МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»
Институт права
(наименование института полностью)

Кафедра «Предпринимательское и трудовое право»
(наименование)

40.04.01 Юриспруденция
(код и наименование направления подготовки / специальности)

Правовое обеспечение предпринимательской деятельности
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему Правовое регулирование в сфере защиты персональных данных

Обучающийся Э.Д. Абдулова
(Инициалы Фамилия) (личная подпись)

Научный руководитель к.ю.н., доцент О.Е. Репетева
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2022

Содержание

Введение

Актуальность работы: В современном развивающемся мире человеку нужны гарантии неразглашения личной информации, а также гарантии невмешательства в личное пространство работника третьих лиц и работодателя. Личная информация и интересы личности должны выражаться в неприкосновенности частной жизни при обработке персональных данных.

Сейчас персональные данные выступают основным идентификатором личности, требующим надежной защиты.

В современной Российской Федерации проблема защиты персональных данных в сети «Интернет» последние несколько лет является достаточно актуальной. Такая ситуация объясняется тем, что различными социальными сетями, мессенджерами, электронной почтой, да и просто самим интернетом пользуется большое количество граждан. При активном пользовании всем вышесказанным человек оставляет некоторые данные, которые могут дать информацию о нем. Эти данные могут быть различными, начиная просто от имени и фамилии и заканчивая всеми данными паспорта.

В настоящее время, несмотря на значительные усилия российского законодателя, процессы, связанные с собиранием, хранением и обработкой персональных данных, не обеспечивают надлежащий уровень их конфиденциальности и правовой защиты. В большинстве случаев данные хранятся и анализируются с целью улучшения качества предоставляемых услуг.

Проблема конфиденциальности и обеспечения безопасного хранения таких данных особенно актуальна в условиях цифрового пространства.

Степень разработанности темы: правовое регулирование в сфере защиты персональных данных фрагментарно изучали многие авторы, такие как Л.К. Терещенко, И.Ю. Павлова, А.А. Гадельшин, М.М. Степанов, Д.Р. Салихов, но комплексного исследования по данной теме с основными проблемами и путями решения в 2020-2022 годах не удалось выявить. Хотя фрагментарно тема достаточно изучена в работах российских авторов. «Например, в работе

Л.К. Терещенко рассматриваются два проблемных вопроса российского законодательства о персональных данных - (1) определение понятия «персональные данные» и (2) разграничение операторов и обработчиков персональных данных. Для решения каждого из них автор предлагает использовать трехступенчатые тесты, позволяющие понять, является ли та или иная информация персональными данными и какую конкретно роль играет организация в обработке персональных данных» [39].

Работа И.Ю. Павлова посвящена проблемам новейшего правового регулирования персональных данных гражданина; вопросам соотношения персональных данных с банковской тайной, в том числе со сведениями о клиенте, составляющими банковскую тайну; вопросам совершенствования правового регулирования соотношения согласий на обработку и распространение персональных данных в целях защиты прав и законных интересов участников правоотношений [36].

В работе А.А.Гадельшина, М.М.Степанова рассматривается проблема законодательной классификации такого вида данных о людях как cookie-файлы, которые в РФ не относятся к персональным данным, рассматриваются возможности получения таких данных злоумышленниками и вероятностью свободного обмена ими между третьими лицами, проводится сравнительно-правовой анализ законодательства РФ и ЕС в отношении персональных данных [14].

Д.Р. Салихов в работе утверждал, что распространение новой коронавирусной инфекции актуализировало многочисленные вопросы, связанные с защитой персональных данных граждан. Это и обработка традиционных персональных данных в экстраординарных целях (например, для использования «цифровых пропусков»), и применение биометрической идентификации к отдельным категориям лиц, и возможность использования генетической информации [37].

Объект исследования: отношения, связанные с защитой персональных данных в Российской Федерации.

Предмет исследования: правовые нормы, регулирующие отношения в сфере защиты персональных данных в Российской Федерации.

Эмпирическая база включает судебную практику по выбранной теме исследования, данные российского законодательства о нарушениях персональных данных.

Цель исследования: рассмотреть правовое регулирование в сфере защиты персональных данных и выявить актуальные проблемы защиты персональных данных.

Задачи исследования:

- изучить персональные данные как объект правовой охраны;
- представить законодательство в области защиты персональных данных;
- охарактеризовать обработку персональных данных;
- оценить сбор, анализ, хранение персональных данных;
- рассмотреть передачу персональных данных;
- раскрыть проблемы реализации законодательства РФ о защите персональных данных;
- определить проблемы применения юридической ответственности за нарушение законодательства о персональных данных.

Методологическая основа исследования представлена двумя группами методов:

1 группа: Общенаучные методы, которые используются в любом исследовании, политическом, правовом, управленческом т.д.

Правовые проблемы изучаются с помощью научного анализа, который делит правовые явления на мысленно различающиеся элементы, чтобы каждый из них можно было изучить. Однако каждый элемент лишь взаимодействует и соотносится с другими элементами. Это означает, что анализ элементов предполагает также понимание их взаимодействия и взаимосвязей, которые определяют содержание синтеза. Анализ и синтез

неразделимы и являются неотъемлемой частью познавательного процесса, в нашем случае - юридического процесса.

Применение индуктивного метода необходимо для процесса выявления правовых явлений, который начинается с определения экспериментальных (эмпирических) данных, их анализа, систематизации, обобщения и общего вывода. Однако все процедуры, в которых используется метод индукции, должны быть проверены. Это предполагает метод умозаключения, основанный на передаче общих данных, которые считаются правдоподобными, конкретным следствиям, некоторые из которых могут быть проверены на опыте. Индуктивные выводы подтверждаются практическим опытом (экспериментами или реальными юридическими процессами), что означает, что выводы можно считать достоверными и соответствующими действительности.

Методы сравнения, обобщения и классификации являются важными методами исследования. Например, сравнительно-правовое исследование, в котором в полной мере применяются вышеуказанные методы и дается полная картина возникновения, существования, развития и взаимодействия различных правовых систем государств, их интеграции в правовые семьи и особенностей этих процессов, является основой для такого исследования.

2 группа: Частно-научные методы исследования, которые применяются при исследовании правовых процессов и в анализе теории государства и права.

- Сравнительно-правовой метод применяется при сопоставлении одно порядковых юридических понятий, явлений, процессов и выявление между ними сходства и различия, используется при сравнении нормативно-правовых актов и правовых норм.

- Историко-правовой метод, который применяется при изучении истории развития законодательства Российской Федерации в сфере персональных данных.

- Формально-юридический метод представляет собой определенную систему обработки и анализа действующих норм права и существующей

юридической практики, используется для характеристики субъектов в сфере персональных данных.

Применение описанных методов в комплексе способствует изучению объекта исследования с разных сторон в соотношении его элементов между собой, а также предполагает достижение поставленных целей и задач исследования.

Теоретическая основа исследования: Теоретическая основа исследования представлена на основании учений и идей о правовом регулировании персональных данных.

Нормативно-правовая основа исследования: Конституция РФ, Уголовный кодекс Российской Федерации и другие.

Научная новизна исследования определяется разработкой и решением научной задачи, имеющей теоретическую и практическую значимость, и заключается в расширении научных представлений о совершенствовании зашиты персональных данных в Российской Федерации.

Гипотеза: российское законодательство о персональных данных несовершенно, так как отсутствует точный перечень персональных данных; низкие штрафы не снижают количество нарушений в сфере персональных данных.

«Положения на защиту:

– в Федеральном законе от 27.07.2006 № 152-ФЗ (ред. от 24.04.2020) «О персональных данных» необходимо закрепить точный перечень данных, которые относятся к персональным, такие как: 1. Общие персональные данные — те, которые сообщают ключевую информацию о субъекте: Ф.И.О., дата рождения, адрес (регион, город, улица, дом, квартира), паспортные сведения, образование, место работы, уровень дохода и т.д. Если использовать их по отдельности, то нельзя говорить о том, что это сведения, относящиеся к персональным данным, поскольку идентифицировать личность, например, по одной только фамилии невозможно.

В категорию ПДн они попадают в комбинированном варианте, в частности Ф.И.О. в сочетании с местом регистрации. 2. Биометрические — позволяют определить биологические и физиологические отличительные черты конкретного физического лица, которые могут использоваться для установления его личности. Отпечатки пальцев, ДНК человека, радужная оболочка глаз, индивидуальные анатомические особенности. Наиболее востребованы подобные ПДн на таможне и в государственных органах, которые осуществляют выдачу виз и загранпаспортов, а также в современных системах идентификации. 3. Общедоступные персонифицированные данные - это информация о благосостоянии известных людей (представителей власти и шоу-бизнеса, руководителей крупных предприятий и т.д.). Они присутствуют в открытых источниках и могут быть получены без дополнительных разрешений. 4. Обезличенными персональными данными является информация, по которой невозможно определить ее принадлежность к конкретному физическому лицу. 5. Специальные — ПДн, присутствующие в личных делах, медицинских книжках, закрытых реестрах и т.д. Речь идет о философских и политических убеждениях, сексуальных предпочтениях, хронических заболеваниях, расовой и национальной принадлежности, вероисповедании. Чтобы с ними работать, нужно предварительно обеспечить санкционированный доступ, а именно — получить официальное согласие владельца в письменном виде» [5]. Для этого можно взять классификацию персональных данных, которая была разработана учеными-юристами, и закрепить ее в статье 3 вышеуказанного правового акта;

– для устранения причины низких административных штрафов необходимо попытаться увеличить их до таких размеров, чтобы нарушать положение закона было невыгодно. В Кодексе Российской

Федерации об административных правонарушениях нужно закрепить дифференцированный подход к административным штрафам, чем выше оборот юридического лица, тем выше размер наказания, при обороте от 10 млн.руб., штраф должен составлять 500 тыс.руб., при обороте от 100 млн.руб., штраф – 5 млн.руб.

Теоретическая значимость выражается в изучении основных понятий в сфере персональных данных и существующего законодательства в области защиты персональных данных.

Практическая значимость заключается в использовании результатов исследования для совершенствования российского законодательства в сфере персональных данных.

Структура диссертации: введение, основная часть, заключение, список используемой литературы и используемых источников.

1 Общая характеристика персональных данных

1.1 Персональные данные как объект правовой охраны

«Защита персональных данных является одним из наиболее актуальных вопросов для российских компаний и организаций - как коммерческих, так и государственных. В Российской Федерации защита персональных данных регулируется на законодательном уровне рядом федеральных законов и нормативных актов. Например, в 2006 году был принят Федеральный закон № 152-ФЗ «О персональных данных», направленный на защиту персональных данных, обрабатываемых государственными и коммерческими организациями. С момента принятия этого закона прошло более десяти лет, но защита персональных данных, обрабатываемых или хранящихся в информационных системах, остается одной из главных задач по его реализации, как с точки зрения разработки нормативно-правовой базы, так и организации ее внедрения» [33].

На сегодняшний день существует множество трудов отечественных и зарубежных ученых, монографии, материалов и периодических научных изданий по исследуемому вопросу обеспечения безопасности персональных данных, которые можно найти как в интернет-ресурсах, так и выпускаемых печатных журналах и бюллетенях. В данной работе хотелось бы остановиться на тех, которые наиболее полно отражают проблематику в рамках ее организации на государственном предприятии, поэтому остановимся на некоторых. Так, например, в «статье И.С. Козина [24] предложен метод определения опасности угрозы, позволяющий подготовить перечень опасных угроз с учетом степени важности объекта защиты, в статье В.В. Соловьева [38; с. 39-44] предложен способ организации схемы защиты информационной системы персональных данных. Концептуальны также труды, посвященные разработке методик маскирования персональных данных в базе данных [22].

Вместе с тем в рамках данной проблематики должны учитываться результаты работ таких авторов, как А.В. Минбалеев из Южно-Уральского государственного университета (г. Челябинск)» [32, с. 4-9], раскрывающих также проблематику защиты персональных данных.

Все персональные данные, которые существуют в Российской Федерации, подразделяются на следующие виды (научное деление):

- общие персональные данные. К ним можно отнести: Ф.И.О. человека, место регистрации и жительства, номер мобильного телефона, адрес электронной почты. Такие данные в большинстве своем известны не только их обладателю, но и каким-либо другим гражданам;
- специальные персональные данные. К ним относятся политические взгляды, религиозная принадлежность, данные о состоянии здоровья, подробности о судимостях человека. Этот вид персональных данных отличается от общего вида тем, что они обычно находятся в закрытом доступе. Узнать их можно только в том случае, если их обладатель сам захочет их рассказать;
- биометрические персональные данные. К ним относятся отпечатки пальцев, группа крови, физиологические параметры человека. Такие данные становятся персональными только в том случае, если используются для идентификации личности. Например, если у какого-либо юридического лица на входе стоит датчик распознавания отпечатков пальцев, то тогда это юридическое лицо работает с персональными данными, так как именно по ним вы определяете личность человека;
- иные виды персональных данных. В эту категорию персональных данных входят все те данные, которые не попадают во все вышеперечисленные, например, информация о заработной плате, о датах отпуска, о стаже работы [1].

Российское законодательство охраняет все вышеперечисленные данные от неправомерного использования и распространения. Однако, несмотря на

законодательную защиту и богатую судебную практику, такие данные граждан Российской Федерации постоянно утекают в свободный доступ и достаточно часто становятся предметом купли-продажи. В соответствии с материалами исследования международной IT-организации «Лаборатория Касперского» в сети «Интернет» цифровой профиль человека, который включает в себя Ф.И.О., данные об аккаунтах в социальных сетях, данные об удаленном доступе к компьютеру, реквизиты банковских карт, которыми платили в сети «Интернет», стоит порядка $50-75. Наличие этих данных позволяет совершать некоторые противоправные деяния лицам, которые эти данные приобретают, например, оформить кредит в банке по чужому паспорту [8].

В наше время число пользователей Интернета значительно возросло. Люди стали практически зависимы от общения и Интернета. Информация стала не только основным ресурсом, но и величайшим оружием общества. Почти у каждого есть учетная запись электронной почты, и не одна, а несколько. И не все знают о последствиях взлома. Угроза потери ваших самых конфиденциальных данных, например, паспортных данных. И риск, которому мы подвергаемся, когда привязываем свои банковские карты при совершении покупок на веб-сайтах[4]. Это привело к значительному увеличению ресурсов, доступных хакерам, которые несанкционированно пользуются имеющейся у них информацией о сообществе путем удаленного доступа к базам данных. Быстрая обработка персональных данных представляет собой реальную угрозу законным интересам и правам физических лиц [2]. Проблема защиты личности от несанкционированного сбора персональных данных, злоупотреблений, возможных при сборе, обработке и распространении информации персонального характера на сегодняшний момент является достаточно актуальной для нашего государства [50].

Так что же представляет понятие «персональные данные» и чем оно регламентировано. В каждом государстве имеется своя законодательная база, определяющая регламент защиты персональных данных. В России в

настоящее время вопросу обеспечения надежной защиты уделяется особенное внимание [3]. Согласно части первой статьи 24 Конституции России сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются, что по сути является важнейшим личным правом. Однако реализация этого права гражданами не была предусмотрена. В части 1 ст. 24 Конституции России присутствует элементы информации о частной жизни. Понятие «частная жизнь» в законодательстве четко не определено. В соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ (ред. от 30.12.2020) "О персональных данных" определено понятие персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу [33]. Очевидно, что действия, приводящие к утрате информации о частной жизни человека без его согласия, нарушают основной закон страны - Конституцию Российской Федерации [26].

