генетической, физиологической, умственной, экономической, схожести этого физического лица.

Совокупность прав и обязанностей устанавливаемая законодателем основывается на концепции законной, прозрачной и контролируемой субъектом обработки ПД, отвечающей интересам самого субъекта [39, С. 380].

Изначально вышеупомянутая концепция была изложена в Директиве № 95/46/ЕС о защите физических лиц при обработке персональных данных и о свободном обращении таких данных.

В следствии изменений проведенных в европейском законодательстве о ПД была разработана и принята новая Директива ЕС «О защите физических лиц в отношении обработки персональных данных уполномоченными органами с целью устранения, расследования, обнаружения или уголовного преследования за уголовные преступления или исполнения уголовных наказаний, а равно за открытое перемещение данных и отмене Рамочного решения Совета Европейского Союза 2008/977/JHA» и новый Регламент (Европейского союза) № 2016/679 «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об

отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)».

Одно из главенствующих изменений в Регламенте является регламентация на уровне Европейского союза важнейшего права на забвение. Ранее в директиве от 19995г у граждан была возможность требования исключения данных в том случае, когда обработка и хранение таких данных потеряла свою необходимость, либо в случае, если лицо не желает пользоваться услугами определенной компании. Однако это абсолютно не значит, что по любому запросу гражданина организация должна была бы удалить его ПД.

Статья 17 Регламента закрепляет право на забвение (удаление). Таким образом субъект ПД имеет полное право вынудить контролера данных удалит ПД, без какой-либо задержки, а контролер обязан немедленно удалить такие данные, исключением может быть случай когда обработка таких данных необходима. Но, к сожалению, в данном Регламенте отсутствует разделение двух прав: «право на удаление» и «право быть забытым», что может вызывать трудности при осуществлении такого права в практике.

Директива 1995 года также содержала право на доступ субъекту ПД к информации с содержанием о нем. Во всяком случае новый Регламент имеет более расширенное содержание такого права, раскрывается данное право в ст.15 «Право доступа субъекта данных», с помощью включения следующего положения: субъект ПД обладает правом получения от контролера следующей информации: об обработке его ПД и о том, с какой целью они обрабатываются; со сведениями о получателях или категориях получателей, которыми была получена информация содержащая его личные данные; данные о возможном сроке на протяжении которого ПД будет храниться; наличие законной возможности востребовать у контролера изменения (исправления), ограничения обработки ПД или их удаление; возможность автоматизированного принятия решений, в том числе сбор характеристик работы программы.

Статьей 18 Регламента предусматривается «Право на ограничение обработки данных» таким образом законодатель закрепляет перечень условий при которых субъект данных имеет право требовать от контролера ограничения

обработки ПД: 1) субъектом ПД оспаривается точность данных в течении определенного периода, позволяющего контролеру проверить их точность; 2) субъект данных требует не удаления ПД а их ограничения, однако их обработка является незаконной; 3) ПД для целей обработки больше не нужны контролеру, однако такие данные необходимы субъекту с целью осуществления прав или для их защиты.

Статья 20 Регламента закрепляющая право на портативность данных является новеллой. Так закрепилось , что субъект ПД имеет законное право на получение ПД о самом себе, которые он предоставил контролеру в организованном виде, который обычно используется или в формате машиночитаемом [44].

У субъекта ПД имеется право на возражение обрабатывать его ПД (право на возражение секция 4), исключением является случай, если такая обработка требуется для обеспечения общественных интересов или для осуществления полномочий, возлагаемых на контролера данных.

Анализируя Регламент Европейского Союза, появляется возможность сделать следующий вывод: в правовом акте содержится широкий спектр прав субъектов ПД, которые регламентируются достаточно детально. Однако Регламентом не менее подробно устанавливаются и ограничения прав субъектов ПД, применяющихся только в исключительных случаях.

Область прав, раскрываемых в Регламенте, подлежит ограничению в той мере, в какой требуемое ограничение необходимо и равнозначно мере направленной на обеспечение национальной и общественной безопасности а также публичных интересов.

Вместе с тем любая мера предусматриваемая законодателем должна включать точно определенные тезисы относительно следующих положений: вида ПД; целей обработки ПД; объема примененных ограничений; обеспечение предотвращения злоупотребления, незаконного доступа и распространения ПД; характеристик контролера или их категорий; временных отрезков их хранения и применяемых гарантиях с учетом объема, характера, целей обработки ПД; рисков, связанных с правами и свободами субъектов ПД.

Необходимо отметить, что Регламент в отличие от Директивы 1995 года наиболее полно содержит в себе права субъектов ПД. Сюда можно отнести право исправления, удаления, уведомления и пр.

Данные права находят свое закрепление в гл. 3 Регламента поименованная как: «Права субъекта данных». Глава предусматривает наличие условий при реализации прав в сфере ПД, что облегчает работу при их исполнении. В тоже время Регламент содержит также информацию о доступе к ПД. Закрепление данных положений является положительным моментом в реализации субъектами прав с точки зрения международного права.

Есть некоторые исключительные случаи, при наличии которых Законодательство Европейского Союза или государства-члена имеет возможность предусматривать ограничения вышеупомянутых прав. Подобные ограничения должны представлять собой закрытый перечень, который бы не позволял вольность со стороны рассматриваемых субъектов. Закрепление такого закрытого перечня является одним из главных элементов правового регулирования ЗПД в Европейском союзе.

Субъект ПД – физическое лицо, которое прямо или косвенно определено либо определяемо с помощью ПД. Специфичность прав субъекта заключается в том, что обязанности по их исполнению ложатся на плечи операторов. В тоже время предъявление таких требований может быть ограничено лишь теми данными, которые касаются обработки ПД. В это же время лица наделяются такими правами, которые касаются мер их защиты.

Каждому человеку предоставлено право ознакомления со своими данными. При этом должны учитываться права других людей, которые находятся под государственной защитой. Таким образом, данные должны быть переданы субъекту любыми способами, но не позволяющие раскрыть личные данные другого человека.

Обозначим основополагающие права субъекта ПД.

1. Право субъекта ПД на доступ к своим ПД. Здесь идет речь о праве субъекта ПД в той части, которая позволяет получать ему информацию об операторе. Стоит отметить, что такое право есть, но может использоваться в

случае необходимости. Например, при уточнении или изменении данных. То есть взаимодействие с оператором позволит быстрее разрешить проблемы и установить достоверность [39, С. 450].

2. Право субъекта ПД при обработке его ПД, если это нужно для продвижения на рынке, а точнее услуг или товаров. Сюда же можно отнести информации о выборах, например. Если же имеет место быть незаконная обработка данной информации, то субъект может выразить свое требование на немедленное прекращение такой деятельности. В этом случае оператор обязан удовлетворить подобное требование и прекратить обработку.

3. Право субъекта ПД при автоматизированной обработке таких данных. Решения разрабатываемые для социальной системы признаются законными, если имеется согласие субъекта.

4. Право на обжалование действий (бездействия) оператора. Такое право включает в себя то, что данное лицо может получить компенсацию за разглашение или появление недостоверной информации о себе, которая негативно повлияла на личную жизнь или бизнес.

5. Право на защиту прав и интересов. Данное право предоставляется всем гражданам. Оно выражается в защите своих прав в области охраны ПД.

Лица, виновные в нарушении законодательства о ПД, несут как гражданскую, так и уголовную (ст. 137, 272 УК РФ), административную (ст. 5.39, 13.11. 13.14 КоАП РФ), дисциплинарную (ст. 192 ТК РФ) и иную ответственность.

2.2. ОСОБЕННОСТИ СБОРА, ХРАНЕНИЯ, ПЕРЕДАЧИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТДЕЛЬНЫХ КАТЕГОРИЙ ГРАЖДАН

На данный момент особую актуальность получили вопросы защиты ПД работников силовых структур, так как осуществление таких целей государственными учреждениями оставляет особенный след на работу их сотрудников.

Подчеркнем, что важнейшим вопросом, решаемым как на федеральном,

так и на остальном уровне государственной власти, служит возрастание навыков работы с ПД клиентов, а также самих работников государственных учреждений, в число которых входит МЧС России.

Безопасная и уверенная работа с персональной информацией оказывает огромное влияние на процесс усовершенствования различных направлений деятельности.

МЧС России и все его звенья системы, являясь операторами, выполняющими функции по обработке, хранению и использованию персональной информации, должны удовлетворять в области охраны основных прав граждан, проходящих службу в системе МЧС России, по ЗПД.

Правовую базу этой деятельности составляют: Конституция Российской Федерации, Трудовой кодекс Российской Федерации, Гражданский кодекс Российской Федерации, Федеральный закон от 27 июня 2006 г. № 152-ФЗ «О персональных данных» (ФЗ № 152-ФЗ), Федеральный закон 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ФЗ № 149-ФЗ) и иные нормативные правовые акты Российской Федерации и ведомственные нормативные акты.

