Министерство образования и науки Российской Федерации
Федеральное государственное автономное
образовательное учреждение высшего образования
«Российский государственный профессионально-педагогический университет»
Институт гуманитарного и социально-экономического образования
Кафедра документоведения, истории и правового обеспечения

К ЗАЩИТЕ ДОПУСКАЮ:
Заведующий кафедрой ДПО
_____М.Б. Ларионова
«___» _____ 20___г.

ПРАВОВАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профиля подготовки «Правоведение и правоохранительная деятельность»
профилизации «Административное право»

Идентификационный код ВКР: 105

Исполнитель:
студент группы Пу-411о АП В.Е. Чупин

Руководитель:
доцент кафедры ДПО,
канд. ист. наук С.Л. Разинков

Нормоконтролер:
ст. преподаватель кафедры ДПО С.Л. Разинков

Екатеринбург 2017

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Интенсивное развитие и внедрение в повседневную жизнь информационных технологий, появление новых форматов взаимоотношений между операторами и субъектами персональных данных (далее – ПД) определяют возникающую необходимость сохранения и поддержания тонкого баланса публичных и частных интересов. Значительный прогресс в развитии информационно-коммуникационных технологий и средств, формирующих информационное пространство, устанавливает обязанность государства создавать эффективные механизмы правовой защиты данной отрасли. В этой связи законодательство о ПД в современном обществе является необходимым инструментом в соблюдении основополагающих прав граждан.

Основные идеи о неприкосновенности частной жизни, ограничении оборота личной информации получили первоначальное распространение в Европе, а на сегодняшний день закреплены в международных нормативных актах и в национальном законодательстве Российской Федерации (далее РФ). Так, Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ)[1] (далее Конституция РФ) в ст. 23 содержит необходимую в демократическом обществе меру, направленную на неприкосновенность частной жизни. Постоянное повышение требований к обеспечению безопасности ПД личности, высокой степени их защиты, является приоритетным направлением политики любого правового государства.

Актуальность темы определяется сложностью регулирования оборота ПД в информационном пространстве. В связи с необходимостью каждого человека на протяжении жизни вступать в отношения с различными

[1] Собрание законодательства РФ. 2014. № 31. Ст. 4398

операторами ПД, при этом, у последних накапливаются важная личная и особо чувствительная информация о человеке, незаконное использование которой приводит к нежелательным для индивида последствиям. Особое внимание следует уделять мерам по защите колоссального объема ПД в социальных сетях. Личная информация, которую пользователь делает общедоступной в социальной сети подвергается сбору и систематизации различными органами и организациями, а правовой режим защиты этих данных пока только формируется. Контроль потоков персональной информации, понимание её истинной ценности является необходимым знанием как для субъекта персональных данных, так и для оператора.

Сейчас технологии позволяют с большой скоростью передавать данные по всему миру. В связи с этим повышаются риски утечки информации, попадание ее в недобросовестные руки. На долю хищения персональных данных приходится 64% всех утечек данных. К примеру, в первом полугодии 2016 года это 621 инцидент, в результате которых было украдено более 294 миллионов записей персональных данных (53% всех похищенных или потерянных записей данных).[1] Так же, проводимое исследование компании Google с июля 2014 по июнь 2015 года обнаружило неутешительные выводы, это 760 935 фактов взлома 313 190 сайтов.[2]

Проблемы становления и практики применения Законодательства о ПД являются предметом многих научных исследований российских учёных. Среди них можно выделить работы А.И Савельева, А.А Иванова, Е.В. Тереховой, посвященные проблемам трансграничной обработки, защиты ПД в сети интернет. Исследования, проведенные вышеперечисленными авторами, показывают коллизионность, избирательность правоприменения нормативных актов в сфере оборота ПД. Особо тщательно и кропотливо

[1] Утечки данных в 2016 году – предварительные итоги года [Электронный ресурс]. URL: https://habrahabr.ru/company/gemaltorussia/blog/314352/ (дата обращения: 01.05.2017).

[2] Remedying Web Hijacking: Notification Effectiveness and Webmaster Comprehension [Электронный ресурс]. URL: http://dl.acm.org/citation.cfm?id=2883039 (дата обращения: 02.05.2017).