«Федеральный закон №152-ФЗ «О персональных данных» был принят в 2006 году и затрагивает защиту персональных данных, обрабатываемых в государственных и коммерческих организациях. Со времени принятия данного закона прошло больше десяти лет, но до сих пор защита персональных данных, обрабатываемых или содержащихся в информационной системе, является одной из актуальных прикладных задач как в плане усовершенствования нормативной базы, так и организации его реализации» [33].

Закон о персональных данных устанавливает минимальные требования к обработке биометрических персональных данных с целью проверки личности субъекта данных. Однако вопрос сообщения о таких утечках данных остается открытым и представляет серьезную угрозу безопасности граждан [5].

Поэтому одной из важнейших задач в области информационной безопасности в России является обращение к законодательной базе по защите конфиденциальных данных физических лиц и совершенствование этой

законодательной базы.

В последнее время количество массовых утечек персональных данных в России значительно возросло[37].

Понятно, что утечка персональных данных может иметь как объективные технические, так и субъективные причины, например, халатность сотрудников или мотивы жадности до денег. Персональные данные, попавшие в руки злоумышленников, могут быть использованы в преступных целях (займы, незаконные сделки с недвижимостью, денежные переводы и т.д.) [9].

Для организации защиты конфиденциальных данных необходима лицензия ФСТЭК на защиту персональных данных. Однако профессионалов, обладающих необходимой квалификацией, опытом и знаниями, очень мало. Кроме того, необходимы специальные помещения и соответствующее оборудование, которые небольшие организации не могут себе позволить [17].

Не все работодатели имеют средства на переподготовку персонала, приобретение дополнительного оборудования и получение необходимых лицензий для обеспечения безопасности персональных данных, поскольку стоимость приобретения технических средств защиты персональных данных и обслуживания системы во много раз превышает размер выплачиваемых штрафов [6].

К сожалению, приходится признать, что новые технологии находятся в прямом противоречии с существующими принципами законодательной базы, что свидетельствует о сомнительной эффективности законодательства о защите персональных данных. В своем нынешнем виде законодательство о защите персональных данных все больше отстает от реалий современных технологий и действительно нуждается в коренном изменении.

1.2 Законодательство в области защиты персональных данных

«Нормативно-правовая основа решения данной актуальной и прикладной проблематики также значительна и фундаментальна, ниже перечислим самые основные документальные акты, включающие и федеральную законодательную базу, и ведомственную» [37]:

- Федеральный Закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» [33];
- Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [35].
- Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- 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 персональных данных при их обработке в информационных системах персональных данных”;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. (ФСТЭК России,2008 г.);
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (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».

Обработкой персональных данных сегодня занимаются специалисты по безопасности в каждой организации. Трудно найти организацию, которая не управляет персональными данными своих сотрудников или партнеров. Каждый гражданин, в свою очередь, устанавливает отношения с различными физическими и юридическими лицами, что приводит к созданию регистров (баз данных) персональных данных. В то же время службам безопасности трудно применять существующие правила к этой сфере общественных отношений.

Когда персональные данные обрабатываются в любой базе данных, соблюдение, применение и исполнение правил является необходимым условием. Одна из основных реформ коснулась регулирования Федерального закона 152-ФЗ[33], который добавил требование о хранении персональных данных на серверах с 1 января 2021 года. «При сборе данных, в том числе через информационно-телекоммуникационные системы, оператор обязан обеспечить регистрацию, систематизацию, составление, хранение, корректировку (обновление, изменение) данных о гражданах Российской Федерации посредством баз данных, расположенных на территории Российской Федерации» [12].

Нередко случаются ситуации, когда в силу разных причин персональные данные того или иного гражданина становятся общедоступными, происходит так называемая утечка персональных данных человека. Об этом мы в настоящее время слышим достаточно часто. Так, например, в ноябре 2019 года произошла утечка данных клиентов «Альфа-банка». В Сети на продажу были выставлены данные лиц, заключавших кредитные договоры и договоры страхования. В договорах содержатся Ф.И.О., номер мобильного телефона,

паспортные данные, адрес регистрации, сумма кредитного лимита или оформленной страховки, предмет страхования, а также дата заключения договора [1]. Гражданин, передавая свои личные данные какому-либо юридическому лицу, индивидуальному предпринимателю или публично-правовому образованию, надеется на то, что их получатель защитит эти данные и никому не передаст.

Для начала необходимо поговорить о том, что такое персональные данные и как они в современной Российской Федерации охраняются.

В соответствии с пунктом первым части первой статьи 3 Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 24.04.2020) [33] «О персональных данных» под персональными данными следует понимать любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Нормативной основой для защиты персональных данных человека выступают положения следующих нормативных правовых актов:

- Конституции Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). Данный правовой акт в статье 24 закрепляет положение о том, что «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются». Это конституционное положение получает свое развитие в двух нижеуказанных правовых актах, которые посвящены охране информации о частной жизни лица [26];
- Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ. Данный правовой акт направлен на «обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну» [33];
- Кодифицированных правовых актов (Уголовный кодекс Российской Федерации (статья 137, 272 УК РФ) [40], Кодекс Российской

Федерации об административных правонарушениях (статья 13.11 КоАП РФ), Гражданский кодекс Российской Федерации (статья 152.2 ГК РФ)), которые предусматривают различные виды ответственности за нарушение законодательства о персональных данных;

- Указа Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера». Данный правовой акт в своем содержании содержит точный перечень сведений, которые относятся к сведениям конфиденциального характера (коммерческая тайна, служебная тайна и т.д.) [34];
- Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Данный правовой акт устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных[35].

Попробуем теперь разобраться с тем, почему возникают ситуации утечки персональных данных в сеть «Интернет» и какие проблемы защиты таких данных в сети «Интернет» существуют.

Первой проблемой защиты персональных данных в сети «Интернет» является проблема их непосредственной утечки в эту самую Сеть. Она возникает в силу следующих разноплановых причин.

В Российской Федерации положения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [36] содержат общие формулировки, которые могут трактоваться по-разному. Позиции Роскомнадзора и суда по одному и тому же вопросу могут различаться. Также в рамках правоприменительной практики существуют разные решения судов по одному и тому же спорному вопросу. Примером такой ситуации является вопрос о том, является ли номер мобильного телефона персональными данными. Согласно закону, номер мобильного телефона может считаться персональными данными, но, по мнению Роскомнадзора, это не так, поскольку

номер мобильного телефона - это не характеристика человека, а характеристика технического устройства и, следовательно, не персональные данные. Судебная практика также неясна в этом вопросе. Вот два примера. В 2019 году житель Белгорода обратился в суд с жалобой на ООО «Яндекс Справочник» за публикацию его номера телефона в Интернете. Роскомнадзор не нашел нарушений, так как номер телефона был опубликован без указания владельца. Суд согласился с государственным органом в том, что номер телефона не является персональными данными, поскольку не поддается персональной идентификации, и не согласился с жителем Белгорода. Московский суд по аналогичному делу решил иначе. Коллекторское агентство позвонило гражданину без его согласия. У коллекторского агентства не было никакой информации об этом человеке, кроме номера его телефона. Суд постановил, что такая обработка персональных данных, т.е. номера телефона, коллекторским агентством была нарушением Закона о персональных данных. Также в качестве еще одного примера вышеуказанной ситуации можно привести разные трактовки того, являются ли фотографии, которые применяются в системе СКУД, биометрическими персональными данными или нет [1]. Вследствие этого из-за того, что нет четкого понимания законодательных положений, многие юридические лица могут надлежащим образом не охранять номера телефонов или фотографии лиц, так как они не считают их персональными данными, что приводит к их утечке и распространению в сети «Интернет».

В Российской Федерации существует достаточно низкий размер административных штрафов для юридических лиц, которые в процессе своей деятельности допускают нарушение законодательства о защите персональных данных.

Размер таких штрафов находится в диапазоне от 15 000 до 75 000 рублей. Только мелкому юридическому лицу может быть трудно заплатить такой административный штраф [37]. Крупные юридические лица, продающие персональные данные, могут легко заплатить такой штраф. Для них это

«издержки производства».

У некоторых юридических лиц утечка персональных данных происходит из-за человеческого фактора. Он может проявляться в разных аспектах: сотрудники слабо понимают требования положений российского законодательства о персональных данных, сотрудники халатно относятся к исполнению своих должностных обязанностей, сотрудники выполняют требования закона «для галочки», а не по факту, сотрудники организаций сами продают персональные данные своих работников или клиентов каким-либо третьим лицам.

Второй проблемой защиты персональных данных в сети «Интернет» является проблема того, что российским гражданам, которым был причинен какой-либо ущерб утечкой персональных данных, почти нереально добиться компенсации за это в судебном порядке от частных юридических лиц или государственных органов, допустивших утечку персональных данных. Такое положение вещей объясняется тем, что в случае, если какой-либо из подобных процессов, увенчавшийся успехом, может привести к цепной реакции, когда каждый пользователь, сталкивавшийся с утечкой данных, обратится в суд за компенсацией. Учитывая низкий уровень защиты персональных данных в России, это может обернуться разорением юридических лиц.

Следом иски можно вчинить и государственным органам, которые, несмотря на требования закона, весьма халатно относятся к защите персональных данных россиян.

Подобные иски могут очень больно ударить по бюджету страны [36]. Вследствие этого в российских судах рассмотрение дел такой категории происходит достаточно долго и нередко заканчивается присуждением минимальной компенсации лицу, чьи персональные данные были использованы неправомерно. Однако эта компенсация не всегда сможет покрыть те убытки, которые были причинены утечкой персональных данных.

Для решения первой проблемы, на взгляд автора данной работы, необходимо бороться со всеми причинами, которые порождают утечку

персональных данных в сеть «Интернет». Во-первых, нужно привести в порядок законодательство о персональных данных. В Федеральном законе от 27.07.2006 № 152-ФЗ (ред. от 24.04.2020) «О персональных данных» [33] необходимо закрепить точный перечень данных, которые относятся к персональным. Для этого можно взять какую-либо классификацию персональных данных, которая была разработана учеными-юристами, и закрепить ее в статье 3 вышеуказанного правового акта. Например, статья 3 Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 24.04.2020) «О персональных данных» может звучать так: «Персональные данные – информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу. К персональным данным относится следующая информация: Ф.И.О. человека, место регистрации и жительства, номер мобильного телефона, адрес электронной почты. Такие данные в большинстве своем известны не только их обладателю, но и каким-либо другим гражданам, политические взгляды, религиозная принадлежность, данные о состоянии здоровья, подробности о судимостях человека, а также иная информация, признанная таковой судом, в рамках рассмотрения и разрешения дела».

Для устранения причины низких административных штрафов необходимо попытаться увеличить их до таких размеров, чтобы нарушать положение закона было невыгодно. В Кодексе Российской Федерации об административных правонарушениях нужно закрепить дифференцированный подход к административным штрафам, чем выше оборот юридического лица, тем выше размер наказания.

Решить третью причину может только сама организация, так как, кого нанимать на работу решает организация, а не государство. Вследствие этого устранение этой причины необходимо возложить на юридические лица, а не на государство.

Для решения второй проблемы защиты персональных данных в сети «Интернет» необходимо донести до судов Российской Федерации, что права и

свободы человека являются приоритетом в деятельности судов. Суды не должны заботиться об экономическом состоянии юридических лиц или государственных органов, которые допустили нарушение законодательства о персональных данных, которое привело к причинению вреда гражданину. Суд обязан рассмотреть и разрешить дело справедливо и не думать о том, какие последствия будут для «виновника» утечки персональных данных в случае вынесения решения суда не в его пользу. Сделать такое донесение можно посредством издания Верховным Судом Российской Федерации специального пленума, в котором бы были разъяснения, как следует применять положения всего комплекса российского законодательства о защите персональных данных.

В России, органом, осуществляющим функции по контролю и надзору в сфере средств массовой информации, функции по контролю и надзору за соответствием обработки персональных данных, по защите прав субъектов персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

«В Соединенных Штатах Америки, в отличии от большинства ведущих европейских стран до настоящего времени отсутствует конкретный единый орган, который бы занимался вопросом защиты персональных данных. Отсутствует общее законодательство о персональных данных. В США сложилась собственная практика защиты конфиденциальной информации, которая основана на наличие закона о защите частной жизни. Существенными нормативными документами являются Privacy Act и Privacy Protection Act, которые регламентируют деятельность органов государственной власти при обработке персональных данных граждан. Каждый штат принимает свой закон, обязывающий компании сообщать о любых утечках информации. Отсутствие в США единого законодательства в данной сфере затрудняет деятельность по обеспечению защиты персональных данных. Следует отметить, что в США постоянно проводят обучение сотрудников нормам работы с персональными данными» [11].

«В Японии 1 апреля 2005 г. вступил в силу Закон "О защите персональной информации". Законодательство на протяжении нескольких лет неоднократно менялось, приняты нормативно правовые документы, регулирующие не только деятельность телерадиокомпаний, но и регламент получения информации от государственных и местных органов власти, в целом определяющие дальнейшее развитие информационного общества и порядок защиты персональной информации. Органы власти утвердили в Японии основательную законодательную базу по осуществлению мер реализации свободы информации, что явилось существенным прорывом в формировании законодательной базы о защите персональных данных граждан в Японии» [15].

Германия, несомненно, является ведущим европейским законодателем в области защиты персональных данных. Федеральное законодательство Германии о защите данных основано на принципе независимости данных. Физические лица имеют право самостоятельно обрабатывать свои личные данные и решать, какой объем информации они должны предоставить по запросу властей. Федеральная комиссия по защите данных является надзорным органом, ответственным за выполнение этого закона на федеральном уровне. В каждой земле Германии действуют свои региональные законы. Согласно немецкому законодательству, персональные данные, которые не нужно хранить или которые не следует хранить, должны быть уничтожены [53].

В Китае практически отсутствует правовая база для внедрения режима защиты персональных данных, формулировки «руководящие принципы» страны очень расплывчаты и неоднозначны, отсутствует понятие «персональные данные». Существующие системы контролируют деятельность людей во всех сферах жизни общества. Однако для внедрения этих систем нет правовой основы, и не разработано законодательство, регулирующее их работу. В октябре 2020 года проект закона о защите персональных данных был представлен в Постоянный комитет Всекитайского

собрания народных представителей, что свидетельствует о том, что Китай переходит к более строгому контролю за защитой персональных данных [12].

Существуют и другие общие организационные и технические проблемы. Таким образом, можно сказать о том, что персональные данные – это любые сведения, относящиеся к прямо или косвенно определённому или определяемому физическому лицу, которые предоставляются другому лицу. Правовое регулирование охраны таких данных осуществляется положениями Конституции Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ [33], а также различными подзаконными актами. Однако, несмотря на такой большой объем правовой защиты, сейчас существуют две проблемы защиты персональных данных в интернете. Первая проблема - это утечка этих данных в Сеть, а вторая - это почти нереальная возможность добиться компенсации за вред, который был причинен такой утечкой. Решение этих двух проблем должно заключаться в устранении причин, которые их вызывают. Вследствие их устранения в Российской Федерации должен резко снизиться процент утечки персональных данных в сеть «Интернет».