Сами же работники МЧС России, независимо от того являются они сотрудниками или государственными служащими, имеют абсолютно свободный доступ к личным ПД и информации об их обработке.

Вышеприведенные права сотрудников Государственной противопожарной службы МЧС России содержатся в п. 24 приказа МЧС России от 20 марта 2017 г. № 121 «О некоторых вопросах централизованного учета ПД сотрудников федеральной противопожарной службы Государственной противопожарной службы и граждан Российской Федерации, поступающих на службу в федеральную противопожарную службу Государственной противопожарной службы» [23], в котором закреплено право на ознакомление сотрудника с отзывами о его служебной деятельности и другими документами до внесения их в его личное дело и др. Это обязательно сопровождается письменной просьбой.

В соответствии с п. 8 ст. 86 ТК РФ работники и их представители должны

быть ознакомлены под подпись с документами работодателя, устанавливающими порядок обработки ПД работников, а также об их правах и обязанностях в этой области. Расммотрим акты МЧС России, где зафиксированы идентичные требования по регулированию порядка обработки, хранения и ЗПД сотрудников МЧС России.

В федеральном органе исполнительной власти в области пожарной безопасности в подразделениях ведутся личные дела, документы учета сотрудников федеральной противопожарной службы, банки данных о сотрудниках и гражданах, поступающих на службу в федеральную противопожарную службу, содержащие ПД сотрудников, сведения об их служебной деятельности и стаже службы (выслуге лет), а также персональные данные членов семей сотрудников и граждан, поступающих на службу в федеральную противопожарную службу.

Основополагающие требования, которые относятся к ПД сотрудников федеральной противопожарной службы, закреплены в ст. 39 Федерального закона от 23 мая 2016 г. № 141-ФЗ «О службе в федеральной противопожарной службе Государственной противопожарной службы и внесении изменений в отдельные законодательные акты Российской Федерации» [16].

В федеральном органе исполнительной власти в области пожарной безопасности нашли отражение требования, которые должны соблюдаться в подразделении при получении, хранении, обработке, использовании и передаче ПД сотрудника федеральной противопожарной службы:

1) ПД должны обрабатываться в соответствии с действующим законодательством Российской Федерации в сфере защиты ПД, а также на основании ведомственных нормативных актов;

2) правильность ПД, полученных от сотрудника, обязана проверяться с участием иных федеральных государственных органов;

3) персональная информация о политических, религиозных и иных убеждениях, частной жизни, о членстве в общественных объединениях сотрудника запрещается получать, обрабатывать и приобщать к личному делу;

4) принимая решения, касающиеся интересов сотрудника,

запрещается основываться на персональных данных сотрудника, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;

5) ЗПД сотрудника от неправомерного их использования или утраты обеспечивается за счет средств оператора обработки ПД в области пожарной безопасности и в порядке, установленном законодательством Российской Федерации;

6) передача ПД сотрудника третьей стороне не допускается без согласия сотрудника, выраженного в письменной форме, за исключением случаев, установленных федеральными законами.

Исходя из вышеизложенного, можно определить, что сотрудники МЧС имеют довольно много прав в области обработки сведений и данных. Здесь стоит отметить то, что в основном это касается государственной тайны, к которой многие сотрудники допускаются при осуществлении своей профессиональной деятельности. В тоже время выделяется специфика ПД в данной области.

Таким образом, сотрудники МЧС напрямую связаны с тайными сведениями и имеют доступ к ним ежедневно в процессе осуществления своей профессиональной деятельности. Это касается государственной тайны. Из чего можно предположить, что личные дела сотрудников представляют особый интерес для изучения их как персональных данных.

В министерстве проблему ЗПД личного дела сотрудника разрешает п. 23 приказа МЧС России № 121, в котором говорится, что документы, содержащие информацию, составляющую государственную тайну и надлежащую засекречиванию, в личное дело не прилагаются и хранятся с соблюдением норм законодательства Российской Федерации о государственной тайне [23].

Конституция Российской Федерации является важнейшей регламентацией права на сведения о ПД. Из этого следует, что подобные права являются основополагающими для сотрудников данного ведомства. Здесь следует ссылаться на ст. 24 Конституции Российской Федерации. Данная правовая норма содержит в себе запрет на собирание информации о частной

жизни граждан без их согласия. На уполномоченные органы возлагается обязанность по сообщению граждан подобной информации, если на этот счет нет законодательных ограничений.

Однако п. 27.9 приказа МЧС России № 121 предполагает, что сотрудник знакомится с записями в послужном списке при оформлении личного дела, далее - не реже одного раза в пять лет, а также перед убытием к новому месту службы и перед представлением к увольнению со службы.

Становится допустимым, что необходимо распространение норм гл. 14 ТК РФ и «Положения о персональных данных государственного гражданского служащего Российской Федерации» и на работников МЧС России, в целях соблюдения прав сотрудников ведомства в области оборота документов, на которых хранятся персональные сведения.

На примере Апелляционного определения Челябинского обл.суда от 14.03.2016 года дело №11-1913/2016 рассмотрим возможности защиты ПД сотрудников работающих в МЧС России [47].

Из материалов дела известно, что работником кадровой службы ФГКУ «СУ ФПС № 29 МЧС России» совершена утеря трудовой книжки сотрудника государственного органа, в последствии данное лицо было привлечено к дисциплинарной ответственности по итогам служебной проверки.

Работодатель лица работающего в кадровой службе доказал его обязанность по обеспечению сохранности личных дел, трудовых книжек, документов воинского учета, подлежащих хранению в запертом металлическом сейфе в соответствии с п.п. 3.11, 3.20 «Должностной инструкции», п. 7.4 «Инструкции по организации и техническому обеспечению безопасности ПД, обрабатываемых в информационных системах», п.п. 1.5, 3.14 «Положения о группе кадровой и воспитательной работы» ФГКУ «СУ ФПС №29 МЧС России», с которыми истица была ознакомлена в установленном порядке.

Невыполнение истцом указанных должностных обязанностей свидетельствует о нарушении Приказа Министерства труда и социальной защиты РФ от 19 мая 2021 г. № 320н «Об утверждении формы, порядка ведения и хранения трудовых книжек» [24].

По итогам рассмотрения в качестве примера данного апелляционного решения необходимо резюмировать следующее: Локальными актами организации возможно установить порядок работы с ПД за нарушение которого работник понесет ответственность.

Проводя анализ аналогичных судебных дел, связанных с нарушениями инструкций по хранению и использованию ПД сотрудниками кадровых отделов МЧС России, было установлено, что базовые нормы об охране такого вида информации отражаются чаще всего в локальных актах и должностных инструкциях сотрудников.

Создание таких вспомогательных актов регламентирующих вышеупомянутые положения способствуют упрощению механизма привлечения сотрудников кадровых служб к различным видам ответственности, за несоблюдение порядка использования и обработки ПД сотрудников.

Однако, не мало важным фактом является то, что в существующем порядке обработки, хранения, использования и защиты ПД работниковм МЧС России не отражен ряд организационных моментов, способствующих ЗПД.

Радикальные новации в части определения порядка и использования ПД всех категорий работников и сотрудников МЧС России должен внести приказ №626 от 31.10.2019г. МЧС России «Об обработке и обеспечении защиты персональных данных в Министерстве Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий». [25]

Целью такого ведомственного правового акта является формирование единых приоритетов, принципов и правил обработки ПД в структурах МЧС России а также определение центральных мер, которые будут реализовываться данной государственной структурой в целях обеспечения ЗПД.

Приказ МЧС России № 626 будет распространяться не только на ПД работников и сотрудников МЧС России, но так же и на ПД граждан РФ полученные федеральным органом исполнительной власти в процессе осуществления своих обязанностей.

По итогам изучения существующего порядка обработки, хранения, использования и защиты ПД граждан, работающих в системе МЧС России, следует отметить что нормы фиксирующие данные положения имеют отсылочный характер в зависимости от категории служащего имеются отдельные отсылки на федеральное законодательство в части использования и ЗПД.

Однако, в ходе проведения исследования также выяснилось, что все НПА закрепляющие положения регламентирующие обработку ПД различных категорий служащих, основываются на общих принципах установленных Федеральными законами №152 и №149.

В связи с тем что правила обработки ПД отдельных категорий работников МЧС России отличаются друг от друга, возникают пробелы в области правового регулирования ЗПД служащих, а также образовывается огромная система, не позволяющая операторам ПД эффективно осуществлять мероприятия применение и защиту ПД

Выходом из такой ситуации является создание единообразного правового подхода МЧС России в области обработки и защиты ПД, а также модификация системы ведомственного нормативного регулирования в области обработки и защиты информации персонального характера как работников соответствующего ведомства, так и иной обрабатываемой информации, затрагивающей интересы других физических лиц.

Важным этапом развития такого направления деятельности является разработка Приказа №626 МЧС России.