рассматривается вопрос о сверхимперативности, отсутствии правовой дефиниции понятий законодательства о ПД в трудах А.Ю. Бурковой, Бычкова А.И, Н.В. Власовой, В.Б. Наумова, В.В. Архипова. Проблемам недостаточно эффективных административных мер, идентификации в государственных информационных системах, законодательного регулирования данных в социальных сетях посвящены работы Л.К. Терещенко, М.В. Залоило, Р.В. Амелина. Следует подчеркнуть, что отмеченные ранее труды исследователей охватывают множество вопросов, однако с учетом динамично развивающегося законодательства в сфере ПД, можно отметить быструю потерю актуальности трудов правоведов.

Объектом исследования данной работы являются правоотношения, касающиеся защиты ПД в информационном пространстве.

Предметом исследования являются нормы международного и национального права, а так же судебная практика, регулирующая оборот ПД в РФ.

Целью работы является определение действующих проблем правового регулирования в области защиты оборота ПД в информационном пространстве РФ и проектирование дальнейшего его развития.

Для достижения цели, в работе поставлены следующие задачи:

1. Изучить становление и охарактеризовать актуальное законодательство о ПД;

2. Рассмотреть основные проблемы правового регулирования защиты ПД в информационном пространстве РФ;

3. Исследовать перспективы развития законодательства о ПД в РФ.

В работе помимо общенаучных (анализ, синтез, сравнение) используются методы: сравнительно-правовой (применялся при обращении к зарубежной практике правовой защиты ПД), статистический (позволил провести анализ количественных сведений о жалобах граждан в Роскомнадзор по поводу нарушения законодательства о ПД), комплексного анализа нормативных правовых актов.

1. ОБЩАЯ ХАРАКТЕРИСТИКА ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1. Становление законодательства о персональных данных

Понятие персональных данных ПД, информации, позволяющей установить личность, и подобные им возникли в различных правовых системах во второй половине XX в. в связи с появлением информационно-телекоммуникационных технологий, прежде всего сети Интернет. Проблема правового регулирования ПД на современном этапе становится одной из системных проблем правового регулирования отношений в этой сфере, наряду с проблемами идентификации пользователей, определения юрисдикции и ответственности информационных посредников.[1]

Огромную роль в становлении и формулировании права на частную жизнь сыграла деятельность американских судов. Так, в 1965 г. в деле Griswold v. Connecticut судья Верховоного суда США Дуглас вывел «право на прайвеси» из первых пяти поправок к Конституции США, признав, что эти поправки «охраняют различные аспекты неприкосновенности частной жизни». Широко известны слова, которые он произнес, резюмируя решение суда: «Мы имеем дело с правом на неприкосновенность частной жизни, которое старше, чем Билль о правах»[2].

Предупреждая бурное развитие информационных технологий и в том числе автоматизированной обработки данных, Совет Европы еще в 1981 г. принял «Конвенцию о защите физических лиц при автоматизированной обработке персональных данных» (далее Конвенция № 108).[3] Главными идеями Конвенции являлись разработка фундаментальных принципов

[1] Наумов В.Б., Архипов В.В. Понятие персональных данных: интерпретация в условиях развития информационно-телекоммуникационных технологий // Российский юридический журнал. 2016. № 2. С. 186-196.

[2] Развитие законодательства о защите персональных данных [Электронный ресурс]. URL: http://www.smartmanage.ru/deels-430-1.html (дата обращения: 01.06.2017).

[3] Собрание законодательства РФ. 2014. № 5. Ст. 419.

обработки информации, установление гарантий защиты данных субъектов, утверждение правил трансграничного потока информации.

Европейская модель защиты ПД наряду с государствами членами Европейского союза объединяет страны, в которых действует Конвенция №108. На их законодательство о ПД существенное влияние оказали правовые акты Европейского союза, в частности в Директива Европейского Союза и Парламента 95/46/ЕС от 24 октября 1995 г. «О защите прав частных лиц применительно к обработке персональных данных и свободном движении таких данных»[1] и Директива 97/66/ЕС от 15.12.97 «Касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций».[2]

В данных актах были определены основные принципы организации обработки данных личного характера и обеспечения права граждан на защиту ПД. Такие как:

- данные персонального характера должны быть собраны только для определенных целей и в строгом соответствии с законом;

- данные должны соответствовать требованиям, быть точными, полными и вовремя обновленными;

- цели, для достижения которых собираются и обрабатываются ПД, должны быть определены и утверждены до начала деятельности и использоваться только в этих целях;

- в системах учета ПД должны быть внедрены механизмы, предотвращающие потери или неправильное (или злоумышленное) использование ПД;

- деятельность организаций (как государственных, так и частных), имеющих базы данных, содержащих ПД, должна быть открытой;

---

[1] Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» [рус., англ.] (Принята в г. Люксембурге 24.10.1995).