2 Обработка персональных данных

2.1 Характеристика обработки персональных данных

По российским законам любая компания, работающая с личными данными своих пользователей в России, становится оператором ПДн, хочет она того или нет. Это накладывает на нее ряд формальных и процедурных обязательств, которые не каждый бизнес может или хочет нести самостоятельно.

Как показывает практика – совершенно правильно не хочет, потому что эта область знаний еще настолько новая и не обкатанная на практике, что сложности и вопросы возникают даже у профессионалов.

Например, утечка информации о персональных данных лица - это на сегодня самая распространенная проблема. Персональные данные, такие как номера телефонов, домашние адреса, данные персональных платежных карт, банковские счета и другая информация оказываются известны третьим лицам, которые их используют в корыстных целях, совершая порой умышленные уголовные преступления. [29]

В трудовой сфере также часто происходят нарушения в сфере работы с персональными данными. Так без согласия работника или лица-претендента на работу работодатель не имеет право обрабатывать ПД работника, даже если они размещены на сайте. Это нарушение закона и судебная практика подтверждает это.[4]

Также судами часто рассматриваются дела о подделке подписей, оформлении кредитов и займом, т.е. использование паспортных данных лицами не имеющие отношения к персональным данным владельца персональных данных. Поэтому необходимость пересмотра отдельных положений законодательства о защите персональных данных требует

действительность и судебная практика. Анализируя судебную практику, хотелось бы отметить, что пресекая распространение персональных данных, суды защищают интересы граждан, и тем самым оберегают тайну их личной жизни.

1 марта 2021 года вступили в силу изменения в Федеральный закон № 152-ФЗ «О персональных данных». Отдельные положения этих изменений согласно, приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24 февраля 2021 года № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения» вступили в силу с 1 июля 2021 года.

Внесенные изменения определяют совершенно новое понятие «персональные данные, разрешенные для распространения». Данный термин заменяет понятие «общедоступные персональные данные». Также определен порядок удаления персональных данных из общего пользования. Теперь субъект персональных данных имеет право выбирать, какие ПД, в каких случаях, на каких условиях, в каких целях, и на какой срок он дает разрешение, например, оператору, имеющему к ним доступ, обрабатывать и распространять их третьим лицам. Лицо, желающее использовать данные субъекта персональных данных обязательно должен получить лично у субъекта ПД согласие об использовании или распространении персональных данных на бумажном носителе с подписью лица-субъекта персональных данных или через информационную систему Роскомнадзора. Но не совсем понятно, где должны быть опубликованы данные сведения. Кроме всего, в согласие на распространение ПД должен быть оговорен срок действия и сведения, на которые установлен запрет на использование. В тех случаях, когда субъект персональных данных прямо не указал, что оператор не имеет права обрабатывать его персональные данные, но и не предоставил согласие, то оператор не имеет право передать их неограниченному кругу лиц. Но в любом случае оператор обязан опубликовать информацию о таких условиях

или запретах. На это действие законодатель определил 3 рабочих дня с момента получения согласия или запрета.

Кроме всего за субъектом персональных данных остается право в любой момент отозвать свое разрешение на обработку информации о нем. В этом случае он должен будет оформить письменное заявление и направить его оператору.

Исключение составляют лишь сведения, на которые не получено согласие от субъекта ПД на обработку, если это представляет угрозу государству и обществу. Персональные данные в таких случаях могут быть обработаны, не взирая на запреты. Установления данной меры необходимо чтобы иметь возможность пресечь правонарушения или иные действия, влекущие опасность для граждан и общества.

Выше перечисленные правила обработки и распространения персональных данных распространяются и на трудовые отношения. Но в отдельных случаях получение дополнительного согласия на передачу ПД в трудовых отношениях не распространяется на передачу данных, например, в налоговые органы, в пенсионный фонд, в финансовый отдел работодателя.

Судебная практика показывает, что, не смотря на увеличение штрафных санкций, запреты не соблюдаются, а правила очень часто нарушаются. Мошенники в сфере персональных данных часто идут на шаг вперед. Поэтому в век информационных технологий и стремительного развития системы искусственного интеллекта способы защиты персональных данных должны постоянно усовершенствоваться и обновляться.

В современных условиях внедрения цифровых платформ, большой объём информации, в том числе и персональные данные, находятся в виртуальной форме и являются элементами электронного документооборота. В таких обстоятельствах повышается актуальность безопасности информации, которая находится в обороте[7].

Развитие информационных технологий послужило началом изменений способов и целей распространения личных данных человека. В случае

раскрытия личной информации человеку может быть причинен как материальный, так и моральный вред. В результате появилась необходимость нормативного правового регулирования порядка получения, хранения, обработки, передачи и защиты личной информации. Действующее законодательство не вполне соответствует требованиям современности: в системе национального права отсутствует понятие личной информации, понятие персональных данных не конкретизировано[14].

Российские граждане (как и все остальные) все активнее используют цифровые технологии. Мобильный телефон уже давно превратился в портативный компьютер, позволяющий получить доступ к широкому спектру программного обеспечения и приложений, доступ к серверам различных служб (в том числе государственных и муниципальных) и облегчающий общение как с отдельными людьми, так и в более широкой социальной среде (через социальные сети и каналы) [16].

«Ежедневно каждый из нас порождает огромный объем информации, включающий в себя различные персональные данные, которые отправляются во внешнее пространство. Конституция России [26] установила общий режим защиты таких данных, предусматривая в ст. 23 право на неприкосновенность частной жизни, а в ст. 24 - запрет на сбор информации о частной жизни лица без его согласия. Предусматриваются отраслевые гарантии, закрепленные, в частности, в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [33]. С учетом действия значительных информационных массивов и в связи с участившимися кибератаками был принят Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». В приведенных законах вводятся определенные режимы для того или иного вида информации, затрагивающей частную жизнь гражданина. Предусматривается дифференциация информации по категориям допуска. Ко многим процедурам каждый гражданин России уже привык: как,

например, согласие на обработку персональных данных при их предоставлении в какую-то организацию. В то же время быстрое технологическое развитие, усложнение обмена данными в цифровом пространстве, создание новых программ такого обмена показывают, что обработка сведений о гражданах может оказать влияние на объем прав и обязанностей, устанавливая запреты (или ограничения) в рамках осуществления какой-то деятельности. Зависимость реализации многих прав от технологического аспекта обработки информации обусловливает повышенную актуальность нового формата метаданных» [28].

«Несколько слов о понятии метаданных и изменении их роли в цифровом обществе в вопросах реализации гражданином своих прав и свобод. Общее определение метаданных заключается в том, что это данные о других данных. Национальный стандарт Российской Федерации «Система стандартов по информации, библиотечному и издательскому делу. Набор элементов метаданных “Дублинское ядро”» (ГОСТ Р 7.0.10-2010) представляет следующее определение: «Метаданные (metadata) - структурированные данные, характеризующие информационный ресурс для целей его идентификации, поиска и управления им». В другом Национальном стандарте «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения» (утвержден Приказом Росстандарта от 17 октября 2013 г. № 1185-ст) понятие метаданных представлено несколько иначе: «Данные, описывающие контекст, содержание, структуру документов, обеспечивающие управление документами в информационной системе»»[25].

«Национальный стандарт «Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы» (утвержден Приказом Росстандарта от 26 марта 2019 г. № 101-ст) предусматривает понятие «метаданные документов (metadata for records)»: структурированная или полуструктурированная информация, которая позволяет создавать,

управлять и использовать документы в разное время и в различных областях деятельности. Кстати, заполнение указанных сведений закрепляется Приказом Росархива от 24 декабря 2020 г. № 199 «Об утверждении Методических рекомендаций по разработке инструкций по делопроизводству в государственных органах, органах местного самоуправления»» [34].

«Есть и краткие формулы понятий. Так, в соответствии со ст. 33 Закона Российской Федерации от 20 августа 1993 г. № 5663-1 «О космической деятельности» метаданные включают в себя информацию об основных характеристиках данных и копий данных. Правила организации хранения, комплектования, учета и использования научно-технической документации в органах государственной власти, органах местного самоуправления, государственных и муниципальных организациях (утверждены Приказом Росархива от 9 декабря 2020 г. № 155) вообще подразумевают под метаданными лишь реквизиты документа. Ряд документов Роскосмоса понимают под метаданными лишь копии данных (например, Приказ Госкорпорации «Роскосмос» от 16 июля 2019 г. № 215, совместный Приказ Госкорпорации «Роскосмос» № 257, Росгидромета № 388 от 15 августа 2019 г. и др.), что в целом соответствует ограничительному видению Закона «О космической деятельности»» [35].

Приказ Минобрнауки РФ от 31 января 2008 г. № 34 «О национальной системе мониторинга исследований и разработок в сфере нанотехнологий» понимает под метаданными формализованное описание информации.

Для примера: автор научной статьи предоставляет информацию о себе, когда публикует статью. Итак, на практике на сайте любого журнала есть много информации, которую должен предоставить автор, принимая решение о публикации своей научной работы: фамилия, имя, отчество, адрес электронной почты, место работы, должность, степень и ученое звание. Запрашиваемая информация может включать и другую информацию (например, реквизиты банковского счета в случае выплаты роялти [27]). В законодательстве есть некоторая ясность: на такие метаданные

распространяется режим персональных данных, требующий согласия владельца. При этом каждый автор представляет статью (в большинстве случаев) в электронном формате. Если материал написан в Microsoft Word, каждый файл будет содержать собственные метаданные, такие как комментарии, отслеживаемые изменения, информация о версии, свойства документа (включая информацию об общем резюме, статистике, редактируемых вкладках в диалоге свойств документа), адрес электронной почты, имя, имя пользователя, некоторые скрытые элементы форматирования и т.д. Этот список отнюдь не исчерпывает информацию, которую вы можете получить при углублении в результирующий файл[31].

При отправке цифровой фотографии метаданные также могут включать множество информации, связанной с изображением, например, дату съемки, имя владельца камеры, модель камеры и настройки (чувствительность, фокусное расстояние и т.д.). Если фотография была сделана с помощью мобильного телефона, в зависимости от встроенных эффектов, метаданные могут включать геолокацию и другую связанную информацию из указанных приложений[23].

Если бы мы сейчас подробно описали метаданные, связанные с любой записью в цифровом пространстве, список метаданных мог бы занять не одну страницу. Это объясняет, что конфиденциальность управления метаданными подчиняется конституционным требованиям по защите права на неприкосновенность частной жизни[19].

Особенности правового режима метаданных заключаются в ряде аспектов, заметно отличающих их от персональных данных:

- метаданные в цифровом пространстве сопровождают сведения в автоматическом режиме, без ведома обладателя основной информации;
- удаление метаданных в большинстве случаев - сложная процедура, требующая специальных навыков, что исключает ее использование каждым в стандартном режиме;

- автоматическая обработка метаданных зачастую происходит вне ведома обладателя основной информации, в силу установленного программного обеспечения.
- на порядок обработки метаданных во многих случаях не распространяется режим защиты, установленный для персональных данных;
- анализ метаданных с помощью искусственного интеллекта и специальных программ позволяет получить значительный объем конфиденциальной информации;
- сбор метаданных происходит непрерывно и постоянно, что многими коммерческими компаниями объясняется потребительскими целями улучшения качества оказываемых услуг;
- в условиях борьбы с террористической угрозой и преступностью правоохранительные органы настаивают на облегченном порядке доступа к метаданным.

«Размещение информации в сети Интернет также связано с целью ее максимального распространения и включения в различные поисковые системы для ее быстрого и четкого отражения. Для этого используются связанные элементы, которые формируют собой как раз метаданные. Представление открытых данных основано на базовом стандарте RDF (Resource Description Framework), разработанном консорциумом Всемирной паутины (World Wide Web Consortium - W3C). Не вдаваясь в подробности, обозначим, что указанный стандарт позволяет максимально быстро находить необходимую информацию благодаря предложенным техническим решениям. К тому же RDF позволяет объединять распределенные источники данных. Именно поэтому данный стандарт (как и другие, например RDFa (Resource Description Framework in attributes), Microdata, RFC2413) предлагается в Методических рекомендациях по публикации открытых данных государственными органами и органами местного самоуправления, а также технических требованиях к публикации открытых данных (Версия 3.0,

утверждена протоколом заседания Правительственной комиссии по координации деятельности открытого правительства от 29 мая 2014 г. № 4)» [16].

«В то же время благодаря этому же стандарту при обработке файла возможно получение внешне скрытой информации, но несущей в себе ключевую нагрузку. Именно благодаря метаданным в настоящее время возможно раскрытие киберпреступлений, как раз оставляющих в указанном формате электронные «следы». Анализ метаданных позволяет раскрыть и различные правонарушения, как, например, сговор при участии в аукционе, что было выявлено в ходе рассмотрения антимонопольного законодательства при организации аукциона на поставку детского питания в Пермском крае (Решение Пермского УФАС России от 14 июля 2020 г. по делу № 059/01/11-1231/2019 - метаданные заявок от различных организаций указывали на их формирование в одном юридическом лице). При этом в юридической литературе подчеркивается, что использование метаданных в правоприменительной практике не имеет единообразия (в частности, в трактовке переписки в социальных сетях и иные аспекты «цифровой жизни» граждан). Более того, процессуальное законодательство не ввело специальный термин «электронное доказательство», рассматривая электронный документ как единое целое, приравняв его к письменным доказательствам (Федеральный закон от 23 июня 2016 г. № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти»)» [18]. А.А. Грибанов, анализируя нововведение, подчеркивает: «Отнесение электронных документов к письменным доказательствам основано на том, что сведения, которые содержатся в электронных документах, представляют собой человеческую мысль (понятия, суждения, умозаключения и т.д.) о существующей действительности. В тех случаях, когда документ представляет собой фотоснимок либо иное отражение реальной действительности, которое не содержит мысль, его никак нельзя признать

письменным доказательством. Такой документ следует исследовать как вещественное доказательство. Сегодня в доказательственной деятельности преимуществом обладает письменная форма, что свидетельствует о признании законодателем самодостаточности такой формы, в том числе и для электронных доказательств» [16]. Автор отстаивает взвешенный подход о недопустимости безграничной технологизации права.

«Активно внедряется технология блокчейн, которая «основывается на том, что у каждого пользователя базы данных, основанной на блокчейне, хранится ее полная копия (правило распределенного реестра)» [36]. Происходит децентрализация данных, но с их синхронизацией, что минимизирует риски уничтожения информации, а также несанкционированного манипулирования и мошеннических действий. Все это выстраивает новые перспективы перед новой технологией, активно внедряемой в различные сферы деятельности [4]. Так, набирают популярность смарт-контракты, которые Д.Р. Салихов именует «умными контрактами», преобразующими основы договорного права [37]. В технологии блокчейн метаданные приобретают ключевое значение» [41].