Здесь стоит отметить принципы деятельности реализации такой политики. Именно они играют главную роль в раскрытии содержания главных правовых аспектах.

Основополагающими являются следующие принципы:

1) Легитимность;
2) Законность;
3) Демократический характер;
4) Гласность;

5) Обоснованность в науке;
6) Системность;
7) Прогнозирование;
8) Гарантированность;
9) Направление на реально достижимый результат [40, С. 116].

Так как «работа государственных органов выполняется непосредственно их сотрудниками» [31, С. 32], особую роль представляет защита прав и интересов сотрудников МЧС России в сфере работы с их ПД.

Выделяются такие области, в которых имеются пробелы в обработке ПД. Так рассмотрим область ПД в отношении подозреваемых, обвиняемых и осужденных.

Конституцией гарантируется право на неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни человека без его согласия.

Федеральный закон «Об информации, информационных технологиях и защите информации» являются базовым в области изучения информации. В нем раскрывается её понятие и способы для её сохранности и защиты.

Стоит обратиться и к другим нормам закона, которые бы отвечали на наши вопросы. Следует отметить наличие принципа, который является специфичным по отношению к другим институтам информационного права. Речь идет о личной жизни. Ведь такая информация носит личной характер и может распространяться только с согласия лица.

В ФЗ №152 «О персональных данных» дается понятие ПД, раскрываются принципы и условия обработки ПД, согласно данным положениям, обработка ПД ограничена точно определенными заранее целями.

Как уже упоминалось ранее, при обработке личных данных гражданина требуется его согласие. Но есть ли такие ситуации, при которых происходит освобождение от такого согласия? Конечно, есть. Здесь следует привести пример любого судебного акта. Его важность заключается в обязательном исполнении, а также служит документом, который устанавливает юридическую справедливость.

Выше были рассмотрены, которые можно отнести к общим. Что же касается специальных, то здесь есть некоторые отличия. Например, национальная принадлежность, вероисповедание. Управление данными сведениями регламентируется законом. Если мы говорим об осужденных, то это в первую Уголовно-исполнительный кодекс.

В тоже время в приведенном законе отсутствует норма прямо регулирующая понятие и способы защиты ПД у осужденных [11]. Такая ситуация приводит нас на размышления к тому, что данная категория граждан в этой области приравнивается к остальным. Другими словами, осужденные имеют одинаковые права на защиту ПД наравне с остальными гражданами РФ. Однако у осужденных имеются некоторые ограничения, которые написаны в законе. Использование ПД в отношении них должно учитывать подобные обстоятельства.

Закон РФ от 21 июля 1993 г. № 5473-I «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы» [17] устанавливает за учреждениями, исполняющими наказания, право производить регистрацию осужденных, дактилоскопирование, а также их фотографирование, звукозапись, кино- и видеосъемку.

Федеральный закон «Об обеспечении доступа к информации о деятельности судов Российской Федерации» [18] предусматривает регламентацию закрытого перечня ПД, используемых в судебных актах а также правила их использования при публикации текстов судебных решений в открытой сети «Интернет», запрещено публиковать персонифицированные данные позволяющие осуществить идентификацию участников судебных процессов.

В соответствии с ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» [19] «обязательной дактилоскопии, при которой происходит снятие биометрических персональных данных субъекта, подлежат граждане Российской Федерации, иностранные граждане и лица без гражданства, подозреваемые в совершении преступления, обвиняемые в совершении преступления, осужденные за совершение преступления,

подвергнутые административному аресту» [37, С. 156].

Для начала следует обратить внимание, что в уголовно-исполнительных учреждениях имеют место быть внутренние акты, которые регулируют деятельность как осужденных, так и надзирателей. В подобных учреждениях уголовно-исполнительной системы существуют различные подразделения. Сюда можно отнести воспитательные работы, охрану, оперативный отдел и пр. Именно работникам данных отделов открыт доступ к сбору и переработке информации [26].

В этой области задействуются данные не только осужденных, но и их приближенных. Происходит нарушение границ личной свободы других участников, случайно попавших в обработку информации. Несомненно, подобные сведения не входят в ту категорию персональных данных, при которых не требуется согласие на обработку.

Как мы уже выяснили, у заключенных и осужденных нет персональной защиты данных на законодательном уровне, что в полной мере не отражает их право на защиту личной информации. Для этого необходимо предпринять законодательные инициативы, разрешающие данный вопрос.

Таким образом, необходимо дополнить ст. 14 «Права учреждений, исполняющих наказания» Закона РФ от 21 июля 1993 г. № 5473-I «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы» п.7.1) «осуществлять сбор, хранение и обработку ПД, в том числе специальных ПД, осужденных, подозреваемых и обвиняемых, в отношении которых в качестве меры пресечения применено заключение под стражу, полученных при осуществлении функций по исполнению наказаний, а также ПД иных лиц, полученных в результате обработки ПД осужденных, подозреваемых и обвиняемых, в отношении которых в качестве меры пресечения применено заключение под стражу».

2.3. ЮРИДИЧЕСКАЯ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Комплексных исследований на тему ЗПД не проводилось, а количество правоприменительной практики ничтожно мало, появляется немало открытых вопросов в области ответственности. Подобную проблему можно считать относительно новой. Это наглядно проявляется как в теории, так и на практике. Учитывая постиндустриальный тип общества, когда происходит наплыв информации и цифровых технологий, такая проблема является актуальной на сегодняшний день.

Следует подчеркнуть особую важность разрешения проблемы юридической ответственности в области защиты ПД. Основным элементом механизма реализации закона выступает институт юридической ответственности, от которого зависит реализация предпринятых мер.

Законодатель в ходе разработки Федерального закона от 27.07.2006 №152- ФЗ «О персональных данных» закладывал достижение определенных целей, достижение которых возможно только при предусмотрении соответствующих мерами ответственности.

В Федеральном законе от 27.07.2006 №152-ФЗ «О персональных данных» перечисляются специальные категории ПД: информация, касающаяся расовой, национальной принадлежности; политических взглядов, религиозных или философских убеждений; состояния здоровья; интимной жизни; данные о судимости.

Лица обязаны соблюдать требования по защите ПД. Прежде всего, это касается основных субъектов ПД. Если же они будут легкомысленно относится к своей работе, то могут быть привлечены к ответственности. Особенно в настоящее время, когда информация, попавшая в руки злоумышленников может стоить человек семьи, бизнеса или даже здоровья.

С 01.07.2017г. органом, отвечающим за осуществление контроля и надзора за соответствие обработки ПД требованиям Федерального закона о ПД и иных НПА, является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Для этого уполномоченным органом проводится надзор за соблюдение совершения правонарушений.

За нарушение порядка получения, обработки, хранения и защиты персональных данных сотрудников предусмотрена дисциплинарная, материальная, административная и уголовная ответственность (ст. 90 ТК РФ, ч. 1 ст. 24 Федерального закона от 27.07.2006 № 152-ФЗ).

Как мы выяснили, лица, осуществляющие свою деятельность в информационном потоке, могут быть привлечены к разной ответственности. Начиная от гражданской и заканчивая уголовной.

Привлечение оператора или его должностных лиц к ответственности по ст. 13.11 КоАП РФ возможно в случае невыполнения требований Роскомнадзора об устранении нарушений законодательства о ПД.

В ст. 13.11 КоАП РФ содержится 7 составов административных правонарушений, за которые предусмотрены санкции в виде предупреждения или штрафа.

Ввиду изменений от 01.07.2017г, санкция статьи, предусматривающей размер максимального штрафа была увеличена до 75 000 рублей.

Компания может привлекаться к ответственности неоднократно. Так должностных лиц могут оштрафовать на сумму от 3 тыс. до 20 тыс рублей, индивидуальных предпринимателей - на сумму от 5 тыс. до 20 тыс. рублей, организации - на сумму от 15 тыс. до 75 тыс. рублей.

Однако не все субъекты подлежат привлечению к ответственности по ч.7 ст. 13.11 КоАП РФ.

Рассмотрим в качестве примера привлечения оператора и его должностных лиц к ответственности, по ч.1 ст. 13.11 КоАП РФ. Данные лица подлежат ответственности в том случае, если оператором велась или ведется обработка ПД, которую он не в праве осуществлять, либо оператором или оператор и его должностные лица ведут обработку ПД, полученных на законном основании, однако цель обработки не совпадает с целью заявленной на момент сбора данных.

В 2018 году, должностном лицу исполнительно-распорядительного органа муниципального образования г. Тюмени было вынесено

предупреждение – привлечение к ответственности по ч. 1 ст. 13.11 КоАП РФ. Причиной избрания такой меры ответственности явилось следующее:

Как выяснилось, житель Тюмени может получить выплаты от городской власти. В каком случае это может произойти? Если лицо будет находиться по объективным причинам в довольно затрудненной жизненной ситуации. Поэтому наличие такой ситуации необходимо доказать, прежде всего предоставить документы. Стоит заметить, что предоставляются документы не только самого лица, но также и тех людей, с которыми данное лицо проживает. Тут же возникает вопрос о том – реально ли признать предоставление таких сведений законными?