[2] Директива 97/66/ЕС от 15.12.97 «Касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций» // Официальный журнал ЕС. Раздел С 200. 1994. 22 июля. С. 4.

- держатели данных должны быть подконтрольными для обеспечения соблюдения настоящих принципов, для этих целей должно быть предусмотрено создание независимого контролируемого органа как важного элемента защиты личности при автоматизированной обработке информации личного характера.

Исходя детальности регулирования Европейскими актами оборота ПД, можно смело говорить о важности практики иностранных государств по правовой защите информации о неприкосновенности частной жизни, в вопросах защиты компьютерных баз данных и свободы информации. Такая практика, в большей степени, разработана в странах континентальной Европы (особенно в Германии) и в меньшей - в Канаде и Соединенных Штатах.[1]

В РФ законодательство о ПД имеет более короткую историю, чем в европейских странах, однако приведение в соответствие внутреннего законодательства международному длилось долго и имело большое количество подводных камней. Так еще в 1995 году Комитет ООН по правам человека настоятельно рекомендовал РФ принять специальное законодательство о защите частной жизни «с целью предотвращения нарушений права на защиту от незаконного или произвольного вмешательства в личную и семейную жизнь и посягательств на неприкосновенность жилища и тайну корреспонденции».[2] Хотя Конституция РФ на момент проверки уже имела положения, защищающие неприкосновенность частной жизни (ст. 23, 24), рекомендации комитета ООН касались практического применения законов. В области защиты частных интересов предлагалось выстроить отдельные законодательные акты, гарантирующие исполнение международных положений.

---

[1] Параскевов А.В., Левченко А.В., Кухоль Ю.А. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом // Научный журнал КубГАУ. 2015. № 110. С. 866-894.

[2] Майоров А.В., Поперина Е.Н. Формирование и развитие права на неприкосновенность частной жизни // Юридическая наука и правоохранительная практика. 2012. № 3. С. 34-38.

Конвенция № 108 была подписана РФ 7 ноября 2001 года, ратифицирована в 2005 году, а вступила в силу лишь с 1 сентября 2013 г. Конвенция №108 предполагала, что страна, подписавшая документ, предъявляет собственные технические требования к защите персональных баз данных своих контролёров (операторов), обрабатывающих ПД. Для реализации Конвенции №108, страна должна принять закон о ПД, который эти требования закреплял. Так, во время работы над встраиванием положений Конвенции в российское законодательство, был составлен законопроект ныне действующего Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017) «О персональных данных» (далее ФЗ № 152).[1]

В действующей редакции, ФЗ №152 определяет основные принципы и условия обработки персональных данных, регулирует отношения, связанные с обработкой персональных данных, осуществляемой как государственными и муниципальными органами власти, так и юридическими и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях.[2] Сфера действия ФЗ № 152, в соответствии с п.1 ст.1 охватывает отношения по обработке персональных данных с использованием и без использования автоматизированных средств, если обработка позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

Анализируя сегодняшнее состояние законодательства о ПД в РФ, необходимо отметить появление новых вызовов и угроз, возникающих вследствие интенсивного развития и внедрения в повседневную жизнь информационных технологий. Перспектива развития законодательства о ПД

[1] Парламентская газета. 2006. 03 августа.

[2] Савельев А.И. Электронная коммерция в России и за рубежом: правовое регулирование. 2-е изд. М.: Статут, 2016. 640 с.

в РФ находится в рамках регионального и международного сотрудничества с уполномоченными органами иностранных государств в целях обмена положительным практическим опытом и его последующего внедрения на национальном уровне, сравнительного анализа действующего законодательства и положительного опыта отдельных иностранных государств и подготовка на их основе предложений по внесению изменений в законодательство РФ в области ПД.