«Появление метаданных к электронным файлам ставит на новый уровень необходимость предотвращения киберугроз, несанкционированного доступа. Следует учитывать, что требования специальной защиты связано даже с такой ситуацией, когда метаданные не позволяют устанавливать личность, поскольку сбор и обработка информации может касаться систематизации иных данных, имеющих косвенное отношение к персональным, но позволяющим формулировать определенные выводы (например, о нуждаемости в лекарственных средствах и медицинском оборудовании, предпочтениях потребителей, скоплении граждан на территории и др.). Именно поэтому сейчас наблюдается особый интерес к метаданным со стороны хакеров, мошенников и иных киберпреступников. К тому же систематизация метаданных создает основу для социальной инженерии и управления массами. Актуальность приобретает такая

профессия, как аналитик данных. Таким образом, защитный механизм должен включать в себя как технический, так и правовой моменты» [10].

«Правовой режим защиты метаданных находится в «серой зоне». Это обусловлено как минимум несколькими факторами: 1) сложностью самого регулирования технических процессов; 2) отсутствием заинтересованности в регулировании со стороны разработчиков программных продуктов; 3) возможностью получения информации правоохранительными органами в упрощенном порядке. Обращение к российскому законодательству показывает, что сам термин «метаданные» в нем используется. Например, ст. 14 Федерального закона от 30 декабря 2015 г. № 431-ФЗ «О геодезии, картографии и пространственных данных и о внесении изменений в отдельные законодательные акты Российской Федерации» содержит указание на пространственные метаданные. Однако изучение иных документов показывает, что законодатель не видит большой разницы между пространственными данными и пространственными метаданными (и в том и в другом случае речь идет об информации, изложенной в виде файлов в формате XML, созданных с использованием XML-схемы)» [16].

«Выше приводились примеры закрепления понятия «метаданные» в Национальных стандартах (кстати, даже в стандартах нет единства терминологии, причем в общих чертах и при описании сходных категорий), но они не пригодны в установлении методов и форм защиты неприкосновенности частной жизни [21]. В данном аспекте законодатель должен определить различные уровни метаданных, распределяя их по значимости как для самого лица, так и для определения формы защиты. Анализируя зарубежный опыт, можно увидеть разносторонний подход к защите прав личности через введение особого правового режима метаданных. В рамках Европейского Союза действует Общий регламент защиты персональных данных (General Data Protection Regulation; GDPR [44]), действующий с 2016 г., распространяющий свое действие на некоторые метаданные - в частности, на геолокацию. Аналогичный подход используется в США. Например, в

Принципах таргетированной рекламы Федеральной торговой комиссии США точное местоположение лица - это так называемые чувствительные персональные данные» [43].

«В Российской Федерации геолокация (возьмем только один пример метаданных) вряд ли может быть отнесена к понятию персональных данных, которое предусматривается ст. 3 Федерального закона «О персональных данных» следующим образом: «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)». С одной стороны, геолокация указывает на место нахождения лица, с другой - место нахождения мобильного устройства (которое в момент определения может находиться с каким-то иным лицом, не ассоциированным с мобильным устройством)» [42].

«Ряд авторов подчеркивают возможность включения метаданных в понятие персональных данных за счет специальной оговорки в Федеральном законе «относящаяся прямо или косвенно», внесенной в 2011 г. (Федеральный закон от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон “О персональных данных”») [33]. Иными словами, закон создал некий потенциал для возможного расширения понятия и распространения его на дополнительные инструменты, не предусматривая при этом (даже примерного) перечня составных элементов. Л. К. Терещенко посчитала, что это привело к разночтениям в судебной практике [39]. Д. Р. Салихов, наоборот, подчеркнул, что такой подход связан с приведением российского закона в соответствие с международными подходами» [37].

«Обобщая, можно указать на популярность общего подхода распространения режима персональных данных на метаданные, что включает защитный механизм, вытекающий из содержания права на неприкосновенность частной жизни (вплоть до привлечения к уголовной ответственности по ст. 137 Уголовного кодекса РФ «Нарушение неприкосновенности частной жизни») [40]. Это не требует дополнительных правовых конструкций, тем более что правоприменитель уже разобрался с

тонкостями защиты частной жизни, понимая логику требуемых от него со стороны общества и государства действий. Данный подход (условно назовем традиционным) характерен для тех ученых, которые изначально разрабатывают общее содержание права на неприкосновенность частной жизни, его структуру, а также отдельные элементы [25]. К тому же в рамках требования конфиденциальности информации, относящейся к конкретному лицу, документы, ее закрепляющие, начали свое формирование еще в 80-х гг. прошлого столетия» [20].

«Иной подход связан с формированием самостоятельного права - права на защиту данных. Основой его формирования выступает ст. 8 Хартии Европейского Союза об основных правах, которая устанавливает право на защиту данных, дополняющее установленное в Хартии право на уважение частной и семейной жизни (ст. 7). Это первый опыт формулирования самостоятельного права, вне привязки к устоявшейся системе прав человека. Показательна структура ст. 8 Хартии. Часть 1 предусматривает общее право каждого «на защиту относящихся к нему данных личного характера». Часть 2 устанавливает гарантии соблюдения права» [37]:

- обработка данных должна производиться без манипуляций;
- обработка допускается только в определенных целях;
- наличие согласия заинтересованного лица либо наличие других правомерных оснований, предусмотренных законом;
- каждый имеет право на получение доступа к собранным в отношении него данным;
- право на устранение в данных ошибок.

Часть 3 ст. 8 Хартии закрепляет необходимость создания независимого органа, уполномоченного на проведение контроля за соблюдением установленных гарантий.

«Необходимо отметить, что долгое время европейская правовая политика строилась на объединении права на защиту данных и права на уважение частной жизни. Этому способствовала также практика Суда

Европейского Союза. Однако расширение технических возможностей автоматической обработки различных данных, а также увеличение метаданных, сопровождающих практически каждый вход в «цифровое поле», привели к пониманию необходимости разделения двух прав. Данные, хотя и могут относиться к личным, не всегда обусловливают раскрытие элементов частной жизни. Такие последствия могут происходить при объединении разрозненных данных в единую схему или базу. Именно выделение права на защиту данных позволяет распространить охранительный механизм на большее количество типов сведений (чем это произошло бы при наличии только права на уважение частной жизни). Усиление контроля над персональными данными способствует реализации двух целей: продвижение «цифровых» прав личности и снижение ассиметрии между гражданином и владельцем персональных данных в вопросах обладания ими» [37].

Таким образом, конституционная защита оборота метаданных о гражданах выстраивается в мире по двум основным направлениям: а) в рамках элемента основного права - права на неприкосновенность частной жизни; б) в рамках формулирования самостоятельного права на защиту данных (вне упоминания персональных данных). Техническое развитие цифрового пространства все больше обусловливает актуальность второго подхода.

2.2 Сбор, анализ, хранение персональных данных

Быстрое развитие информационного общества, в котором важность информации и доступ к ней оказывают существенное влияние на экономические, культурные, социальные и другие условия жизни граждан, практически невозможно без комплексного использования различных информационных технологий для обработки различных видов персональных данных. В области защиты персональных данных особое значение имеют

международные стандарты, устанавливающие основные принципы защиты таких данных, которые также развиваются в национальном законодательстве.

«В настоящее время сформировалось конкретное международное регулирование этой сферы. В первую очередь необходимо обратить внимание, что вопросы, касающиеся сферы защиты персональных данных, как правило, рассматриваются в виде одного из аспектов частной жизни. Закрепление данного положения можно увидеть в актах органов ООН, а также в документах иных органов, которые действуют на универсальном уровне в сфере защиты прав человека. Такой же подход является присущем региональным и межрегиональным международным организациям. В качестве примера можно привести Конвенцию о защите прав человека и основных свобод 1950 году, в 8 статье гарантировано такое право, как уважение частной и семейной жизни. Парламентская Ассамблея Совета Европы определяет право на уважение личной жизни человека, а также дополняет его правом на контроль личных данных» [4].

Не менее важно обратить внимание на Конвенцию о защите физических лиц при автоматизированной обработке персональных данных 1981 г., которая является единственной конвенцией, посвященной защите персональных данных. Данная конвенция находит свое применение в отношении автоматизированных файлов персональных данных и автоматизированной обработке персональных данных в государственной и частной жизни. Конвенция все еще находится на стадии доработки и усовершенствования. 10 октября 2018 г. был подписан Протокол о внесении изменений в существующую Конвенцию, который предполагает ее действие на обработку персональных данных в целом.

«Возможность распространения конкретных норм и различных рекомендаций на государства, которые не являются членами соответствующих организаций - еще один крайне важный аспект регулирования вопросов персональных данных на международной арене. «Например, Коллегия Евразийской экономической комиссии выдает

рекомендации государствам-членам по рассмотрению возможности учета лучших практик этой организации, а именно опыта, направленного на реализацию единых путей к налаживанию самых минимальных требований по обработке и защите персональных данных»» [52].

«Продолжая говорить о тех или иных международных стандартах защиты персональных данных, необходимо определить само понятие «персональные данные». Конвенция под номером 108 дает определение персональным данным как любой информации о конкретном лице или поддающемся определению физическом лице, то есть субъекте данных (статья 2). ЕСПЧ применяет конкретно это определение в процессе применения статьи 8 ЕКПЧ в части защиты персональных данных. Иногда определение может перечислять примерный перечень данных. Регламент ЕС указывает имя, сведения местоположения, идентификационный номер и т.д. Российская судебная практика признает персональными данными сведения о месте жительства, паспортные данные, ИНН и СНИЛС, семейное положение, адрес электронной почты, сведения о заработной плате и т.д.» [11].

Можно сделать вывод, что не существует какого-либо закрытого перечня персональных данных. Европейское право содержит определенное разграничение анонимных данных, не относящихся к конкретному физическому лицу, а также полученных анонимно в таком образе, что лицо невозможно идентифицировать; псевдонимизированных данных, отнесение которых к конкретному лицу невозможно без помощи дополнительных данных [55].

Разграничение этих групп информации и оценка уровня возможности идентификации определенного субъекта учитывают то, какие необходимо понести расходы на их выявление, а также количество времени, учитывающее используемые для обработки технологии [11].

Российское право в свою очередь использует понятие «обезличивание персональных данных» [12]. В связи с этим при появлении каких-либо анонимных данных у оператора будет возможность сохранять

консервативный подход или же использовать аргументы в пользу того, что данная информация является анонимной и коммерциализировать ее.

Таким образом, из вышеприведенного законодательства можно сделать вывод, что обработка персональных данных должна отвечать следующим требованиям: законность, справедливость, основываться на свободном, конкретном, информированном и недвусмысленном согласии заинтересованных лиц или на другом правовом основании, предусмотренном законом, быть необходимой и соразмерной законной цели, преследуемой контролером, и т.д. Однако эти требования могут меняться в зависимости от потребностей современного общества.

В международном праве субъекты персональных данных - это лица, обладающие определенными правами: право знать о сборе и обработке своих данных, право на доступ к этим данным, право на исправление неточных или устаревших данных, право возражать против обработки своих персональных данных в определенных случаях и т.д. [13]. У обработчиков также есть обязательства, включая соблюдение принципов и правил, регулирующих обработку персональных данных. Особое значение имеют обязательства государства, даже если оно не участвует в обработке персональных данных. К ним относятся, например, обязательства по предотвращению постороннего вмешательства со стороны юридических и физических лиц (в области неприкосновенности частной жизни и защиты семейной жизни) [14].

Государствам особенно рекомендуется уделять внимание предоставлению надежной защиты права на неприкосновенность частной жизни граждан, а также на способах по защите персональных данных, которые передаются другому иностранному государству. В различных международных актах государствам рекомендовано создавать независимые органы надзорного характера в области обработки личных данных [15].

Можно с уверенностью заявить, что в нынешнее время созданы определенные правила и механизмы по обеспечению защиты личных данных на международном уровне. Использование и соблюдение этих правил играет

огромную роль в сфере обеспечения определенного уровня защиты прав человека в современном цифровом обществе.

На сегодняшний день банки очень часто сталкиваются и борются с угрозами утечки информации и персональных данных. К сожалению, как показывает практика, о случаях кражи конфиденциальной информации аферистами и инсайдерами становится известно все чаще. Огромный массив циркулируемой, безусловно, важной информации в кредитных учреждениях обязывает обеспечить максимальную и всестороннюю защиту как на уровне государства, так и в масштабах самого банковского учреждения. Цифровизация в своем динамичном развитии открывает новые способы кражи и взлома данных, тем самым усложняя работу службы информационной безопасности банков. Ведь попав в руки злоумышленников, конфиденциальная информация может превратиться в орудие преступления - ей могут воспользоваться с целью причинения вреда как финансовому состоянию, так и личной жизни человека. Для банков же утечка, потеря или изменение персональных данных приводит к невосполнимому ущербу - в серьезных случаях к полной остановке деятельности организации или урону деловой репутации. Трудно организовать информационную защиту множества различных баз данных, содержащих информацию персонального характера, держателями которой являются государственные, частные и коммерческие структуры. Еще проблемой, относящейся к рассматриваемой теме, является широкое распространение вычислительных сетей, территориально распределенных систем и систем с удаленным доступом к совместно используемым ресурсам, так как мероприятия по защите таких систем требуют высокой квалификации и экспертной компетенции сотрудников [1].

Наличие человеческого фактора также не стоит оставлять без внимания, так как он является распространенной угрозой не только в банковской сфере. К сожалению, многие сотрудники проявляют небрежность по отношению к своим должностным обязанностям - 80 % банковских правонарушений,

согласно статистике, совершают работники этих же банков, что заставляет насторожиться и предпринять комплекс мер.

Таким образом, появление потенциальных угроз является последствием имеющихся слабых мест в информационной системе, уязвимостью технического оснащения банков, недостаточной компетентностью сотрудников и несоблюдения в полной мере властных законных предписаний.

Такой серьезный вопрос, конечно же, не остается без государственного надзора и нормативного регулирования. Законодательство Российской Федерации в области персональных данных основывается на Конституции РФ и состоит из Федерального закона «О персональных данных» от 27.07.2006 N 152-ФЗ [33] и других законодательных актов, определяющих обработку и использование конфиденциальной информации [4].

Определение персональных данных дано в вышеупомянутом Федеральном законе «О персональных данных». Так, персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [33].

Любая кредитно-финансовая организации может запросить у обратившегося клиента следующую личную информацию, которая подходит под термин «персональные данные» - паспортные данные, сведения о семейном положении, сведения об образовании, номера ИНН, СНИЛС, медицинской страховки, сведения о трудовой деятельности, социальное и имущественное положение, сведения о доходах [3]. Субъектом конфиденциальных данных выступает физическое лицо, в том числе работники банка, давшие согласие на обработку персональных данных банковским учреждением.

И степень успешности деятельности банка зависит во многом от организации им защиты банковской тайны, регулируемой федеральным законом «О банках и банковской деятельности» от 02.12.1990 № 395-1. Также Центральный банк РФ осуществляет надзор за сохранностью

конфиденциальной информации, составляющую банковскую тайну, издавая инструкции и указания.

Как только сотрудники банка получают доступ к персональным данным клиента, они обязаны, согласно своим должностным инструкциям, обеспечить все меры сохранности и защиты представленных данных. В их обязательства входят применять все меры, организационные и технические, по защите личной информации клиентов от свободного доступа, уничтожения, блокировки и иных противозаконных действий носителей внутренних и внешних угроз [49].