В последствии ответ от суда последовал отрицательный. Хранение копий документов нельзя признать законными.

Согласно ч.2 статьи 13.11 КоАП РФ ответственность наступает, когда для осуществления обработки ПД необходимо согласие субъекта ПД в письменной форме, однако у оператора нет такого согласия, либо не соблюдены требования к форме такого согласия, установленные ч. 4 ст. 9 ФЗ-152.

Для наглядности следует обратиться к административной практике. Рассматриваемое нами дело было установлено в г. Москве. ТСЖ было признано виновным. Был применен штраф. Содержание судебного разбирательства состояло в установлении причин размещения персональных данных физического лица. В открытом доступе присутствовало размещение судебного решения, в которым на всеобщее обозрение были разглашены сведения о гражданине. Общие данные такие как место жительство, место жительства и пр. Несомненно, нельзя признать размещение такой информации законной. Председатель ТСЖ был привлечен к ответственности по ч. 2 ст. 13.11 КоАП РФ.

В ходе исследований было установлено, что письменное согласие субъекта является обязательным. Лишь некоторые, установленные законом случаи, могут использоваться данные без согласия. Следовательно, ТСЖ поступило неправомерно.

Самой жестокой санкцией является та, которая предусмотрена УК РФ. Стоит рассмотреть виды преступлений, которые совершаются в области персональных данных. Всегда ли преступное посягательство связано с использованием средств или для этого достаточно доступа к открытому источнику.

Таким образом, имеют место быть следующие основания для привлечения к ответственности в связи с нарушением правовых норм в сфере ПД работников:

1) п. 2 статьи 137 УК РФ «в случае незаконного собирания или распространения сведений о частной жизни лица без его согласия либо публичное распространение этих сведений, совершенные лицом с использованием своего служебного положения, применяется наказание в виде штрафа до 200 000 рублей, либо обязательными работами на срок до 360 часов, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет или без такового), либо арестом на срок до 4 месяцев, либо лишением свободы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет)» [12];

2) В связи с разглашением персональных данных работников к виновным может применяться статья 272 УК РФ.

В частности, неправомерный доступ с использованием служебного положения к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации наказывается штрафом до 200 000 рублей, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок;

3) Обратной стороной разглашения персональных данных является непредставление информации, касающейся работника.

В статье 140 УК РФ устанавливается ответственность за неправомерный отказ должностного лица в предоставлении собранных в установленном

порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, а также предоставление гражданину неполной или заведомо ложной информации, в связи с чем, причиняется вред правам и законным интересам граждан, в виде штрафа до 200 тыс. рублей, либо лишения права занимать определенные должности на срок от двух до пяти лет.

Какой же ещё вид ответственности мы забыли упомянуть? Это – гражданская. К данному виду ответственности привлекаются субъекты, которые осуществляют свою деятельность в области ПД. Гражданскую ответственность стоит рассматривать учитывая законы, а именно ГК РФ. Теперь рассмотрим статьи, которые относятся к нашей теме:

1) Лицо, чье право нарушено, вправе требовать возмещения причинённых убытков (расходов) которые понесло пострадавшее лицо, и неполученных этим лицом доходов ст. 15.

2) Гражданин, которому вследствие нарушения правил обработки ПД причинен моральный вред, вправе требовать компенсацию морального вреда (независимо от возмещения имущественного вреда и понесенных субъектом убытков), ст. 151 ГК РФ [13].

Вопросом является выявление определяющих признаков. Другими словами, в законе отсутствует прямая связь, предусматривающая определенный размер денежной компенсации за причиненный вред. Необходимым элементом в данном случае будет являться выявление степени причиненных страданий.

Помимо всех вышеперечисленных видов ответственности Трудовым кодексом РФ предусматривается дисциплинарная ответственность, возникающая на основании статей 81, 192 ТК РФ.

Дисциплинарный проступок – неисполнение или ненадлежащее исполнение по вине работника, возложенных на него трудовых обязанностей, то есть, нарушение требований законодательства, обязательств по трудовому договору, правил внутреннего трудового распорядка, должностных инструкций, положений, приказов работодателя, технических правил и т.д (ч. 1 статьи 192 ТК РФ).

Что касается ответственности работника, то к нему может быть применено дисциплинарное взыскание. Чаще всего это замечание, выговор, но в самых крайних случаях – увольнение. Здесь речь идет о легкомыслии со стороны работника при обращении с ПД.

В настоящее время трудовое законодательство регламентирует порядок увольнения работника, который разгласил ПД. Именно это правонарушение может послужить основанием для увольнения и оно будет являться обоснованным. Увольнение производится в связи с совершением однократного грубого нарушения трудовых обязанностей по пп. «в» п.6 ст. 81 ТК РФ.

Может применяться только одно дисциплинарное взыскание. Выбор будет зависеть от тяжести совершенного поступка и уточнении обстоятельств.

Список ответственности, к которому могут быть привлечены лица, совершившие правонарушение в области персональных данных, довольно большой. Это административная, уголовная, гражданско-правовая, дисциплинарная ответственность.

В законодательстве в сфере ЗПД существуют значительные недостатки и пробелы.

Прежде всего, это обусловлено тем, что история развития законодательства в области ПД имеет не более нескольких десятилетий.

Проблемы, возникающие в данной области, связаны с быстрыми темпами развития аспектов информации. Сфера довольно новая по сравнению с остальными правовыми институтами. Поэтому требуется особого внимания со стороны законодателя.

Преступники разрабатывают все возможные технологии незаконного доступа в базы данных с целью хищения информации, а нам требуется защитить со всех сторон данные как технически, так и законодательно, но представители власти сталкиваются с проблемами в решении этого вопроса.

Выделим еще такую острую проблему как масштабное освоение компьютерных технологий со стороны населения, ведь огромная часть подходит к этому делу безответственно, так как граждане не понимают всей

серьезности в защите своих персональных данных. Рассмотрим реализацию такой проблемы на примере крупной компании.

В 2020 году с проблемой утечки персональных данных столкнулось 20% компаний РФ на первый взгляд цифра может показаться не такой значительной, однако в итоге более 100 миллионов записей персональных данных оказываются в открытом доступе. Как предотвратить незаконные утечки персональных данных? В качестве примера мной была взята нефтяная компания (НК) «Роснефть». В данной компании разработана ПОЛИТИКА «В ОБЛАСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ» №П2-03 П-07 от 31.12.2019г. Тем самым компания демонстрирует серьезное отношение к данной информации регламентируя принципы компании в области работы с персональными данными и рассматривая их как ключевые элементы корпоративной социальной ответственности.

В 2017 году на НК «Роснефть» была произведена кибератака, но инцидент не повлиял на работу компании. Казалось бы, вся система идеальна и не требует доработки, однако, компания не останавливается. Сформирована корпоративная стратегия «Роснефть – 2022» в которую также входят усовершенствования в области обработки персональных данных. Проводя анализ деятельности различных компаний экспертами, было выявлено две основные угрозы, приводящие к различным нарушениям в области персональных данных: отсутствие сотрудника, несущего ответственность за обработку персональных данных и ненадежное программное обеспечение.

Проанализировав деятельность Роскомнадзора, а именно нарушения, которые выявляются и политику образцовой компании «Роснефть» следует сделать вывод, что «защита и обработка персональных данных в РФ» не утратит свое значение, а также постоянно требует усовершенствования ввиду постоянного развивающегося общества. Компаниям, у которых отсутствуют локальные акты, рекомендую, за основу брать положения крупных компаний и разрабатывать своё, кроме этого необходимо ежегодно сопоставлять нарушения выявляемые государственным органом с нормами

сформулированными в положениях во избежание утечки персональных данных и возможных пробелов.

Для решения таких проблем нужно подойти с двух сторон. Во-первых, модернизировать работу уполномоченных органов и ускорить процесс внедрения и разработки новых норм регламентирующих защиту персональных данных. Тут же можно разработать небольшие памятки, отражающие способы защиты персональных данных, которые необходимо будет разместить на сайтах государственных органов, а также просто в информационной сети в виде рекламы. Еще одним способом является более квалифицированное обучение специалистов в этой области и увеличение их числа, создание современных способов борьбы с хищением информации, ведь зачастую методы устаревают, а способы хищения, наоборот, развиваются.

Также человеческий фактор является проблемой, поэтому стоить разработать более эффективную систему защиты персональных данных, сделать ее более автоматизированной, для того чтобы у сотрудников не было возможности доступа к базам для их изменения и обработки.

В области защиты данных существует богатая судебная практика [48]. Дискуссия по поводу того, является ли информация персональными данными, остается главным вопросом. Законодатель четко и ясно не закрепил само понятие в законодательстве. Так федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» определено, что персональными данными является любая информация, прямо или косвенно относящаяся к определенному физическому лицу.