1.2. Регламентация защиты персональных данных

Целью законодательства о ПД в первую очередь является обеспечение защиты прав и свобод человека и гражданина как субъекта ПД в соответствии с основными правоустанавливающими законодательными актами. В целях защиты прав граждан в области ПД, РФ с учетом трансграничности потоков ПД, в первую очередь обеспечила имплементацию в российское законодательство требований общеевропейского права, создала систему защиты прав субъектов ПД, соответствующую основным принципам, заложенным в межгосударственных нормативных правовых актах в области ПД.[1]

Законодательство РФ в области ПД, с учетом проведенных мероприятий по совершенствованию и гармонизации его положений, почти в полном объеме повторяет основные положения международных актов.

ФЗ №152 фактически является логическим продолжением Конституции РФ и более детально регламентирует нормы о правах субъекта персональных данных. В текущей редакции, ФЗ №152, согласно п.1 ст.3 относит к ПД любую информацию, относящуюся прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Как

[1] Федеральный закон «О персональных данных»: научно-практический комментарий (постатейный) / под ред. А.А. Приезжевой. М.: Редакция «Российской газеты», 2015. Вып. 11. С. 176.

показывает судебная практика, суды, наряду с определением ПД, в обоснование своего решения часто ссылаются на Указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»[1], в котором ст.1 определяет понятие ПД как «сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях».

ФЗ № 152, согласно ст. 8, 10, 11 выделяет несколько особых категорий ПД, среди них:

1. Специальные (касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни)

2. Биометрические (характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность)

Для обработки таких данных о личности, закон обязует оператора получать письменное согласие от субъекта ПД. Базовые принципы государственной регламентации оборота ПД заложены в ст. 5 ФЗ №152:

1. Обработка ПД должна осуществляться на законной и справедливой основе.

Данная норма является первым и важным постулатом обработки ПД, поскольку любые действия с ПД должны основываться на законах, т.е. на установленных государством обязательных правилах и норм общественного поведения.

2. Обработка ПД должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПД, несовместимая с целями сбора ПД.

[1] Российская газета. 1997. 14 марта.

Данный пункт предусматривает информированное согласие субъекта на обработку ПД. Личная информация, получаемая от субъекта ПД, должна ограничиваться целью обработки, оператор не должен собирать избыточные сведения по отношению к заявленным целям их обработки.

3. Не допускается объединение баз данных, содержащих ПД, обработка которых осуществляется в целях, несовместимых между собой.

В одной системе не должны обрабатываться совершенно разнородные данные, объединение которых влечет за собой нарушение закона. Не допускается смешение, соединение ПД, собранных и обрабатываемых в разных целях.

4. Обработке подлежат только ПД, которые отвечают целям их обработки.

Для достижения поставленных целей оператор прибегает к обработке тех ПД, которые собраны для достижения определенных задач и целей. Например, работодатель обрабатывает ПД работников, состоящих с ним в трудовых отношениях, а также лиц, состоящих с ним в гражданско-правовых отношениях.[1]

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

Часто операторы ПД собирают сведения, не относящиеся к заявленным целям обработки, примером данного правонарушения может послужить Решение Куйбышевского районного суда г. Омска по делу 12-283/2011[2] от 21.09.2011 г. по жалобе ОАО Омское ипотечное агентство на постановление мирового судьи судебного участка № Центрального АО Чернышевой Е.А., которым привлечено к ответственности по ст. 13.11 Кодекса

[1] Российская газета. 1997. 14 марта.

[2] Решение по делу 12-283/2011 от 21.09.2011 [Электронный ресурс]. URL: https://rospravosudie.com/court-kujbyshevskij-rajonnyj-sud-g-omska-omskaya-oblast-s/act-513897244/ (дата обращения: 13.06.2017).

Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 17.04.2017)[1] (далее КоАП РФ) РФ: «Судом установлено, что ОАО «Омское ипотечное агентство» нарушает обязательные требования при обработке специальных категорий персональных данных, а именно включает в заявления-анкеты на ипотечный кредит и заявления-анкеты на кредит избыточные сведения о судимости. Также данные сведения противоречат сведениям о персональных данных, которые может обрабатывать кредитная организация».

6. При обработке ПД должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПД. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных. Установление данной обязанности оператора направлено на защиту прав субъекта персональных данных и находит свое дальнейшее развитие в иных положениях комментируемого в ст. 18, 18.1, 19 ФЗ №152.