Понимая всю серьезность требований, кредитные учреждения системно подходят к защите данных, так как их утеря приводит к урону деловой репутации, которая зарабатывается многими годами, и к появлению судебных исков, что уже несет риски крупных финансовых потерь [5].

Можно сделать очевидный вывод, что защита персональных данных является, без преувеличений, важнейшей задачей кредитно-финансовых организаций. Несмотря на достаточное нормативное регулирования, мы считаем, что необходимо создавать дополнительные подсистемы защиты.

Организация процесса обработки и хранения информационных данных с помощью подключения к сети Интернет также требует появления дополнительных подсистем антивирусной безопасности, выявления внешних вторжений, анализа степени защищенности [7].

Банковские системы очень важны для экономики современных развитых государств, а информационная безопасность первостепенное условие для их успешного функционирования. Информация, которой располагают базы данных банков, имеют реальную материальную стоимость, и требования к хранению и обработке этой информации всегда будут оправданно повышенными. Мероприятия по обеспечению защищенности обработки и хранения персональных данных, несомненно, требуют экспертных знаний, в том числе юридических, и возложения обязательств на доверенного лица по сохранности сведений, составляющих банковскую тайну. Несмотря на

сложную систему обеспечения безопасности данных, банковская организация обязана неукоснительно ее соблюдать и поддерживать, ведь очевидным является тот факт, что защищенность информации является фактором, определяющим успех деятельности любой коммерческой организации.

2.3 Передача персональных данных

На территории Российской Федерации в отношении любых действий и процессов, связанных с персональными данными граждан, действует Федеральный закон № 152 «О персональных данных». ФЗ № 152 распространяется на все организации, зарегистрированные в России, а также представительства иностранных компаний, находящихся в пределах страны.

Согласно ФЗ № 152, под понятие «персональные данные» попадает любая личная информация о гражданине страны, которая позволяет установить его личность.

Основные требования к операторам персональных данных в России:

- Компания-оператор, работающая с базой персональных данных, обязана сообщить каждому субъекту, с какой целью собираются данные о нем, а также получить его согласие на обработку этих данных.
- «В случае, когда личные данные предоставляются онлайн, например, при заполнении какой-либо контактной формы в интернете, на сайте должен быть предусмотрен раздел с Политикой в отношении обработки персональных данных и их конфиденциальности. В самой форме для сбора персональных данных должен присутствовать дисклеймер, проставляя галочку в котором, посетитель сайта дает свое согласие на отправку и дальнейшую обработку своих данных» [4].

– «В случае, если гражданин не дал своего согласия на использование личной информации, данные для обработки могут быть заимствованы из открытых источников. Однако, в отношении этого пункта следует быть предельно внимательными, так как в России уже были прецеденты, когда суд признавал незаконность подобного способа использования информации» [12].
– «Нельзя собирать персональные данные, которые не соотносятся с конечной целью их обработки, вся лишняя информация также должна быть удалена. Например, интернет-магазины не вправе требовать от покупателей предоставление сканов паспортов» [20].
– «В случае, когда цель обработки данных достигнута, личная информация гражданина должна быть удалена или обезличена так, чтобы он не мог быть идентифицирован по хранящимся данным» [5].

Развитие информационных технологий и коммуникаций в современном мире определяет формирование и развитие практически всех общественных отношений. По сути, происходит интеграция информационных технологий и решений в механизм формирования и функционирования различных общественных отношений. Однако данная интеграция создает множество проблемных аспектов, которые необходимо решать на законодательном уровне. Общественные отношения в сфере избирательного права в данном контексте не являются исключением. Безусловно, интеграция информационно-технологических решений в избирательный процесс характеризуется множеством позитивных аспектов. Примером тому служит, в частности, Государственная автоматизированная система Российской Федерации «Выборы», дистанционное электронное голосование и т.д. [30].

Однако существуют, возможно, не самые очевидные, но проблемные аспекты развития информационных технологий, оказывающие влияние на общественные отношения, возникающие в процессе проведения и организации выборов и референдумов. В частности, проблемой является использование персональных данных в целях политической агитации, в том

числе посредством использования таргетированной рекламы и технологий обработки больших данных. Данные проблемы не имеют должной научной разработанности и предметного законодательного решения, однако являются предметом широкой дискуссии в отечественной и зарубежной научной и учебной юридической литературе [2].

Для дальнейшего исследования проблем, связанных с использованием персональных данных в целях политической агитации, необходимо определиться с теми правовыми категориями, которыми следует оперировать в данной работе.

Прежде всего, под персональными данными надо понимать любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [6].

«Агитация предвыборная - это деятельность, осуществляемая в период избирательной кампании и имеющая целью побудить или побуждающая избирателей к голосованию за кандидата, кандидатов, список, списки кандидатов или против него (них)» [30].

«Агитационные материалы - это печатные, аудиовизуальные и иные материалы, содержащие признаки предвыборной агитации, агитации по вопросам референдума и предназначенные для массового распространения, обнародования в период избирательной кампании, кампании референдума» [11].

В данной работе в силу отсутствия законодательного закрепления некоторых технических объектов термин «реклама» и связанные с ним понятия будут использоваться в той части, в которой необходимо отразить некоторые аспекты политической агитации в контексте использования тех или иных технологий, «реклама» не используется в том смысле, который содержит в себе продвижение товаров и услуг.

С развитием технологий сбора и обработки больших объемов персональных данных у операторов (обработчиков и организаторов обработки персональных данных) появилось гораздо больше возможностей использовать

результаты обработки или сами персональные данные в различных исследовательских или коммерческих целях.

В отечественном законодательстве обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. При этом пользователь должен пользоваться лицензированным программным обеспечением [9]. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.

Если рассматривать с формальной точки зрения положения статьи 15 Федерального закона «О персональных данных», то каких-либо проблем с правовым регулированием соответствующих общественных отношений не будет. Законодатель определил условия использования персональных данных в коммерческих и политических целях. Такое использование правомерно только при наличии согласия субъекта персональных данных. Однако существует ряд практических аспектов, которые формируют порочную, отличную от целей законодательного регулирования, правоприменительную практику.

Подавляющее число интернет-ресурсов (социальные сети, сайты и т. д.) предоставляют пользователям свои услуги на безвозмездной основе, однако перед использованием того или иного интернет-ресурса пользователю необходимо ознакомиться и принять условия его использования.

В соответствующих условиях пользования интернет-ресурсы определяют условия обработки и использования персональных данных пользователя, в которых могут быть предусмотрены возможности оператора данных передавать их третьим лицам, а также использовать их в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также

в целях политической агитации, чтобы соблюдать требования законодательства.

У пользователя в данной ситуации есть только два варианта: либо принять такое соглашения, чтобы иметь возможность использовать интернет-ресурс или приложение, либо отклонить его и, соответственно, не иметь возможности пользоваться продуктом. Исходя из этого, как правило, абсолютное большинство пользователей принимают условия использования приложения или интернетресурса, зачастую даже не ознакомившись с ними. Подобный правовой нигилизм в совокупности с отсутствием реального выбора модели поведения предоставляет операторам возможность использовать персональные данные в любых целях, в том числе для политической агитации.

Таким образом, на практике нивелируется та диспозиция для пользователей и субъектов персональных данных, которая регламентирована в ст. 15 Федерального закона «О персональных данных». При отсутствии реального выбора условий использования субъектами персональных данных формируется возможность бесконтрольного влияния на политические процессы посредством политически мотивированной таргетированной рекламы влиять на избирательный процесс.

При этом под таргетированной рекламой следует понимать способ онлайн-рекламы, в котором используются методы и настройки поиска целевой аудитории в соответствии с заданными параметрами (характеристиками и интересами) людей, которые могут интересоваться рекламируемым товаром или услугой. Такую рекламу показывают только выбранной (целевой) аудитории. В данном контексте необходимо отметить, что таргетированная реклама и вопросы, связанные с ней, также не нашли своего законодательного регулирования на сегодняшний день.

Использование персональных данных может повлиять на избирательный процесс и какова роль в этом таргетированной рекламы.

Операторы (интернет-сайты, социальные сети, телекоммуникационные компании и т.д.), получив согласие от пользователей (субъектов персональных данных), могут применять персональные данные для обработки, в том числе для целей, которые преследует таргетированная реклама. Рассмотрим данный процесс поэтапно.

1 этап - оферта и согласие. Социальная сеть (оператор персональных данных) предоставляет возможность бесплатного пользования ее функционалом пользователю (субъекту персональных данных). Для того чтобы последний мог начать использование, ему необходимо выразить согласие в пользовательском соглашении (с точки зрения законодательства пользовательское соглашение является публичной офертой: предложением заключить договор на указанных условиях с любым, кто отзовется - п. 3 ст. 437 ГК РФ). В данном соглашении будут указаны цели и условия обработки персональных данных пользователя.

2 этап - использование. Субъект персональных данных использует социальную сеть, проявляет активность, посещает страницы, делает записи, отправляет сообщения, подписывается на людей/издания с определённой тематикой, проявляет предметный интерес к чему-либо и т.д.

3 этап - сбор данных и анализ. Социальная сеть посредством своих технических возможностей отслеживает всю активность пользователя, формирует информационную систему персональных данных. Исходя из этой активности, происходит анализ полученных данных.

4 этап - использование данных. После обработки и анализа персональных данных пользователя социальная сеть может определить характеристики и интересы конкретного пользователя. Полученная информация может быть использована в таргетированной рекламе.

5 этап - таргетированная реклама. Социальная сеть, обладая детальной информаций о пользователе, может при использовании ее приложения или сайта предлагать и размещать те объявления, которые содержат информацию, ориентированную на пользователя. Например, если пользователь проявляет

интерес к публикациям, в которых критикуются меры излишней государственной поддержки социальной сферы (левые идеи), то, вероятнее всего, такой пользователь придерживается идей правого толка. Алгоритмы социальной сети при использовании будут продвигать ту политическую агитацию, в которой будут отражены политические идеи соответствующих взглядов. Именно на данном этапе может происходить влияние на предвыборную агитацию посредством использования персональных данных. Однако приведённый пример профайлинга пользователя является достаточно примитивным в силу того, что возможные политические предпочтения в условиях развития технологий обработки больших массивов данных представляется возможным определить, исходя из других данных о пользователе и его активности, которая напрямую с политической сферой не связана [7].

Использование персональных данных в целях политической агитации при наличии согласия пользователя не является нарушением законодательства о персональных данных, подобная обработка персональных данных осуществляется в рамках закона. Как ранее было отмечено, у пользователя есть два варианта действий:

- согласиться на условия, которые предложены в соглашении об использовании, и предоставлять свои персональные данные для обработки, в том числе для политических целей;
- отказаться от таких условий, но в то же время лишить себя возможности использования соответствующих интернет-ресурсов, что на практике, безусловно, не является приоритетным вариантом, поскольку необходим тот функционал, которые предоставляют приложения или сайты, и, зачастую подобрать альтернативу тому или иному интернет-ресурсу невозможно.

Другой проблемой при обработке персональных данных является факт того, что в силу недостаточного уровня защищенности и методов передачи или хранения больших объёмов данных нередки случаи хищения (утечки)

персональных данных при содействии злоумышленников в открытый доступ. Данные ситуации характерны как для зарубежных IT компаний, так и для отечественных интернет-агрегаторов.

Если рассматривать сущность самой проблемы, которая заключается в некорректной обработке и использовании персональных данных для профайлинга и таргетирования пользователей, то в данном контексте необходимо отметить позицию, сформированную рядом представителей отрасли и академического сообщества. Данная позиция заключается в запрете самой таргетированной рекламы и профайлинга пользователей. По мнению сторонников такого подхода, все проблемы, которые возникают при обработке персональных данных и их дальнейшем использовании, исчезнут, поскольку пропадет сам объект проблемы [10].

Подход, состоящий в запрете таргетированной рекламы и профайлинга, является весьма радикальной мерой, которая не учитывает такой правовой принцип, как баланс частных и публичных интересов в силу того, что подобный запрет - фундамент экономики некоторых из самых прибыльных компаний как в России, так и за рубежом. Доходы от рекламы являются одним из ключевых элементов в хозяйственно-экономической модели интернет-агрегаторов. Например, Google и Facebook, включая их дочерние компании, такие как Instagram и YouTube, получают примерно 83 % и 99 % своего дохода от одной вещи - продажи рекламы. То же самое у Twitter и других бесплатных сайтов и приложений. Более того, эти компании занимаются так называемым поведенческим таргетингом, чтобы нацеливать рекламу на конкретную аудиторию, исходя из многочисленных метрик, которыми они располагают о пользователя; учитывается все - от настроения и предпочтений в еде до взглядов на религию и общественные процессы [8].

Учитывая уровень развития технологий обработки информации, а также те результаты, которые представляется возможным достигнуть посредством использования соответствующих технологий, на наш взгляд, необходимо внести изменения в действующее законодательство в целях исключения

угрозы влияния использования персональных данных рамках осуществления предвыборной агитации. Необходимость соответствующих изменений также подтверждается зарубежными прецедентами, в которых использование персональных данных оказало влияние как на политическую, так и на предвыборную агитацию, что подорвало доверие граждан к избирательным институтам и демократическим ценностям.

Согласно п. 1 ст. 15 Федерального закона «О персональных данных» [33], обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Исходя из анализа правоприменительной практики относительно содержания исполнения условий обработки персональных данных между субъектами персональных данных и операторами, учитывая распространенность нецелевого использования персональных данных целесообразно в данной связи внести изменения в ст. 15 ФЗ «О персональных данных» посредством запрета на использование персональных данных в целях политической агитации.

Для создания эффективного механизма правового воздействия также необходимо установить санкции за обработку, передачу или использование персональных данных в целях политической агитации в размере 50000000 рублей или до 5 % от годового оборота оператора за предыдущий финансовый год, в зависимости от того, что больше.

В том случае, если использование персональных данных в целях политической агитации будет осуществлено в рамках выборов федерального уровня (выборов Президента, выборов депутатов Государственной думы) или проведения федерального референдума, то санкции для операторов необходимо увеличить и установить в размере 100000000 рублей или до 10 % от годового оборота оператора за предыдущий финансовый год, в зависимости от того, что больше.

Другим необходимым решением в контексте рассматриваемой проблемы является легальное закрепление такого термина, как «таргетированная реклама» в законодательстве.

В частности, таргетированную рекламу следует определять как способ онлайн-рекламы, в котором используются методы и настройки поиска целевой аудитории в соответствии с заданными параметрами пользователей, которые могут интересоваться рекламируемым товаром или услугой.

При закреплении данной правовой категории представляется необходимым внести изменения в Федеральный закон от 12.06.2002 г. № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации», дополнив пункт 1.1 статьи 56 следующим положением: «При проведении предвыборной агитации, агитации по вопросам референдума не допускается использование таргетированной рекламы в сети Интернет».

Введение подобных ограничений необходимо в силу того, что таргетированная реклама является методом влияния на предвыборную агитацию, который в основе своей использует персональные данные пользователей.