Здесь стоит отметить почему этот вопрос вызывает разногласия. Ведь у каждого могут быть свои отличительные черты, которые отражены в информации, позволяющие идентифицировать человека. Следовательно, решающим моментом является вероятность распознания субъекта по имеющееся информации.

Яблоком раздора является вопрос об относимости информации к персональным данным, является возможность распознать субъект на основе данной информации.

Множество разногласий исходит из-за вопроса о том, можно ли считать IP-адрес персональными данными. IP-адрес позволяет распознать устройство, с которого был выполнен выход во всемирную сеть, но не самого юзера. Ведь имея информацию про устройство, возможно определить непосредственно лиц которые им пользовались, что намного упрощает поиск того самого человека.

В настоящее время суды расходятся во мнении IP-адреса. Некоторые относят его к персональным данным, но единого указания на этот факт отсутствует.

Огромное количество дискуссий возникает по поводу того, относится ли изображение субъекта к персональным данным.

В законе говорится о биометрических персональных данных. Просто изображения персональными данными являться не могут, но если их привязать к персональным данным, то тут уже можно говорить об обратном.

Также неоднократно поднимается вопрос касательно адреса электронной почты, так как он не дает возможности установить субъект персональных данных, а является лишь инструментом передачи информации.

Поэтому аналогично, как и в случае с IP-адресом, если учитывать адрес электронной почты, то круг подозреваемых будет намного меньше, что даст нам возможность быстрее вычислить причастного к событию. В настоящее время единого обоснования и подхода к этому вопросу просто нет.

На практике основная часть исков касается именно использование каких-либо персональных данных без согласия этих лиц. Иногда это происходит в журналах или газетах. Для наглядности возьмем ситуацию, которая произошла с несовершеннолетней девушкой. Одна газета «Лабинские вести» опубликовала материал, в котором были обозначены фамилия и имя девушки. Также было сказано о месте её обучения с указанием адреса.

Согласно ФЗ от 27.07.2006 №152 «О персональных данных» такие сведения относятся к персональным данным и для их опубликования нужно согласие гражданина или его законного представителя.

Уполномоченным органом было вынесено письменное предупреждение. Оно предусматривало недопустимость распространения данных, когда не получено было согласие.

Что касается другой стороны спора в лице редактора газеты, то его действия продолжали активизироваться в том же направлении. Редактор не предпринял действий для прекращения распространении информации. Данные лиц продолжали размещаться без их согласия.

Таким образом, в отношении редакции газеты был подготовлен иск о прекращении её деятельности.

Суд удовлетворил исковое заявление Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. Решение суда является полностью обоснованным и абсолютно справедливым.

Суд руководствовался статьей 4 закона РФ от 27.12.1991 № 2124-1 «О средствах массовой информации», согласно которой не допускается разглашение сведений, составляющих государственную или иную специально охраняемую законом тайну, средствами массовой информации. Поэтому персональные данные относятся к сведениям указанным в данной статье.

Согласно ФЗ от 27.07.2006 №152 «О персональных данных» обработка персональных данных может осуществляться только с письменного согласия субъекта персональных данных.

Также, в статье 16 Закона РФ от 27.12.1991 № 2124-1 «О средствах массовой информации» сказано, что суд может прекратить деятельность той или иной организации, осуществляющей СМИ, если оно неоднократно нарушает законодательство.

В случае если редакции стали известные персональные данные, то она обязана обеспечить конфиденциальность такой информации.

Совсем по-другому обстояли дела касаемо магазина, в отношении которого было возбуждено дело об административном правонарушении. Покупатель желал вернуть товар в обратно, но его сотрудники магазина

попросили обязательно заполнить заявление, с полным указанием персональных данных.

Магазин был привлечен к ответственности за совершение административного правонарушения, предусмотренного статьей 13.11 КоАП РФ, так как согласно статье 5 ФЗ от 27.07.2006 №152 «О персональных данных» истребование персональных данных является избыточным. Однако представитель магазина обжаловал такое решение в Верховном суде РФ, который полностью отменил все принятые решения до этого и признал магазин невиновным.

Основанием явился тот факт, что согласно Постановлению Правительства РФ от 19.01.1998 №55 «Об утверждении Правил продажи отдельных видов товаров, перечня товаров длительного пользования, на которые не распространяется требование покупателя о безвозмездном предоставлении ему на период ремонта или замены аналогичного товара, и перечня непродовольственных товаров надлежащего качества, не подлежащих возврату или обмену на аналогичный товар других размера, формы, габарита, фасона, расцветки или комплектации» [22] утверждены Правила продажи отдельных видов товаров, согласно которым покупатель может вернуть купленный товар в магазин и получить свои деньги.

При этом продавец обязан соблюдать Положение о порядке ведения кассовых операций с банкнотами и монетой Банка России на территории Российской Федерации, утвержденное Банком России от 12.10.2011 №373-П [27].

Так получить обратно наличные денежные средства? Указанные в расходном кассовом ордере, возможно при предъявлении паспорта.

Для этого необходимо уточнение по поводу письменного заявление. То есть для признания действий правомерных необходимо требовать такое заявление с указанием общих данных гражданина.

Также в судебной практике нашлось много места спором, связанным с банковской деятельностью. Так как участились случаи утечки информации, содержащей персональные данные третьим лицам.

Рассмотрим один из примеров, где между физическим лицом и банком был заключен договор о потребительском кредите. Так пункт договора конкретно не содержал перечня третьих лиц, которым будут переуступлены права, но содержал условие об уступке прав требования по договору.

Банк был привлечен к административной ответственности по ч. 1 и 2 ст.14.8 КоАП РФ. Банком был нарушен ФЗ от 27.07.2006 №152-ФЗ «О персональных данных». Поэтому у гражданина просто не было выбора, так как не был определен перечень лиц, которым впоследствии могли быть переданы персональные данные субъекта.

В качестве еще одного примера рассмотрим судебное дело, в качестве ответчика выступал банк в связи с включением в кредитный договор пункта, подвергающего избыточной обработки ПД, кроме этого, обработка не соответствовала заявленным целям. Пункт звучал следующим образом «заемщик обязан уведомить кредитора о заключении (изменении) брачного договора, об изменении состава семьи, работы или места жительства, о смене фамилии и об иных данных, позволяющих идентифицировать субъекта».

В ходе судебного разбирательства судом было принято решение о том, что включение такого рода пункта в кредитный договор, является ущемлением прав потребителя, в связи с тем, что требование обязанности по предоставлению в банк персональной информации, является не обязательной так как в Законодательстве РФ не установлена, а кроме этого установление такого требования не влияет на выполнение цели кредитного договора. Суд вынес решение о привлечении банка к ответственности по ч.2 ст.14.8 КоАП РФ.

Законодательство в области ЗПД не является совершенным. Безусловно, решения принимаемые судом в большинстве своем справедливы, однако, имеются и те, которые хоть и приняты на основании действующих нормативно-правовых актов, но по идеи нарушают законы логики.

Для решения такого рода проблем необходимо при разработке правовых актов учитывать каждую мелочь, так как порой, именно они играют значительную роль при принятии решений. Именно это и является загвоздкой в

такого рода проблеме, так как, во-первых, невозможно предусмотреть все варианты событий, а во-вторых, правовые акты будут иметь массивность.

Принято считать, что ЗПД – является задачей государство, однако это не так, помимо того, что это задача государства, это также задача и каждого человека. Согласно Конституции РФ государство должно обеспечивать ЗПД «каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений».

Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Это означает приоритет конституционных прав граждан, которые являются неприкасаемыми. Человек сам решает, какие данные о личной жизни могут стать общедоступными. В идеале так и должно быть, но на практике это случается не всегда. Из-за этого граждане не всегда чувствуют себя защищенными от внешних угроз.

Таким образом, если не будет обеспечиваться ЗПД граждан, то положения Конституции Российской Федерации не будут исполняться. В связи с этим может быть подорван авторитет такого социального института как государство, который в полной мере не может справляться со своими основными задачи. А именно защита граждан не только от внешних угроз, но и от внутренних вмешательств в частную жизнь.

Одной из главных задач государства в данной области – является создание информационных ключей защиты данных, чтобы противостоять мошенническим действиям.

Одн6ако мошенники тоже не сидят на месте и на каждую программу защиты находят ключи взлома, попадая в базу данных хранящую в себе информационные данные граждан. С каждым годом появляется все больше способов для получения личных сведений, что требует своевременного реагирования и пресечения подобных действий.

В тоже время для пресечения преступной деятельности законодательство должно обновляться, подстраиваясь под реалии. Информация в настоящее время является основным ресурсом и достаточно быстро теряет свою

актуальность. Поэтому возникает необходимость в применении наиболее современных инструментов для разрешения данной проблемы [28, С. 25].