7. Хранение ПД должно осуществляться в форме, позволяющей определить субъекта ПД, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения ПД не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПД. Обрабатываемые ПД подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Примечательно, что впервые данный пункт получил общественную огласку и отражение в европейском законодательстве после решения

[1] Собрание законодательства РФ. 2002. № 1 (ч. 1). Ст. 1.

Европейского суда об имплементации принципа о праве «быть забытым».[1] гражданин Испании Марио Костеха Гонсалес, выигравший в мае 2014 г. дело против Google в Европейском Суде. Гонсалеса не устраивало то, что поисковая система Google выдавала по запросу с его именем ссылку на статью 1998 г. в газете La Vanguardia. Там говорилось о том, что из-за долгов ему пришлось продать дом, помещенный под залог. Испанец, посчитавший эту информацию неактуальной, добился удаления ссылки из выдачи Google через государственное агентство по защите данных. Право на «забвение» так же содержится в национальном законодательстве РФ. Так, ст. 10.3 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 06.07.2016) «Об информации, информационных технологиях и о защите информации»[2] (далее ФЗ № 149) содержит обязанность оператора поисковой системы, по требованию гражданина, прекратить выдачу неактуальных, недостоверных и утративших значение сведений.

В соответствии с ст. 4 ФЗ №152, законодательство о ПД в первую очередь основывается на Конституции РФ и международных договорах. Так, согласно положениям ст. ст. 23 и 24 Конституции РФ каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени; сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается, а органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Некоторые нормы, определяющие отдельные случаи регулирования обработки ПД, содержатся в кодифицированных федеральных законах. Так,

[1] Judgment in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González [Электронный ресурс]. URL: http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065 (дата обращения 10.06.2017).

[2] Российская газета. 2006. 29 июля.

Ст. 85-90 Трудового кодекса Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.01.2017)[1] регулируют защиту ПД работника. Жилищный кодекс Российской Федерации от 29.12.2004 № 188-ФЗ (ред. от 28.12.2016) (с изм. и доп., вступ. в силу с 01.01.2017)[2] в п.16 ст. 155 регулирует согласие на обработку ПД жильцов. Также ст. 85.1 Воздушного кодекса Российской Федерации от 19.03.1997 № 60-ФЗ (ред. от 06.07.2016)[3] регулирует порядок передачи персональных данных пассажиров воздушных судов в автоматизированные централизованные базы персональных данных о пассажирах.

Вышеуказанные нормативные акты не являются исчерпывающими. Иными федеральными законами так же регулируется оборот ПД в медицинской, информационной и оперативно-розыскной деятельности и т.д.

В соответствии со ст. 24 ФЗ № 152, виновные в нарушении требований указанного Закона, несут предусмотренную законодательством РФ ответственность. Поскольку указанная норма является отсылочной, то установление конкретных видов правонарушений и применение соответствующих мер ответственности регулируются иными нормативными актами.

Основной и наиболее распространенной формой ответственности за нарушение положений законодательства о персональных данных является административная ответственность. КоАП содержит несколько составов, применимых к нарушениям в указанной сфере:

1) ст. 13.11 КоАП РФ: нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных), предусматривающая ответственность в виде предупреждения или наложения штрафа на граждан - в размере от 300

[1] Парламентская газета. 2002. 05 января.
[2] Российская газета. 2005. 12 января.
[3] Российская газета. 1997. 26 марта.

до 500 руб.; на должностных лиц - от 500 до 1 тыс. рублей; на юридических лиц - от 5 тыс. до 10 тыс. рублей.

2) КоАП РФ предусматривает также ответственность граждан и должностных лиц за нарушение правил защиты информации (ст. 13.12 КоАП РФ), за разглашение информации с ограниченным доступом (ст. 13.14 КоАП РФ), а также ответственность должностных лиц за отказ в предоставлении информации (ст. 5.39 КоАП РФ).

Нецелевая обработка персональных данных может повлечь также уголовную ответственность. Так, ст. 137 Уголовного кодекса Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 04.03.2013)[1] предусматривает уголовную ответственность за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Статья 272 УК РФ устанавливает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, в том числе баз ПД.