Таким образом, развитие информационных технологий послужило началом изменений способов и целей распространения личных данных человека. В случае раскрытия личной информации человеку может быть причинен как материальный, так и моральный вред. В результате появилась необходимость нормативного правового регулирования порядка получения, хранения, обработки, передачи и защиты личной информации. Действующее законодательство не вполне соответствует требованиям современности.

3 Проблемы правового регулирования и защиты персональных данных

3.1 Проблемы реализации законодательства РФ о защите персональных данных

Сейчас судебная практика, связанная с нарушением законодательства о персональных данных, неоднородная, это следует из анализа дел [45], [46], [47], [48].

Согласно ст. 23 Конституции Российской Федерации каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени [26].

Указанный конституционный принцип раскрывает важность защиты и охраны персональных данных, поскольку именно они составляют частную и личную жизнь человека. Под персональными данными принято понимать любые сведения, которые позволяют прямо или косвенно идентифицировать человека.

Персональные данные широко используются каждым человеком. Когда работник заключает трудовой договор, он сообщает свои паспортные данные, работодатель знает его идентификационный номер налогоплательщика и страховой номер индивидуального лицевого счета. Заключая различные гражданско-правовые договоры, физические лица указывают совокупность персональных данных о себе [3].

По мнению Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее — Роскомнадзор), в Российской Федерации в области персональных данных создана эффективная система защиты прав субъектов персональных данных. Но нет ли необходимости в эпоху цифровизации и глобализации общества,

которые подразумевают его трансформацию во всех сферах отношений, обеспечивать условия по совершенствованию системы защиты персональных данных?

Согласно исследованию, проведенному международной компанией в области консалтинга и аудита PricewaterhouseCoopers (PWC), 97 % людей не доверяют компаниям в вопросах защиты своих персональных данных [5]. По данным социального опроса, проведенного Аналитическим центром при Правительстве Российской Федерации, 55 % опрошенных уверены в использовании их персональных данных третьими лицами [5].

Таким образом, несмотря на то что гарантия защиты персональных данных является обязательным элементом для реализации прав, закрепленных в ст. 23 Конституции РФ [26], вопрос о доверии граждан к защищенности их персональных данных остается открытым, так как связан с проблемами реализации прав субъекта персональных данных.

Правоотношения в области персональных данных возникают между двумя субъектами. Первый — это непосредственно сам субъект персональных данных, то есть физическое лицо, чьи персональные данные находятся в обработке, а второй — оператор, то есть обрабатывающий персональные данные.

Одно из ключевых прав, которым наделен каждый субъект, — это право на доступ к своим данным. Это означает, что физическое лицо имеет право на получение сведений о подтверждении факта обработки персональных данных оператором, о правовом основании и цели обработки его данных, а также других сведений, указанных в ч. 7 ст. 14 ФЗ «О персональных данных [33].

Несмотря на фундаментальность этого права, суды зачастую используют формальный подход при разрешении дел, связанных с нарушением прав субъекта персональных данных. Так, рассматривая апелляционную жалобу Т. И. Лариной к АО «Банк Русский Стандарт» с требованием обязать предоставить информацию об обработке ее персональных данных, Московский городской суд пришел к выводам,

которые, на мой взгляд, противоречат природе правоотношений в области персональных данных [27].

Истица заключила с банком договор банковского счета и впоследствии направила запрос, в котором просила подтвердить факт обработки персональных данных, сообщить правовые основания и цели обработки персональных данных, сообщить сведения о лицах, которые имеют доступ к персональным данным, — то есть реализовывала право, представленное ей ст. 14 ФЗ «О персональных данных» [33].

Однако банк отказал в предоставлении перечисленных сведений, при этом отказ выразился в простом бездействии. Суд встал на сторону кредитной организации, так как «истица самостоятельно предоставила ответчику свои персональные данные в целях их обработки. Ей были известны цели обработки персональных данных, наименование и место нахождения оператора. Доказательств того, что ее персональные данные были переданы банком иным лицам в целях их обработки в материалах дела отсутствуют» [27]. Схожая позиция судов находит отражение и в решениях по другим делам.

К сожалению, суды не учитывают тот факт, что право на доступ к своим данным предоставлено законом, выступает императивной нормой и может ограничиваться в исключительных случаях, указанных в законе. Отказывать в реализации права доступа на основании недоказанности существующих нарушений незаконно.

Кроме того, законодательством в сфере персональных данных предусмотрено обязательное согласие субъекта при обработке персональных данных в целях рекламы и политической агитации.

Сложно сказать, что указанное право в Российской Федерации соблюдается в полной мере. В современной России звонки с неизвестных номеров с предложением различных услуг или звонки, которые сразу сбрасываются с целью последующей обработки активности для рекламы, стали обычной практикой [8]. Вопрос о наличии предварительного согласия субъекта персональных данных на рекламу услуг даже не стоит.

При этом проблема игнорирования права на обязательное согласие субъекта персональных данных касается только коммерции — рекламы услуг или товаров, нарушения в части политической агитации отсутствуют.

По моему мнению, причина наличия халатности со стороны рекламодателей и рекламораспространителей в отношении согласия субъекта заключается в сложности идентификации лица, предлагающего товар или услуги, и отсутствие должного механизма выявления лиц для привлечения к ответственности. Хороший пример привела Терещенко Л.К., указав, что наше законодательство для борьбы с незаконной рекламой может позаимствовать правовой механизм, установленный в испанском законодательстве [39].

Законом Испании предусмотрено, что в случае рекламной рассылки лицо обязано в каждом письме или сообщении указывать не только источник получения персональных данных субъекта и его права, но и сведения о лице, осуществляющем рассылку [54]. Такой подход помог бы решить существующую проблему в области рассылки рекламы, поскольку лицо, предлагающее товары, работы или услуги, будет идентифицировано и начнет принимать решение о необходимости подобной рекламы под страхом ответственности.

Таким образом, проблема реализации некоторых прав субъекта персональных данных связана с отрицательной судебной практикой, когда суды игнорируют обязательные требования, установленные законодательством, а также с отсутствием надлежащего правового механизма, защищающего субъекта от рекламы, которую он получает при незаконной обработке его персональных данных.

Представляется, что для решения таких проблем необходимо обязать идентифицировать операторов при обработке персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем (субъектом персональных данных).

Законодательство в сфере персональных данных в современном виде существует в Российской Федерации 15 лет, судебных споров по вопросам

персональных данных возникает множество. Возможно, для улучшения судебной практики, которая бы не допускала вынесения заведомо незаконных решений, необходимо обобщение практики от высших судов. На мой взгляд, обзор практики Верховного суда РФ в согласованности с судами общей юрисдикции позволил бы устранить проблемы, возникающих в связи с неправильным толкованием и применением норм о персональных данных со стороны судов.

Трудно представить современную действительность без новых технологий, связанных с «Всемирной паутиной» (Интернет). В повседневной жизни нормальные правовые отношения вошли в совершенно новое пространство, создав новый вид отношений, в которых возможны преступления и в которых нарушаются конституционные права и законные интересы личности. Сегодня почти каждый человек в мире пользуется Интернетом. После пандемии коронавируса мир осознал, что многие услуги должны быть доступны удаленно через веб-сайты и веб-приложения. Проще говоря, многие аспекты повседневной жизни переместились в виртуальное пространство. По данным Digital 2020, в России 118 миллионов интернет-пользователей - 81% населения.

В содержание этого блага входят несколько элементов, таких

- как право гражданина формировать свою внешность по своему усмотрению,
- право фиксировать или разрешать фиксацию своей внешности любым способом и в любой форме,
- право сохранять и изменять внешность,
- право определить круг лиц, которым граждан представлять возможность обозревать свою внешность.

Внешность, как нематериальное благо прямо не упомянуто в п.1. ст.150 ГК, но данный перечень нематериальных благ является открытым.

«Внешность является средством индивидуализации гражданина в обществе, элементом его личности. Именно поэтому описание внешности

гражданина и его изображение, представляет собой часть сведений о его личности. Этим и объясняется необходимость получения согласия гражданина на обнародование его изображения; поэтому неразрешённое гражданином опубликование его изображения рассматривается, как нарушение его нематериального блага, за исключением случаев, когда такое обнародование или разрешение прямо допускается или предписывается законом» [2].

Согласие гражданина не требуется в случаях, когда:

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

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

- гражданин позировал за плату.

Изготовленные в целях введения в гражданский оборот, а также находящиеся в обороте экземпляры материальных носителей, содержащих изображение гражданина, полученное или используемое с нарушением пункта 2 статьи 152, подлежат на основании судебного решения изъятию из оборота и уничтожению без какой бы то ни было компенсации. Если изображение гражданина, полученное или используемое с нарушением пункта 3 статьи 152, распространено в сети «Интернет», гражданин вправе требовать удаления этого изображения, а также пресечения или запрещения дальнейшего его распространения.

Изображения граждан в той или иной форме использовались на протяжении веков, но сегодня они стали распространены практически во всех сферах жизни общества. В основном это связано с развитием информационных технологий. Однако изображение гражданина может быть использовано в корыстных и иных целях без согласия изображенного лица,

поскольку субъекты использования не обладают правовыми знаниями и полагают, что такие действия не приведут к правовым последствиям.

В то же время к образу физического лица как гражданской группы чаще всего обращаются, когда существует риск, что это личное моральное право будет нарушено или уже нарушено. Это усиливает необходимость гражданских средств правовой защиты, но усугубляется отсутствием исследований права граждан на изображение и, следовательно, его защиты. Поэтому цель нашего исследования - рассмотреть и проанализировать основные проблемы, связанные с защитой этого личного неимущественного права, и сделать необходимые выводы. Прежде всего, необходимо раскрыть юридическую сущность права гражданина на изображение.

«Статья 152.1, регулирующая это право, расположена в гл. 8 «Нематериальные блага и их защита» I раздела Гражданского кодекса РФ [1]. В ранее действующем Гражданском кодекс РСФСР от 11 июня 1964 г. схожая ст. 514 содержалась в разделе IV «Авторское право», однако регулировала она только правоотношения по поводу произведений изобразительного искусства, в связи с чем требовала расширительного толкования. Из этого следует, что по смыслу действующей редакции ст. 152.1, изображение гражданина представляет собой нематериальное благо, тогда как право на изображение – личное неимущественное право, что подтверждают некоторые определения Семейного кодекса РФ (далее - СК)» [33].

«Защита гражданских прав – это некие меры, то есть ограниченное воздействие, применяемое непосредственно в случае нарушения или реальной угрозы нарушения гражданских прав. Однако, если установленные в законе предписания недостаточно точны, а формулировки отдельных положений размыты, то защита права затрудняется банальной невозможностью с полной уверенностью сказать, в каком случае то или иное право вообще нарушено» [1]. Пункт первый ст. 152.1 Гражданского кодекса РФ (далее – ГК РФ) закрепляет: «Обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или

произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина. После смерти гражданина его изображение может использоваться только с согласия детей и пережившего супруга, а при их отсутствии – с согласия родителей» [1], также данная статья устанавливает необходимые исключения из вышеназванного общего правила.

В то же время, законодательно не установлено, что является изображением гражданина. По толковому словарю С.И. Ожегова и Н.Ю. Шведовой, изображение - «предмет, рисунок, изображающий кого/что-нибудь; зрительное воспроизведение чего-нибудь» [7].

Однако, это определение малоприменимо ввиду недостаточной строгости формулировки, его сложно применить к понятию «изображение гражданина». Более ёмкое раскрытие этого термина представил С.В. Баринов: «изображение любого объекта – это то, что создаётся из образа такого объекта ... В случае изображения гражданина образом является его внешний облик (внешность) ...» [1]. Схожая позиция отражена в Апелляционном определении Алтайского краевого суда, где указано, что под изображением гражданина «следует понимать внешний облик гражданина, включающий в себя не только лицо, но внешний вид в целом». Под внешним обликом, по мнению криминалистов, понимается «неразрывную совокупность наружных признаков человека, воспринимаемых в виде целого или фрагментарного образа» [7].

«Такая дефиниция позволяет выделить изображение физического лица, как отдельный объект, однако остаётся вопрос о соотношении изображения гражданина и персональных данных, как любой информации, относящейся к прямо или косвенно определенному или определяемому физическому лицу. Однако в рамках настоящей статьи, подробный разбор этого вопроса затруднителен, тем более что законодательство [2] прямо не определяет изображение физического лица как персональные данные, а некоторые определения СК не относят фотографии граждан к таковым, в связи с чем о

распространении норм Федерального закона «О персональных данных» на рассматриваемые правоотношения пока не приходится» [33].

«Немаловажным предстаёт момент дачи согласия гражданином на использование его изображения. Кажется очевидной форма такого согласия ввиду того, что Пленум Верховного Суда РФ в п. 46 своего постановления установил, что «Согласие на обнародование и использование изображения гражданина представляет собой сделку» и, соответственно, по общему правилу, может она быть совершена в письменной или устной форме, а также путём совершения конклюдентных действий. Однако если согласие дано не в письменной форме, то им «охватывается использование изображения в том объеме и в тех целях, которые явствуют из обстановки, в которой оно совершалось»» [3].

«Возможность различного понимания приведённой конструкции, на практике может создавать прямо противоречащие друг другу правовые позиции. Так существуют два апелляционных постановлений СК по гражданским делам Новосибирского областного суда [2] и по гражданским делам Приморского краевого суда [4], в которых вынесены два противоположных решения о том, свидетельствует ли согласие гражданина на фотографирование и позирование фотографу о его согласии на обнародование и использование фотографии. В связи с этим наиболее бесспорной является такая форма совершения этой сделки, как простая письменная, в виде одного документа. В то же время законодательно не урегулированы порядок получения и содержание согласия на обнародование, и дальнейшее использование изображения» [4].

«Так, исходя из ст. 152.1 не очевидно, что согласие необходимо получать на каждый вид, форму и цель использования, не предусмотрены сроки, на которое оно даётся и так далее. В то же время, данное ранее согласие может быть отозвано гражданином в любой момент, что, в принципе, компенсирует отсутствие определения сроков в статье Гражданского кодекса РФ, однако создаёт некоторую нестабильность гражданского оборота, потому как лицу,

получающему согласие, неизвестно, когда такое согласие может быть отозвано, что усложняется тем, что срок возможности отзыва согласия не ограничивается смертью лица, изображённого на фотографии (п. 1 ст. 152.1 ГК РФ)» [3].

«Также некоторые трудности в понимании ст. 152.1 ГК РФ вызывает раскрытие содержания понятия «использование» изображения. Трактовка использования, как совершения «тех же действий, что и при обнародовании, но другими лицами и другими техническими средствами» [52] представляется неудовлетворительной, если речь идёт о необходимости защиты права. Множественность способов использования, на наш взгляд, требуют более чёткой регламентации для единообразия понимания ст. 152.1 Гражданского кодекса РФ. Кроме того, сложно согласиться с определением СК в котором указано, что анализ указанной ранее статьи, даёт основание утверждать, что для необходимости защиты права на изображение «необходимо наличие двух обязательных условий: это обнародование изображения и его дальнейшее использование. Это обусловлено тем, что одно только использование, например передача изображения в личной переписке, может быть нежелательна для изображенного гражданина, однако такие действия не подпадают под содержание термина «обнародование» в смысле ст. 1268 ГК РФ, в то же время кажется необходимой правовая защита интересов указанного лица» [7].