Однако если граждане будут неосторожно обращаться со своими ПЩД, предоставлять их компаниям размещающим такие данные в открытом доступе, то государству будет тяжело справляться с задачей защиты ПД, даже невозможно. Поэтому важно быть всегда начеку и бережно относится к своим данным. Даже в случае, если знакомое лицо запросило наши личные данные в сети, то не следует спешить их сообщать. Скорее всего это мошенники, которые пользуются доверительными отношениями между людьми и таким способом выманивают информацию.

Граждане должны быть осмотрительными работая в разных интернет-системах, скачивая приложения или ПО из недостоверных источников, а также переходя по ссылкам у мошенников появляется возможность доступа к данным, хранящимся на гаджете, с которого такой переход был совершен.

Поэтому, гражданам следует соблюдать следующие меры способствующие сохранности ПД, 1) ежемесячно проводить смену паролей в аккаунтах содержащих ПД; 2) Не сохранять пароли в браузерах и приложениях, сторонних лиц, либо на устройствах доступ к которому доступен неограниченному кругу лиц; 3) Не предоставлять ПД лицам звонящим по телефону и представляющимися в качестве сотрудников различных государственных органов, банков; 4) Использовать комплексные защитные программы (антивирусы).

Сотрудники компаний обязаны содержать в сохранности данные работников, для этого необходимо проходить своевременно обучение персонала, постоянно совершенствовать программное обеспечение по защите данных работников, а также неукоснительно соблюдать законодательство РФ в данной области.

2.4. ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Для того, чтобы перейти к рассмотрению проблем в данной области, следует отметить, что деятельность правоохранительных органов направлена на защиту прав и интересов физических лиц, а также и юридических от противоправных посягательств.

Органы внутренних дел занимают важное звено в системе правоохранительных органов. Основная цель их деятельности сводится к охране общественного порядка, общественной безопасности, а также охране законных интересов предприятий и организаций.

Административное судопроизводство, осуществляемое должностными лицами органов внутренних дел, охватывает значительное количество административных составов [10].

Здесь же необходимо отметить, что сотрудники органов внутренних дел на практике встречаются с некоторыми проблемами. Прежде всего, они связаны с защитой персональных данных лиц, которые выступают участниками по административному делу. Такая тенденция негативно сказывается на результатах оперативной деятельности.

Из вышеизложенного следует, что наличие подобных практических проблем является основополагающим фактором необходимости в разрешении таких ситуаций. Здесь следует отметить возможность внесения дополнений и изменений в уже действующее законодательство.

Учитывая приведенные данные, нами предпринята попытка обозначить и проанализировать некоторые проблемы, связанные с защитой персональных данных, тех лиц, которые выступают участниками по делам об административных правонарушениях. Считается необходимым изложить свою точку зрения и свой взгляд на решение приведенных проблем.

Что касается состава участников производства по административным правонарушениям, то здесь стоило бы расширить круг. Имеются ввиду не

только лица, которые привлекаются к административной ответственности, но и свидетели, понятые, а также законные представители.

Персональные данные этих лиц: фамилия, имя, отчество, сведения о дате и месте рождения, о месте жительства, контактный телефон, находят отражение в материалах дела об административном правонарушении.

Теперь рассмотрим, где могут отображаться такие данные. В первую очередь информация о понятых указывается в протоколах применения мер обеспечения производства. Чаще всего это происходит в протоколах личного досмотра, а также досмотра транспортных средств и пр. Что же касается юридического оформления, то личные данные свидетелей и потерпевших закрепляются в протоколе.

Федеральный закон «О персональных данных» устанавливает обязанность сотрудников полиции, осуществляющих производство по делу об административном правонарушении, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Вместе с тем, ст. ст. 25.1, 25.3- 25.5 КоАП РФ закреплено право лица, а также его законных представителей и защитника знакомиться с материалами дела.

В данной ситуации возникают спорные ситуации, так как подобные возможности лиц могут негативно отразиться в жизни человека.

Другими словами, когда указанные в статье лица знакомятся с материалами дела об административном правонарушении, то случайным образом могут получить доступ к личной информации о других участниках производства. Если же говорить об объективных последствиях такого ознакомления, то это может спровоцировать давление одной стороны производства на другую, в том числе шантаж.

Из чего можно сформулировать вопрос, который можно обозначить следующим образом: есть ли у сотрудника полиции полномочие в отказе удовлетворения ходатайства. Речь идет об административном судопроизводстве.

Здесь следует отметить, что основанием для такого отказа будет выступать запрет на недопустимость распространения данных.

Согласно разъяснениям Конституционного Суда Российской Федерации, право лица, привлекаемого к административной ответственности, знакомиться с материалами дела направлено «на конкретизацию гарантированного каждому статьей 24 (часть 2) Конституции Российской Федерации права знакомиться с документами и материалами, непосредственно затрагивающими его права и свободы» [46].

Персональные данные лица, заявляющего о правонарушении, указываемые им в официально подаваемом заявлении, а равно личные данные свидетеля, которые фиксируются в процессуальных документах, в том числе с их слов (например, в протоколе об административном правонарушении), не относятся к сведениям о частной жизни таких лиц и не признаются законодательством об административных правонарушениях закрытыми сведениями, поскольку такие данные необходимы для производства по делу об административном правонарушении.

Следовательно, в рамках дела об административном правонарушении должностное лицо органа внутренних дел обязано при наличии ходатайства ознакомить лицо, в отношении которого ведется производство по делу об административном правонарушении, со всеми материалами дела.

Появляется новая проблема, связанная с обеспечением безопасности отдельных участников производства по делам об административных правонарушениях, например, в случае противоправного, по их мнению, вмешательства в их частную жизнь или посягательства на их безопасность со стороны правонарушителя или иных заинтересованных лиц.

В настоящий момент законодательство отсутствует работающий механизм, который бы гарантировал сохранение в тайне персональных данных. Речь идет именно об участниках в том случае, если возникнет угроза сохранению их данных как со стороны лица совершившего преступления, так и со стороны других лиц, которым было бы выгодно раскрытие данных.

По этому поводу может возникнуть вопрос о дополнительных правовых

средствах защиты отдельных участников производства по делам об административных правонарушениях, против которых может быть совершено противоправное деяние. Несомненно, такая проблема вызывает вопросы в деятельности всех правоохранительных органов. Поэтому проблема о средствах защиты является актуальной и требует скорейшего решения.

Возникла необходимость разработки действенного механизма защиты персональных данных для отдельных участников производства, которые фигурируют в административных правоотношениях.

Для этого следует предоставить право выносить определение о сохранении в тайне данных. Оно будет предоставляться тем лицам, в производстве которых находится дело об административном правонарушении. Прежде всего, это касается тех ситуаций, когда требуется обеспечить безопасность участников производства – потерпевших, свидетелей и пр. В последующем при любом упоминании этих лиц будут использованы псевдонимы.

При наличии достаточных данных полагать, что лицо, в отношении которого ведется производство по делу об административном правонарушении и (или) иное заинтересованное лицо может угрожать свидетелю, иным участникам уголовного судопроизводства или иным путем воспрепятствовать производству по делу об административном правонарушении, механизмом противодействия может являться применение административного задержания на срок до 48 часов, что требует внесения изменений в ст.27.3 КоАП РФ.

Также следует внести дополнения в КоАП РФ, которые бы представляли собой нормы, устанавливающие ответственность за угрозы и (или) подкупы. Здесь подразумевается наличие специальной цели – это изменение показаний потерпевшими или свидетелями. Уточнение такой цели устанавливалось бы по аналогии со ст. 309 УК РФ.

Согласно официальным данным Роскомнадзора за последние три года значительно увеличилось количество жалоб граждан на нарушения прав субъектов персональных данных. В 2020 г. их количество возросло на 22,4%.

Большая часть из них указывает на неправомерные действия владельцев

интернет-сайтов, социальных сетей, коллекторских агентств, организаций ЖКХ, кредитных учреждений [49].

Безусловно, учитывая сложившуюся ситуацию, требуется непрерывный контроль и надзор за правоотношениями в исследуемой области, который на данный момент осуществляются Роскомнадзором и другими службами. До 2019 года происходило становление государственной системы контроля и надзора в области персональных данных, а после 2019 года происходит совершенствование правового обеспечения государственной системы контроля и надзора.

Достаточно большое число нарушений может свидетельствовать о ряде объективных недостатков в законодательстве. Следует помнить и о наличии субъективного аспекта. Человеческий фактор может сыграть роль в абсолютно любой деятельности, но когда от выполнения работы зависит личная жизнь и имущественная составляющая, то необходимо быть более внимательным.

Одной из основных проблем является невнимательность оператора к состоянию защищенности информационных систем, обрабатывающих персональные данные внешних и внутренних субъектов. Как было сказано ранее, в современном мире большое количество правонарушений, посягающих на персональные данные, происходит в сети «Интернет», что свидетельствует о специфичности данной сферы.