Необходимо отметить, что в настоящее время меры ответственности за нарушение законодательства о защите ПД «разбросаны» по различным отраслям законодательства - административному, уголовному, трудовому. При этом ни в одной отрасли они пока не систематизированы должным образом, не выделены в отдельную группу как правонарушения, посягающие на конкретный вид общественных отношений. Наиболее частой является практика применения административных мер к нарушителю законодательства о ПД, однако многие исследователи отмечают слабость превентивной функции административной санкции и вследствие этого, частую практику «сознательного правонарушения» операторов ПД.

[1] Собрание законодательства РФ. 1996. № 25. Ст. 2954.

1.3. Структура и полномочия государственных органов в области защиты персональных данных

С вступлением в законную силу ФЗ №152 полномочия по защите прав субъектов ПД были возложены на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций[1] (далее - Роскомнадзор). Сегодня Роскомнадзор является федеральным органом, осуществляющим государственный контроль и надзор за исполнением принимаемых Федеральным Собранием РФ законодательных актов в области ПД.

В своей деятельности, Роскомнадзор руководствуется положениями Конституции РФ, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и Правительства Российской Федерации, международными договорами Российской Федерации, нормативными правовыми актами Министерства связи и массовых коммуникаций Российской Федерации.[2] Роскомнадзор, в порядке административного судопроизводства, вправе обращаться в суд в целях защиты прав субъектов ПД, в том числе неопределенного круга лиц, в соответствии с п. 5 ч. 3 ст. 23 ФЗ № 152.

Следует обратить внимание, что согласно п. 9 ч. 3 ст. 23 ФЗ №152 уполномоченный орган по защите прав субъектов ПД имеет право привлекать к административной ответственности лиц, виновных в нарушении требований данного Закона, однако п. 58 ч. 2 ст. 28.3 КоАП РФ не наделяет Роскомнадзор полномочиями по составлению протоколов об

[1] О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с "Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций"): Постановление Правительства РФ от 16.03.2009 № 228 (ред. от 01.07.2016) // Российская газета. 2009. 24 марта.

[2] Передня В.А. Защита персональных данных в информационно-телекоммуникационной сети международного информационного обмена // Юридический мир. 2013. № 6. С. 13-16.

административных правонарушениях, предусмотренных ст. 13.11 КоАП РФ. Данный состав относится к исключительной компетенции прокурора (ст. 28.4 КоАП РФ). Как результат, Роскомнадзор при выявлении указанных правонарушений направляет материалы для возбуждения дела об административном правонарушении прокурору.

В соответствии с ст. 1.2, КоАП РФ среди главных задач законодательства об административных правонарушениях находятся

1. Охрана прав и свобод человека и гражданина
2. Предупреждение административных правонарушений.

Как показывает практика, исполнение вышеуказанных задач административного права в сфере персональных данных представляется не совсем успешным. По статистике представленной Роскомнадзором в 2015 г. каждая вторая проверка оператора выявляет нарушения. Так, при проведении 461 плановой проверки, что составляет 52% от проведенных плановых проверок, было выявлено 1 397 нарушений. Количество выявленных нарушений при проведении плановых проверок в 2015 году на 37% больше числа выявленных нарушений в 2014 году.[1]

Срок давности привлечения к административной ответственности за нарушения в области обработки персональных данных в соответствии с ч.1 ст. 4.5 составляет 3 месяца. С точки зрения правоприменения такого временного отрезка недостаточно для привлечения к ответственности всех нарушителей. На протяжении нескольких лет в отчетах Роскомнадзора отслеживается низкий показатель подтверждения жалоб пользователей (только по 7% жалоб суд выносит положительное решение).

Несмотря на то, что в остальных случаях также имелось фактическое нарушение закона, к злоумышленникам не удалось применить соответствующее наказание в связи с истечением срока давности. В связи с

[1] Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2015 год [Электронный ресурс]. URL: https://rkn.gov.ru/docs/Otchet_ZPD_rus2015.pdf (дата обращения: 17.05.2017).

этим представляется разумным возложить полномочия по возбуждению административного производства по ст. 13.11 КоАП РФ также и на уполномоченный орган по защите прав субъектов ПД. Такой механизм сотрудничества Роскомнадзора, правоохранительных органов и прокуратуры позволит обеспечить реализацию принципа неотвратимости наказания и одновременно предотвратить значительное число нарушений в будущем.[1]

Усовершенствование системы защиты прав и законных интересов субъектов ПД, а также повысить эффективность осуществления государственного контроля (надзора) в области ПД помогут изменения в административное законодательство в части консолидации административных полномочий в рамках одного ведомства - Роскомнадзора. В настоящее время в рамках Федерального закона от 07.02.2017 N 13-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»[2] из п.1 ст. 28.4 КоАП исключается возбуждение дел об административных правонарушениях прокурором по ст. 13.11. Следовательно, полномочия по возбуждению дел об административных переходят к Роскомнадзору с 1 июля 2017 г.