Рассмотрев судебную практику, можно заметить, что норма права об охране изображения граждан трактуется по-разному. Согласно разъяснениям, содержащимся в п. 7 Постановления Пленума Верховного Суда Российской Федерации от 24 февраля 2005 г. №3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц», по делам данной категории необходимо иметь в виду, что обстоятельствами имеющими в силу ст.152 ГК РФ значимыми для дела являются: факт распространения ответчиком сведений, об истце, порочащие характер этих сведений и несоответствие их действительности. При

отсутствии хотя бы одного из указанных обстоятельств иск не может быть удовлетворен судом.

Под распространением сведений, порочащих честь и достоинство граждан или деловую репутацию граждан, следует понимать опубликование таких сведений в печати, трансляцию по радио и телевидению, демонстрация в кинохроникальных программах и других средствах массовой информации, распространение в сети «интернет», а также использование иных средств телекоммуникационной связи, изложение в служебных характеристиках, публичных выступлениях, заявлениях, адресованных должностными лицами, или сообщение в той или иной, в том числе устной, в форме хотя бы одному лицу. Несмотря на это, решением Арбитражного суда от 25.02.2016 г. по делу о защите исключительных авторских прав на фотографические произведения, Арбитражный суд разрешил российским СМИ, использовать фотографии без разрешения их владельцев.

Это использование только для информации. Теперь СМИ могут использовать чужие фотографии для иллюстрации новостных событий, связанных с экономикой, политикой, обществом и религией. Должны быть соблюдены определенные требования: имя фотографа и источник фотографии. Фотография должна находиться в общественном достоянии, и нет конкретного запрета на ее использование [3].

В российском законодательстве нормы изложены непосредственно в Федеральном законе «О персональных данных» [33], но существуют проблемы с пониманием этих норм. Для юристов важен не сам юридический текст, а то, как его интерпретируют те или иные суды. Это объективный факт, на который необходимо обратить внимание. Суд по интеллектуальной собственности – это, по сути, особая юрисдикция. Другое дело, что есть вопросы, по которым разные суды расходятся во мнениях.

Все вышесказанное указывает на необходимость создания более четких правовых структур для достижения более полного и последовательного понимания права граждан на изображения, что, несомненно, является

необходимым условием для защиты этого права. Особой проблемой для защиты изображений граждан является вопрос о конкретных мерах. Пункты 2 и 3 данной статьи предусматривают конкретные меры, которые должны быть приняты заинтересованными сторонами в случае нарушения права на изображение, т.е. защитные меры. Однако особенности правового регулирования личных неимущественных отношений в целом и специфика данного права ставят вопрос о возможности применения общих способов защиты гражданских прав, открытый перечень которых содержится в статье 12 ГК РФ. «Можно согласиться с ученым С.Ю. Головиной: «если способы защиты нарушенных прав, указанные в пп. 2 и 3 ст. 152.1, дополняют перечень способов, то способы защиты, названные в ст. 12, могут применяться к случаям нарушения права на изображение гражданина». Анализируя ст.ст. 12 и 152.1 ГК РФ, можно сделать вывод, что способы защиты права гражданина на изображение являются частными случаями таких способов, как «восстановление положения, существовавшего до нарушения прав, и пресечение действий, нарушающих право или создающих угрозу его нарушения» и «прекращение или изменение правоотношения» [1], то есть они не являются дополнительными к списку способов, представленных в ст. 12 Гражданского кодекса РФ. Следовательно, можно констатировать, что в случае нарушения права гражданина на изображение применимы только способы защиты, указанные в Гражданском кодексе РФ (ст.152.1 и ст. 151 - компенсация морального вреда)» [15].

Следует отметить, что это не единственное решение, приводимое в доктрине гражданского права, и, на наш взгляд, создающее неоправданные ограничения при защите права физического лица на собственное изображение. Так, в апелляционном определении СК Пензенского областного суда сказано: «Исходя из системного толкования [ст. 12 и 152.1 ГК РФ], помимо универсального способа защиты нематериальных благ в виде компенсации морального вреда способом защиты изображения личности следует считать пресечение действий, нарушающих право или создающих угрозу его

нарушения» [5].

В случае нарушения личных нематериальных прав потерпевший может требовать компенсации за физические или психические страдания в соответствии со статьей 151 Гражданского кодекса в качестве компенсации за психические страдания. При нарушении этого личного морального права причинение нравственных страданий презюмируется и не требует доказывания, что логически подтверждается апелляционным определением Брянского районного суда по гражданским делам СК 433.

Мы не рассматриваем проблемы, связанные с расчетом суммы такой компенсации, поскольку они относятся скорее к самой схеме компенсации, чем к защите права на изображение. Однако у некоторых авторов вызывает вопросы предложение принять стандарты, предусматривающие «денежную компенсацию за нарушение права на изображение, аналогичную компенсации морального вреда» [3].

Нематериальные блага не могут иметь денежную стоимость как объекты личных неимущественных прав. Следовательно, право на публичный образ и особенности защиты этого права изучены недостаточно, а их правовое регулирование не успевает за развитием общественных отношений в этой сфере. Данная ситуация создает серьезные проблемы для защиты образа гражданина, которые, по нашему мнению, должны быть исправлены путем внесения следующих поправок в гражданское законодательство.

- Необходимо определить, какой образ гражданина подпадает под действие закона;

- Определить в статье 152.1 форму и порядок, посредством которых гражданин дает согласие на обнародование и последующее использование его изображения в качестве сделки.

- Раскрыть содержание использования изображения и его связь с раскрытием информации;

- Статья 152.1 должна содержать расширенный перечень средств защиты этого личного неимущественного права или делать необходимую

ссылку на статью 12 Гражданского кодекса Российской Федерации.

Важно также отметить, что взаимосвязь между правом граждан на изображение, авторским правом и персональными данными нуждается в дальнейшем теоретическом исследовании для создания более детальной правовой базы.

3.2 Проблемы применения юридической ответственности за нарушение законодательства о персональных данных

Российскому законодателю необходимо решить проблемы защиты персональных данных с опорой как на зарубежный опыт, так и на пробы и ошибки «коронавирусного нормотворчества». Автором выявлен ряд проблем, которые являются следствием несовершенства понятийного аппарата и, как следствие, правового режима традиционных персональных данных, биометрических персональных данных и генетических данных.

В современный информационный век знания являются важнейшим ресурсом для развития общества, и их ценность динамично растет. В прошлом основными ресурсами общества были ископаемые материалы и энергия, для которых были созданы соответствующие способы использования, но с информационной революцией появились инструменты, компьютеры и другие цифровые технологии, которые все больше проникают в жизнь современного общества.

Актуальность данной работы основана на том, что ценность персональных данных человека возросла, поэтому к защите персональных данных необходимо подходить более ответственно. Хорошо известно, что персональные данные встречаются буквально в каждой области права, но в уголовном процессе этот институт имеет серьезные ограничения.

Часть 1 статьи 23 Конституции РФ [26] гласит, что “каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту

своей чести и доброго имени", а часть 1 статьи 24 Конституции РФ устанавливает ограничения по сбору, хранению, использованию и распространению указанных сведений.

Уголовный процесс - это деятельность уполномоченных лиц в связи с выявлением, расследованием и преследованием уголовного преступления, а также система правоотношений, которые уполномоченные лица поддерживают между собой и с другими лицами, участвующими в уголовном процессе. Поскольку уголовно-процессуальное право является частью публичного права, его положения по своей сути носят принудительный характер, то есть налагают обязательное правовое ограничение на поведение субъекта.

Основным основанием для возбуждения уголовного дела является совершение преступления как общественно опасного деяния, которое должно быть должным образом наказано. Не секрет, что преступления совершаются везде и даже в больших масштабах. В уголовное дело может быть вовлечено множество людей, некоторые из которых могут даже не иметь личного интереса в этом деле. К ним относятся свидетели и другие участники судебного процесса, которые не были допущены на судебное заседание по собственной воле. Это могут быть прямые и косвенные свидетели преступления, непричастные посторонние лица, выступающие в качестве свидетелей, или лица, не имеющие отношения к преступлению или преступнику, но официально допрашиваемые в качестве свидетелей в рамках досудебного расследования для обеспечения полного установления обстоятельств дела. В некоторых случаях число основных участников уголовного дела может даже превышать число вовлеченных лиц.

Если лица, не вовлеченные в уголовный процесс, включаются в него против их воли, возникает законный вопрос о том, защищены ли их персональные данные. Ведь каждое следственное и процессуальное дело содержит большое количество личной информации о человеке, начиная от его личности, места жительства и контактных данных и заканчивая личными

предпочтениями и частными обстоятельствами [51].

Вопрос обоснован тем, что в ходе уголовного судопроизводства по конкретному делу доступ к персональным данным человека могут иметь многие лица: формальные - следователь, оперативные сотрудники, защитник, прокурор и его помощники, судья и многие другие - и неформальные - общественные помощники следователя, помощники адвокатов, стажеры правоохранительных органов всех видов и студенты, проходящие практику, которые могут иметь неформальный доступ к официальным документам.

Хотя российское законодательство предусматривает ответственность за разглашение конфиденциальной информации и механизм санкций, практика показывает, что время от времени персональные данные известных лиц по уголовным делам просачиваются в общественность и прессу, не говоря уже о безопасности персональных данных обычных граждан.

«Данные негативные обстоятельства являются начисто следствием несовершенства норм уголовного процессуального права по следующим основаниям. В Уголовно-процессуальном кодексе РФ отсутствуют отдельные нормы о защите персональных данных, что по моему мнению является правовым пробелом. Отсутствие таких положений с одной стороны неудивительно, поскольку при принятии Кодекса в 2001 году в российском законодательстве вовсе отсутствовал специальный закон о персональных данных, который появился лишь в 2006 году с принятием Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» [33], а с другой стороны вызывает серьезные опасения по поводу защиты персональных данных. В настоящее время персональные данные можно отнести к одному объемному термину, закрепленному в УПК: данные предварительного расследования, поскольку при «сливе» персональных данных отдельных участников уголовного судопроизводства может нанести серьезный ущерб предварительному расследованию. Как установлено частью 1 статьи 161 УПК РФ: «данные предварительного расследования не подлежат разглашению за исключением случаев, предусмотренных настоящим Кодексом». Согласно ч.

2 ст. 161 УПК РФ: “данные предварительного расследования могут быть преданы гласности лишь с разрешения следователя или дознавателя и только в том объеме, в каком ими будет признано это допустимым, если разглашение не противоречит интересам предварительного расследования и не связано с нарушением прав, свобод и законных интересов участников уголовного судопроизводства»» [33].

Как установлено частью 3 ст. 161 УПК РФ: «следователь или дознаватель предупреждает участников уголовного судопроизводства о недопустимости разглашения без соответствующего разрешения данных предварительного расследования, о чем у них берется подписка с предупреждением об ответственности в соответствии со статьей 310 Уголовного кодекса Российской Федерации». Из этого следует, что об ответственности по ст. 310 УК РФ предупреждаются строго определенные участники уголовного судопроизводства, перечисленные в разделе II УПК РФ.

«Между тем, как указано ранее, доступом к материалам уголовного дела имеют различные лица, от которых подписка с предупреждением об ответственности по ст. 310 УК РФ не берется. В случае нарушения такими лицами конфиденциальности сведений, содержащихся в материалах уголовного дела, в результате чего повлекло нарушение интересов предварительного расследования, отсутствует формальный состав преступления в связи с отсутствием подписки. Данная недоработка является пробелом уголовного законодательства, позволяющим лицам, посредственно участвующим в уголовном судопроизводстве, избегать от уголовного наказания» [40].

Также следует отметить, что во всех остальных случаях нарушения конфиденциальности персональных данных из материалов уголовного дела предусмотрена административная ответственность по ст. 13.14 КоАП РФ «Разглашение информации с ограниченным доступом», согласно которому «разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации

влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 и статьей 17.13 настоящего Кодекса, - влечет наложение административного штрафа на граждан в размере от пяти тысяч до десяти тысяч рублей; на должностных лиц - от сорока тысяч до пятидесяти тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц - от ста тысяч до двухсот тысяч рублей».

Проанализировав составы уголовных и административных правонарушений, можно сделать вывод, что в обоих случаях нарушение прав граждан на защиту персональных данных является допустимым, основным критерием при этом остается подпись следователя или дознавателя. Однако наличие мандата не увеличивает степень нарушения прав субъектов данных, поскольку специальное законодательство запрещает незаконную передачу персональных данных третьим лицам. В этом отношении различие между уголовной и административной ответственностью за одно и то же нарушение прав субъектов данных на основании критерия подписки о неразглашении, на мой взгляд, является пробелом в законодательстве.

Следовательно, возникают правовые проблемы в уголовном процессе, когда лица привлекаются к ответственности за нарушение обязанности сохранять конфиденциальность персональных данных, и эти проблемы могут быть решены следующим образом: Уголовный состав преступления, предусмотренный статьей 310 Уголовного кодекса, нуждается в уточнении путем исключения записи о неразглашении данных как обязательного элемента объективной стороны уголовного преступления и добавления положения о последствиях в виде нарушения процедуры расследования и существенного нарушения прав и законных интересов.

Заключение

Персональные данные – это любые сведения, относящиеся к прямо или косвенно определённому или определяемому физическому лицу, которые предоставляются другому лицу.

Правовое регулирование охраны таких данных осуществляется положениями Конституции Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, а также различными подзаконными актами. Однако, несмотря на такой большой объем правовой защиты, сейчас существуют две проблемы защиты персональных данных в интернете. Первая проблема - это утечка этих данных в Сеть, а вторая - это почти нереальная возможность добиться компенсации за вред, который был причинен такой утечкой. Решение этих двух проблем должно заключаться в устранении причин, которые их вызывают. Вследствие их устранения в Российской Федерации должен резко снизиться процент утечки персональных данных в сеть «Интернет».

Актуальные проблемы защиты персональных данных:

- Для установления личности субъекта персональных данных Законом «О персональных данных» установлены минимальные требования к обработке биометрических персональных данных. Однако вопрос в части информирования об утечке таких данных носит открытый характер, а это представляет существенную угрозу безопасности граждан. Массовые утечки персональных данных в России в последнее время существенно возросли.
- Правовой режим защиты метаданных находится в «серой зоне». Это обусловлено как минимум несколькими факторами: 1) сложностью самого регулирования технических процессов; 2) отсутствием заинтересованности в регулировании со стороны разработчиков программных продуктов; 3) возможностью получения информации

правоохранительными органами в упрощенном порядке. Обращение к российскому законодательству показывает, что сам термин «метаданные» в нем используется. Например, ст. 14 Федерального закона от 30 декабря 2015 г. № 431-ФЗ «О геодезии, картографии и пространственных данных и о внесении изменений в отдельные законодательные акты Российской Федерации» содержит указание на пространственные метаданные. Однако изучение иных документов показывает, что законодатель не видит большой разницы между пространственными данными и пространственными метаданными (и в том и в другом случае речь идет об информации, изложенной в виде файлов в формате XML, созданных с использованием XML-схемы).