Кроме того, немаловажной представляется следующая проблема. Законодатель установил, что при согласии субъекта на обработку персональных данных требуется его подпись в письменном или электронном виде, но не учитывает, что пользователи сети «Интернет» в действительности не имеют таковой, что и является показателем пробела в правовой регламентации области персональных данных.

В частности, мы полагаем, что необходимо дополнить законодательство правовой нормой, которая бы регламентировала электронную подпись субъекта.

Таким образом, решение существующих проблем, затрагивающих правовой институт персональных данных, возможно путем совершенствования

данного института с точки зрения финансового, организационного и правового аспекта.

Следует уделить внимание правовой регламентации, современному программному обеспечению, должному финансированию, а также повышению уровня гражданской сознательности. Безусловно, основная нагрузка ложится на плечи государств в лице контролирующих органов [34, С.36]. Именно от них зависит бдительность граждан при столкновении с аспектами информационного права.

Отметим, что возможности современного мира позволяют получить данные о личности, не прилагая особых усилий, что нарушает не только личное пространство, но и основы прав и свобод.

Тема «защиты персональных данных в РФ» имеет огромное значение и требует еще большего развития, так как общество не стоит на месте и постепенно развивается, что приводит к появлению пробелов в праве и как следствие – нарушение прав граждан в различных сферах.

В связи с этим полагаем, что совершенствование правовой и организационной систем административного регулирования поможет оградить данные человека от незаконного посягательства на них третьих лиц, а также повысит эффективность профилактики предупреждения правонарушений, т. ч. административных, в области персональных данных, тем самым гарантируя защиту неприкосновенности частной и личной жизни человека и гражданина.

ЗАКЛЮЧЕНИЕ

Подводя итог, можно сделать следующие выводы и предложения.

21 век называют веком информационных технологий. Это обусловлено тем, что в мире происходит глобальная автоматизация, происходит переход от «индустриального общества» к информационному». Безусловно, современное техническое оснащение и программное обеспечение значительно облегчают жизнь и работу человеку, но не все так красочно, как можно представить. Автоматизируя сбор, хранение и передачу ПД, ставится в опасность сохранность данных, появляется непосредственная опасность использования ПД в недобросовестных, в том числе незаконных целях. Тема «защиты персональных данных в РФ» имеет огромное значение и требует еще большего развития, так как общество не стоит на месте и постепенно развивается, что приводит к появлению пробелов в праве и как следствие – нарушение прав граждан в различных сферах.

Как уже отмечалось ранее, мы живем в эпоху постиндустриального общества. Поэтому вопрос о защите и охране ПД является особо актуальным. Ведь время развития цифровых технологий сопровождается не только положительными результатами, но иногда и отрицательными и даже преступными. Для этого требуется разработка комплекса мер, направленных на защиту наших персональных данных. Главную роль в области защиты ПД занимает государство. Именно на него возлагает обязанность по установлению действенных механизмов защиты ПД. Защита ПД – неотъемлемое конституционное право каждого гражданина.

К ПД следует относить ФИО, дату рождения, место рождения и проживания и др.

ПД – это информация содержащая сведения относящиеся к конкретному субъекту, позволяющая осуществить идентификацию, однако являющаяся ограниченной для пользования другими лицами.

Законодательство направлено на защиту граждан от противоправных посягательств. Противоправность в данной сфере может быть выражена в

незаконном распространении и использовании ПД. Последствия бывают не из приятных – осквернение чести и достоинства, потеря деловой репутации гражданина.

В Российской Федерации защита ПД от противоправных посягательств гарантируется Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Здесь стоит отметить важность данного органа в области ПД. Он осуществляет контроль в сфере сведений, которые поддаются обработке. Однако самой важной функцией является то, что орган является основным в отношении института ответственности. То есть, ели произойдет нарушение прав гражданина в случае неправомерных действий, связанных с обработкой ПД.

Обрабатывать ПД возможно только в случае согласия на это субъекта ПД и в строгом соответствии с заявленной целью, в случае отсутствия согласия владельца ПД такие деяния будут расцениваться как нарушение Конституции РФ. Ведь основной закон выступает основной поддержкой граждан на частную жизнь.

Обработка ПД осуществляется с помощью специального оборудования и программ, разрешенных Федеральной служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), уполномоченного осуществлять контроль и надзор в рассматриваемой сфере отношений.

В результате данного исследования мы выявили категорию лиц, которые именуются операторами. Они выполняют свою главную функцию, заключающуюся в обработке ПД. В тоже время операторы обязаны соблюдать требования по защите ПД, установленные в законодательстве. За их несоблюдение предусмотрена ответственность, которая может негативно сказаться на их деятельности. Поэтому операторы должны внимательно обращаться с ПД.

В работе были рассмотрены частные случаи из практики, которые продемонстрировали наличие проблемных вопросов. В том числе это касается незащищенность ПД перед открытым доступом.

Предлагаю, для обеспечения должной защиты ПД от неправомерных посягательств внести следующие изменения:

1. Зачастую между преступлением и правонарушением существует очень тонкая грань, но в отличие от уголовного процесса, в административном, крайне мало внимания уделяется вопросу защиты свидетелей.

Такая ситуация приводит к тому, что путем угроз, шантажа или иных незаконных действий виновные полностью уходят от ответственности или сводят санкции к минимуму.

При наличии достаточных данных полагать, что лицо, в отношении которого ведется производство по делу об административном правонарушении и (или) иное заинтересованное лицо может угрожать свидетелю, иным участникам уголовного судопроизводства или иным путем воспрепятствовать производству по делу об административном правонарушении, механизмом противодействия может являться применение административного задержания на срок до 48 часов. Это изменение должно быть закреплено в ст. 27.3 КоАП РФ.

2. Достаточно распространенными в настоящее время являются ситуации, когда в попытках избежать административной ответственности виновные пытаются «договориться» с потерпевшими, свидетелями, предлагая деньги или угрожая, данные действия также должны подпадать под состав административного правонарушения и влечь за собой применение соответствующих мер ответственности.

Видится необходимым включить в Кодекс об административных правонарушениях РФ аналогичные нормы содержащиеся в Уголовном кодексе РФ устанавливающие ответственность за угрозы и (или) подкупы: Здесь стоит отметить наличие специальной цели. Именно это будет являться новеллой в национальном законодательстве. Цель – изменений показаний потерпевшего

или свидетеля. По аналогии со ст.309 УК РФ, например, дополнить статью 17.9 КоАП РФ абзацем вторым следующего содержания:

«Подкуп свидетеля, потерпевшего в целях дачи ими ложных показаний либо эксперта, специалиста в целях дачи ими ложного заключения или ложных показаний, а равно переводчика с целью осуществления им неправильного перевода – наказывается штрафом в размере от 30 000 до 50 000 руб.».

3. В настоящее время нет единой правовой регламентации сбора и обработки персональных данных осужденных, подозреваемых и обвиняемых.

К тому же действующее законодательство не в полном объеме регулирует вопросы защиты информации личного характера граждан Российской Федерации, используемых при выполнении задач Федеральной службы исполнения наказаний.

На наш взгляд, необходимо статью 14 «Права учреждений, исполняющих наказания» Закона РФ от 21 июля 1993 г. № 5473-I «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы» дополнить пунктом 7.1) «осуществлять сбор, хранение и обработку персональных данных, в том числе специальных персональных данных, осужденных, подозреваемых и обвиняемых, в отношении которых в качестве меры пресечения применено заключение под стражу, полученных при осуществлении функций по исполнению наказаний, а также персональных данных иных лиц, полученных в результате обработки персональных данных осужденных, подозреваемых и обвиняемых, в отношении которых в качестве меры пресечения применено заключение под стражу».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативно-правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)// [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).
2. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ: по сост. на 09.11.2021// [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).
3. Уголовно-исполнительный кодекс Российской Федерации от 08.01.1997 № 1-ФЗ: по сост. на 11.06.2021// [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).
4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ: по сост. на 01.07.2021// [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).
5. Гражданский кодекс Российской Федерации от 30 ноября 1994 г. № 51-ФЗ: по сост. на 26.10.2021// [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).
6. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ по сост. на 02.07.2021 // [Электронный ресурс] - Доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).
7. Об информации, информационных технологиях и о защите информации: Федеральный Закон от 27 июля 2006 г. № 149-ФЗ по сост. на 02.07.2021 // [Электронный ресурс] - Доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).
8. О службе в федеральной противопожарной службе Государственной противопожарной службы и внесении изменений в отдельные

законодательные акты Российской Федерации: Федеральный закон от 23 мая 2016 г. № 141-ФЗ по сост. на 30.04.2021 // [Электронный ресурс] - Доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

9. Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы: Закон РФ от 21.07.1993 № 5473-1 по сост. на 26.05.2021 // [Электронный ресурс] - Доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

10. Об обеспечении доступа к информации о деятельности судов в Российской Федерации: Федеральный закон от 22.12.2008 № 262-ФЗ по сост. на 08.12.2020 // [Электронный ресурс] - Доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