– В Российской Федерации существует достаточно низкий размер административных штрафов для юридических лиц, которые в процессе своей деятельности допускают нарушение законодательства о защите персональных данных. Размер таких штрафов находится в диапазоне от 15 000 до 75 000 рублей. Только мелкому юридическому лицу может быть трудно заплатить такой административный штраф. Крупные юридические лица, продающие персональные данные, могут легко заплатить такой штраф. Для них это «издержки производства».
– У некоторых юридических лиц утечка персональных данных происходит из-за человеческого фактора. Он может проявляться в разных аспектах: сотрудники слабо понимают требования положений российского законодательства о персональных данных, сотрудники халатно относятся к исполнению своих должностных обязанностей, сотрудники выполняют требования закона «для галочки», а не по факту, сотрудники организаций сами продают персональные данные своих работников или клиентов каким-либо третьим лицам.

– Российским гражданам, которым был причинен какой-либо ущерб утечкой персональных данных, почти нереально добиться компенсации за это в судебном порядке от частных юридических лиц или государственных органов, допустивших утечку персональных данных. Следом иски можно вчинить и государственным органам, которые, несмотря на требования закона, весьма халатно относятся к защите персональных данных россиян.

При обработке персональных данных является факт того, что в силу недостаточного уровня защищенности и методов передачи или хранения больших объёмов данных нередки случаи хищения (утечки) персональных данных при содействии злоумышленников в открытый доступ. Данные ситуации характерны как для зарубежных IT компаний, так и для отечественных интернет-агрегаторов.

Совершенствование регулирования персональных данных в российском законодательстве:

– В Федеральном законе от 27.07.2006 № 152-ФЗ (ред. от 24.04.2020) «О персональных данных» необходимо закрепить точный перечень данных, которые относятся к персональным. Для этого можно использовать классификацию персональных данных, которая была разработана учеными-юристами, и закрепить ее в статье 3 вышеуказанного правового акта. Например, статья 3 Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 24.04.2020) «О персональных данных» может звучать так: «Персональные данные – информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу. К персональным данным относится следующая информация: Ф.И.О. человека, место регистрации и жительства, номер мобильного телефона, адрес электронной почты. Такие данные в большинстве своем известны не только их обладателю, но и каким-либо другим гражданам, политические взгляды, религиозная принадлежность, данные о

состоянии здоровья, подробности о судимостях человека, а также иная информация, признанная таковой судом, в рамках рассмотрения и разрешения дела».

- Для устранения причины низких административных штрафов необходимо попытаться увеличить их до таких размеров, чтобы нарушать положение закона было невыгодно. В Кодексе Российской Федерации об административных правонарушениях нужно закрепить дифференцированный подход к административным штрафам, чем выше оборот юридического лица, тем выше размер наказания.
- Необходимо донести до судов Российской Федерации, что права и свободы человека являются приоритетом в деятельности судов. Суды не должны заботиться об экономическом состоянии юридических лиц или государственных органов, которые допустили нарушение законодательства о персональных данных, которое привело к причинению вреда гражданину. Суд обязан рассмотреть и разрешить дело справедливо и не думать о том, какие последствия будут для «виновника» утечки персональных данных в случае вынесения решения суда не в его пользу. Сделать такое донесение можно посредством издания Верховным Судом Российской Федерации специального пленума, в котором бы были разъяснения, как следует применять положения всего комплекса российского законодательства о защите персональных данных.

В введении обозначена гипотеза «российское законодательство о персональных данных не совершенно, так как отсутствует точный перечень персональных данных; низкие штрафы не снижают количество нарушений в сфере персональных данных», которая в ходе исследования подтвердилась.

Список используемой литературы и используемых источников

1. Бачило, И.Л. Персональные данные в структуре информационных ресурсов. Основы правового регулирования /И.Л. Бачило, Л.А. Сергиенко, Б.А. Кристальный., А.Г. Арешев // Информационное право. - 2016. - № 3. - С. 50-55.

2. Бачило, ИЛ. Информационное право РФ : Учебник для вузов / И.Л. Бачило. - М.: Издательство Юрайт. 2016.- 522 с.

3. Бойкова О.Ф. Защита персональных данных: касается всех! Практическое пособие. Выпуск № 142 / Бойкова Ольга Феоктистовна. - М.: Либерея, 2018. - 950 с.

4. Болик, В.Н. О правомерности законодательных ограничений конституционного права на неприкосновенность частной жизни / В.Н. Болик., А.М. Туркиашвили А.М. // Законы России: опыт, анализ, практика. - 2015. - № 7. - С. 78 - 84.

5. Бондаренко, К.А. Взаимосвязь признаков индивидуального трудового договора и особенностей договорного регулирования трудовых отношений / К.А. Бондаренко // Трудовое право в России и за рубежом. 2015. — № 3. — С. 23 — 27.

6. Бондаренко, К.А. Взаимосвязь признаков индивидуального трудового договора и особенностей договорного регулирования трудовых отношений / К.А. Бондаренко // Трудовое право в России и за рубежом. 2015. - № 3. - С. 23 - 27.

7. Бондаренко, Э.Н. Конфиденциальная информация в трудовых отношениях. / Э.Н. Бондаренко, Иванов ДВ. - СПб.; Издательство «Юридический центр-Пресс». – 2014. - 213 с

8. Бурдов, С.Н. К вопросу о возможностях совершенствования нормативноправового режима конфиденциальной информации / С.Н. Бурдов // Государство и право. 2015. № 5. - С. 103-105.

9. Буркова А.Ю. Определение понятия "персональные данные" // Право и экономика. - 2015. - № 4. - С. 20 - 24

10. Буркова, А.Ю. Локализация баз данных на территории Российской Федерации: первые толкования // Законодательство и экономика. 2015.- № 9.- С. 59 - 64.

11. Буркова, А.Ю. Локализация баз данных на территории Российской Федерации: первые толкования // Законодательство и экономика. 2015.- № 9.- С. 59 - 64.

12. Власов Д.С. Защита персональных данных в автоматизированных системах обработки информации органов государственной власти // Успехи современной науки. 2016. Т. 8. - № 12. - С. 33-38.

13. Выговская, И.Г. Трудовое право России: учебник / И.Г. Выговская, С.В. Колобова, О.С. Королькова и др.; под общ. ред. М.В. Преснякова, С.Е. Чаннова. - Саратов: Поволжский институт управления им. П.Л. Столыпина, 2014.- 288 с.

14. Гадельшин А.А., Степанов М.М. СООКІЕ-ФАЙЛЫ как объект персональных данных и способ нарушения конфиденциальности персональных данных //Вопросы российской юстиции. 2021. - № 16. - С. 516-531.

15. Головина, С.Ю. Конституционные принципы и права в сфере труда и их конкретизация в трудовом законодательстве России // Российский юридический журнал. - 2015. - № 1. - С. 132 - 145.

16. Грибанов А.А. Определение персональных данных, разграничение операторов и обработчиков персональных данных //Судья. 2021. - № 4 (124). - С. 30-34.

17. Дроменко А.Ю. Информационные права граждан Российской Федерации и защита персональных данных в сети «Интернет» // Science Time. - 2016. - № 2 (26). - С. 203-206.

18. Дудко И.Г. Защита персональных данных кандидата в избирательном процессе // Проблемы права. - 2017. - № 5 (64). - С. 26-31.

19. Журавлев, М.С. Персональные данные в трудовых отношениях: допустимые пределы вмешательства в частную жизнь работника //

Информационное право. - 2017. - №4. - С. 35 - 38.

20. Загородников, С.Н. Чужие тайны и их защита: нормативно-правовые аспекты / С.Н. Загородников, Максимов Д.А. // Российский следователь. - 2014. - № 3.- С. 40.

21. Иванов А.А. Хранение персональных данных за рубежом с точки зрения российского права // Закон. - 2015. - № 1. - С. 134 - 143.

22. Исакова, Л.В. Международно-правовое регулирование защиты персональных данных работников / Л.В. Исакова, К.Е. Статуева // Экономика и право: Новый университет. - 2015. - № 4(50). - С. 93-95.

23. Катунцева М.О. Конституционное право на информацию и проблема защиты персональных данных в социальных сетях // В книге: Конституционные права и свободы человека и гражданина в РФ: проблемы реализации и защиты Материалы межвузовского студенческого круглого стола.- 2016. - С. 31-37.

24. Козин И.С. Метод определения опасности угрозы персональным данным при их обработке в информационной системе. // Известия СПбГЭТУ «Лэти». – 2017. – №10. – С. 19-26.

25. Коломыцев М.В., Носок С.А. Маскирование таблиц базы данных с использованием технологии SQL // Защита информации. – 2017. – №19. – С. 16-22.

26. Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)) // Собрание законодательства РФ. 04.08.2020. № 81.

27. Костомаров К.В., Качанова Е.А. Банк России в сфере защиты персональных данных клиентов коммерческих банков: экономический и юридический аспекты. Монография / Екатеринбург, 2015. - 321 с.

28. Кутенков Ю.И. Понятие персональных данных работника в российском трудовом праве // Азиатско-тихоокеанский регион: Экономика, политика, право. - 2015. - № 4 (37). - С. 116-133.

29. Лебедев, В.М. Трудовое право: Учебник / В.М. Лебедев, Д.В. Агашев, А.А. Белинин, А.В. Дворецкий; Под ред. В.М. Лебедева. - М.: Норма: НИЦ Инфра-М, 2018. - 464 с.

30. Мархгейм М.В., Никонова Л.И. Предвыборная агитация в сети Интернет: версии доктрины и динамизм практики // Научные ведомости БелГУ. Серия: Философия. Социология. Право. - 2018. - № 3. - С. 532-538.

31. Меликов У.А. Гражданско-правовая защита персональных данных // Вестник УрФО. Безопасность в информационной сфере. – 2015. – № 4 (18). – С. 49-53.

32. Минбалеев А.В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. - 2012. - № 2 (4). - С. 4-9.

33. О персональных данных: федеральный закон от 27.07.2006 № 152-ФЗ: ред. от 24.04.2020 // Собр. законодательства Рос. Федерации. - 2006. - № 31, ч. I, ст. 3451.

34. Об утверждении Перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 № 188: ред. от 13.07.2015 // Собр. законодательства Рос. Федерации. - 1997. - № 10, ст. 1127.

35. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012 № 1119 // Собр. законодательства Рос. Федерации. – 2012. - № 45, ст. 6257.

36. Павлова И.Ю. Соотношение правового регулирования банковской тайны и персональных данных гражданина в свете новелл законодательства о персональных данных //Государственная служба и кадры. - 2021. - № 3. - С. 43-47.

37. Салихов Д.Р. Пандемия и персональные данные: как распространение новой коронавирусной инфекции бросает новые вызовы персональным данным //Конституционное и муниципальное право. - 2021. - № 3. - С. 46-50.

38. Соловьев В.В. Улучшение защищенности распределенной информационной системы персональных данных на основе технологии VPN и терминального доступа // Информационные технологии и проблемы математического моделирования сложных систем. – 2017. – №18. – С. 39-44.

39. Терещенко, Л.К. Правовой режим персональных данных и безопасность личности /Л. К. Терещенко //Закон. -2018.- №6.- С. 37 -43. Трофимова, И.А. Обработка и хранение персональных данных/ И.А. Трофимова // Делопроизводство.- 2015. - № 3. - С. 107 - 110.

40. Уголовный кодекс Российской Федерации: Федеральный Закон Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 07.04.2020) // Собрание законодательства РФ. 17.06.1996. № 25.

41. Шумекеева Г. Б. Защита персональных данных как одна из проблем современного мира / Право: современные тенденции : материалы VI Междунар. науч. конф. (г. Краснодар, октябрь 2018 г.). - Краснодар : Новация, 2018. - С. 47-49.

42. Яковец, Е.Н. Своеобразие состава защищаемой конфиденциальной информации / Е.Н. Якрвец // Право и кибербезопасность. - 2014. - № 2. - С. 51 - 58.

43. Готовы ли пользователи рунета делиться персональными данными? - Текст: электронный // Цифровая экономика. 2021: [сайт]. - URL: https://issek.hse.ru/mirror/pubs/share/450608071.pdf (Дата обращения 25.06.2021)

44. В ФБК объяснили утечку базы сторонников Навального действиями бывшего сотрудника. - Текст: электронный // Телеканал Дождь: [сайт]. - URL: https://tvrain.ru/news/v_fbk_objasnili_utechku_bazy_storonnikov_navalnogo_dejstvijami_byvshego_sotrudnika-528437/(дата обращения: 24.11.2021).

45. Решение № 2-3916/2018 2-3916/2018~М-413/2018 М-413/2018 от 15 мая 2018 г. по делу № 2-3916/2018 [сайт]. - URL:

https://sudact.ru/regular/doc/1ue1oKQoWolE/ (Дата обращения 25.04.2022)

46. Решение № 2-1181/2018 2-1181/2018 ~ М-850/2018 М-850/2018 от 7 мая 2018 г. по делу № 2-1181/2018 [сайт]. - URL: https://sudact.ru/regular/doc/xtfN2dlh2rLw/ (Дата обращения 25.04.2022)

47. Решение № 2-822/2020 2-822/2020~М-80/2020 М-80/2020 от 3 января 2020 г. по делу № 2-822/2020 [сайт]. - URL: https://sudact.ru/regular/doc/oh0t7tlyzwoR/ (Дата обращения 25.04.2022)

48. Решение № 2-2652/2015 2-43/2015 2-43/2016 2-43/2016(2-2652/2015;)~М-2596/2015 М-2596/2015 от 3 февраля 2016 г. по делу № 2-2652/2015 [сайт]. - URL: https://sudact.ru/regular/doc/lveqLAe5hSJn/ (Дата обращения 25.04.2022)

49. Fleming P., Bayliss A.P., Gareth Edwards S., Seger C.R. The role of personal data value, culture and self-construal in online privacy behaviour //PLoS ONE. 2021. Т. 16. № 7 July. С. e0253568.

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

51. Kamalieva, L.A., Kazakova, I.A., Nikonovich, S.L., Goncharov, V.V., & Livson, M. (2020). Improving information security: criminal-legal means of counteracting digital data leakage. Laplage in Journal, 6 (Extra-A), p. 222-229. https://doi.org/10.24115/S2446-622020206Extra-A657p.222-229/ (дата обращения: 10.02.2021).

52. Mityushin D.A. Issues and possibilities of personal data remote processing in the covid19 pandemic environment //В сборнике: Software Engineering Application in Informatics. Proceedings of 5th Computational Methods in Systems and Software. Сер. "Lecture Notes in Networks and Systems. 232" 2021. С. 86-94.

53. Pavelek O., Zajíčková D. Personal data protection in the decision-making of the cjeu before and after the lisbon treaty //Baltic Journal of European

Studies. 2021. Т. 11. № 2. С. 167-188.

54. Nukusheva A., Ilyassova G., Kudryavtseva L., Popova L., Shayakhmetova Z., Jantassova A. Transnational corporations in private international law: Do kazakhstan and russia have the potential to take the lead? // Entrepreneurship and Sustainability Issues. 2020. Т. 8. № 1. С. 496-512.

55. European Commission, Factsheet on the "Right to Be Forgotten" ruling (C-131/12). Электронный ресурс // URL: https://ec.europa.eu/info/law/law-topic/data-protection_en (Дата обращения: 06.12.2021)