11. О государственной дактилоскопической регистрации в Российской Федерации Федеральный закон от 25.07.1998 № 128-ФЗ по сост. на 13.07.2020 // [Электронный ресурс] - Доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

12. Об утверждении перечня сведений конфиденциального характера: Указ Президента РФ от 6 марта 1997 г. № 188 по сост. на 13.07.2015 // [Электронный ресурс] - Доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

13. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012 №1119 по сост. на 01.11.2012 // [Электронный ресурс] - Доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

14. О некоторых вопросах централизованного учета персональных данных сотрудников федеральной противопожарной службы Государственной противопожарной службы и граждан Российской Федерации, поступающих на службу в федеральную противопожарную службу Государственной противопожарной службы: Приказ МЧС России от 20 марта 2017 г. № 121 по

сост. на 20.03.2017 // [Электронный ресурс] - Доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

15. Об утверждении формы, порядка ведения и хранения трудовых книжек: Приказ Министерства труда и социальной защиты РФ от 19 мая 2021 г. № 320н по сост. на 19.05.2021 // [Электронный ресурс] - Доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

16. Об обработке и обеспечении защиты персональных данных в Министерстве Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий: Приказ МЧС России от 31 октября 2019 г. № 626 по сост. на 31.10.2019 // [Электронный ресурс] - Доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

17. Об утверждении Инструкции по профилактике правонарушений среди лиц, содержащихся в учреждениях уголовно-исполнительной системы: приказ Минюста России от 20.05.2013 № 72 по сост. на 20.05.2013 // [Электронный ресурс] - Доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

18. О порядке ведения кассовых операций с банкнотами и монетой Банка России на территории Российской Федерации: Положение ЦБР от 12 октября 2011 г. № 373-П по сост. на 12.10.2011 // [Электронный ресурс] - Доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

Международные договоры и документы

19. Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948) // [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

20. Международный пакт о гражданских и политических правах" (Принят 16.12.1966 Резолюцией 2200 (XXI) на 1496-ом пленарном заседании

Генеральной Ассамблеи ООН) // [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

21. Конвенция о защите физических лиц при автоматизированной обработке персональных данных" (Заключена в г. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ N 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

22. Конвенция о защите прав человека и основных свобод (Европейская конвенция о правах человека, ETS № 005) (Рим, 4 ноября 1950 года) (с изменениями и дополнениями по состоянию на 13.05.2004 г.) // [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

23. Декларация о средствах массовой информации и правах человека, принята Резолюцией Парламентской Ассамблеи Совета Европы № 428 (1970) http:// [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

24. Директива № 95/46/ЕС Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

25. Резолюция, принятая Генеральной Ассамблеей 18 декабря 2013 года «Право на неприкосновенность личной жизни в цифровой век» // [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

26. Резолюция Парламентской Ассамблеи Совета Европы № 1165 (1998) «О праве на неприкосновенность личной жизни» http:// [Электронный

ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения: 17.11.2021).

Научная и учебная литература

27. Боброва Н.А. Парадоксы применения законодательства о персональных данных // Юрист вуза. 2019.№5. С. 24-33 // [Электронный ресурс] – Доступ из научной электронной библиотеки «eLIBRARY.RU».

28. Вельдер И.А. Система правовой защиты персональных данных в Европейском Союзе. Диссертация на соискание ученой степени кандидата юридических наук. - Казань, 2006. – 98 с. // Книжное издание.

29. Вуколова Т. Законодательство о персональных данных в Германии и России. Сравнительно-правовое исследование / Т. Вуколова // ИС. Авторское право и смежные права. 2016. № 4. С. 15 – 30 // [Электронный ресурс] – Доступ из научной электронной библиотеки «eLIBRARY.RU».

30. Гавриленко В.А., Уткин Н.И., Фастович Г.Г. Кадровая работа и роль института поощрения в системе государственной службы. // Право. Безопасность. Чрезвычайные ситуации. 2019. № 3 (31). С. 32 //[Электронный ресурс] – Доступ из научной электронной библиотеки «eLIBRARY.RU».

31. Долинская В.В. Защита прав в сфере персональных данных в России и ЕС. // Законы России: опыт, анализ, практика. - 2019. - № 9. - С. 22-29 //[Электронный ресурс] – Доступ из научной электронной библиотеки «eLIBRARY.RU».

32. Иванский В.П. Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования. - Москва: РУДН, 1999. - 276 с. //Книжное издание.

33. Крюкова Д.Ю., Мокрецов Ю.В. Актуальные проблемы правового регулирования оборота и защиты персональных данных в России // Пенитенциарная наука. 2017. № 38. С. 34-38 //[Электронный ресурс] – Доступ из научной электронной библиотеки «eLIBRARY.RU».

34. Лушников А. М. Защита персональных данных работника: сравнительно-правовой комментарий гл. 14 Трудового кодекса РФ // Трудовое право. - 2009. - № 9. - С. 93-101 //Книжное издание.

35. Мамаев В. Биометрия: от предчувствия к материализации. // Банковское обозрение. - 2018. - № 3. - С. 68-71 //[Электронный ресурс] – Доступ из научной электронной библиотеки «eLIBRARY.RU».

36. Матросов Д. А., Назарова А. Б., Ширкин А. А. Об определении угроз безопасности при создании систем защиты информации в учреждениях и органах уголовно-исполнительной системы // Закон и право. 2018. № 11. С. 155-158 // [Электронный ресурс] – Доступ из научной электронной библиотеки «eLIBRARY.RU».

37. Постовалова Т.А. Трудовое право Европейского союза: теория и практика. / Т.А. Постовалова. - М.: Проспект, 2015. С.496 // Книжное издание.

38. Право Европейского Союза: учебник для академического бакалавриата / С.Ю. Кашкин. П.А. Калиниченко, А.О. Четвериков; под ред. С.Ю. Кашкина. - 4-е изд., перераб. и доп. - Москва: Издательство Юрайт, 2019. - 386 с. // Книжное издание.

39. Правовая политика в сфере обеспечения пожарной безопасности, гражданской обороны, чрезвычайных ситуаций и ликвидации последствий стихийных бедствий: обзор материалов «круглого стола» // Государство и право. 2015. № 6. С. 116 // [Электронный ресурс] – Доступ из научной электронной библиотеки «eLIBRARY.RU».

40. Проскурякова М.И. Персональные данные: российская и германская национальные модели конституционно-правовой защиты в сравнительной перспективе / М.И. Проскурякова // Сравнительное конституционное обозрение. 2016. № 6. С. 84 – 98 // [Электронный ресурс] – Доступ из научной электронной библиотеки «eLIBRARY.RU».

41. Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». /под ред. А.И. Савельева М.: Статут, 2017. 320 с. // Книжное издание.

42. Харитонова А.Р. Сохранность и анонимность персональных данных в социальных сетях. // Право и бизнес. - 2019. - № 4. - С. 48-55 // [Электронный ресурс] – Доступ из научной электронной библиотеки «eLIBRARY.RU».

43. Garfinkel S.L. Database Nation; the Death of Privacy in the 21st Century. O'Reilly and Associates, 2000. -319 p. // Книжное издание.

44. Wakes R. Protection of Privacy. London. Sweet&Maxwell. 1980. P. 31. // Книжное издание.

Материалы судебной практики

45. Определение Конституционного Суда РФ от 28 июня 2012 г. № 1253-О: «Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации» // [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения 17.11.2021).

46. Апелляционное определение Челябинского областного суда от 14 марта 2016 г. по делу № 11-1913/2016 // [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения 17.11.2021).

47. Апелляционное определение Санкт-Петербургского городского суда от 15.11.2016 г. №33-22976/2016 по делу №2-2932/2015 // [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения 17.11.2021).

48. Апелляционное определение Московского городского суда от 12.12.2016 г. по делу №33-42101/2016 // [Электронный ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения 17.11.2021).

49. Апелляционное определение Санкт-Петербургского городского суда от 31.01.2017 г. №33а-1151/2017 по делу № 2а-4760/2016 // [Электронный

ресурс] – доступ из справочно-правовой системы «Консультант плюс» (дата обращения 17.11.2021).

Статьи и иные источники

50. В 2019 году вновь выросло количество поступивших в Роскомнадзор жалоб по тематике защиты персональных данных: [сайт]. - URL: https:// rkn.gov.ru/news/rsoc/news71528.htm.

51. Доклад Защита персональных данных: международные документы и национальные законодательства [сайт]. - URL: https:// www.lawtrend.org/information-access/zashhita-personalnyh-dannyh/mezhdunarodnye-i-natsionalnye-pravovye-akty.

52. Исследовательский потенциал молодых ученых: взгляд в будущее. Сборник материалов XV Региональной научно-практической конференции магистрантов, аспирантов и молодых ученых [сайт]. - URL: https: // elibrary.ru/item.asp?id=35612794 (дата обращения 07.09.2021).