В целом рассмотренные положения ФЗ №152 и КоАП РФ следует считать существенным шагом в развитии правовых основ информационного общества и электронного государственного управления, формирующихся в стране. Вместе с тем следует отметить малоэффективность положений КоАП, которые могут негативно повлиять на обеспечение информационной безопасности граждан, общества и государства. Несмотря не несовершенство законодательной базы, регламентирующей защиту ПД, учитывая возможность применения мер принуждения контролирующими органами, можно утверждать о том, что предложенная система контроля и надзора за

[1] Туркиашвили А.М. Защита персональных данных личности как информационная функция современного государства // Современный юрист. 2013. № 4. С. 110-123.

[2] Парламентская газета. 2017. 16 февраля. (начало действия документа – 01.07.2017).

реализацией прав субъектов персональных данных может функционировать достаточно эффективно. Для дальнейшего рассмотрения проблемных вопросов правового регулирования обработки персональных данных целесообразно перейти ко второй главе работы.

2. ПРОБЛЕМЫ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Исполнение законодательства о персональных данных в сфере оказания государственных услуг

Политика многих государств, в том числе и РФ, направлена на стимулирование развития информационно-телекоммуникационных технологий в интересах общества и государства. Реализуются проекты электронного государства, электронного правительства, электронного правосудия, формируется сфера электронных услуг. В настоящее время ПД граждан находятся в различных информационных системах и базах данных и обрабатываются во всех сферах государственного и муниципального управления: налоговой службой, службой занятости, ПФР, ФФОМС, органами загса и т.д.[1] Предоставление государственных услуг в электронной форме повышает их доступность, минимизирует коррупционные риски и обеспечивает экономию бюджетных средств.

Тщательное исследование вопроса обработки персональных данных в сфере гос. и муниципальных услуг обуславливается необходимостью идентификации личности для оказания услуги, а, следовательно, неизбежной обработки ПД индивида. В связи с данной необходимостью законодатель выделяет особенности обработки ПД в государственных или муниципальных информационных системах ПД (Ст. 13, пп. 4 п.1 ст.6 ФЗ № 152).

Обработка осуществляется в силу выполнения возложенных на тот или иной орган государственной или муниципальной власти функций для достижения законных целей и в пределах его полномочий. Когда обработка ПД необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27.07.2010 № 210-ФЗ (ред.

[1] Федеральный закон «О персональных данных»: научно-практический комментарий, М.: Редакция «Российской газеты», 2015. Вып. 11. 176 с.

от 28.12.2016) «Об организации предоставления государственных и муниципальных услуг» [1], для обеспечения предоставления такой услуги, для регистрации субъекта ПД на едином портале государственных и муниципальных услуг, согласие субъекта ПД на обработку указанной информации не требуется.

Статьей 6 ФЗ №152 определены условия обработки персональных данных, в том числе указаны случаи, когда допускается обработка ПД без согласия на это субъекта ПД, среди которых и получение госуслуги. Из буквального толкования названной нормы следует, что каждый из таких случаев является самостоятельным основанием обработки персональных данных.

В науке административного права ставится вопрос о необходимости исследования идентификации различных лиц, как и других объектов материального мира в целях повышения эффективности государственного управления. Только идентификация человека, определение его социального и правового положения позволяют государственным служащим и иным должностным лицам предпринять все необходимые меры по защите его прав и интересов, определяемых его статусом. Наличие прав в свою очередь, влечет за собой и обязанность предоставить идентификатор для подтверждения своего социального статуса. «С операционной точки зрения можно считать, что «первичную» идентификацию граждан осуществляют уполномоченные органы государственной власти и государственные учреждения. Они же выдают гражданину документ, удостоверяющий личность. Это документ выступает идентификатором физического лица, несущим информацию о его уникальных признаках. Личная фотография в документе, удостоверяющем личность, иные биометрические данные дают возможность другим лицами и организациям проводить «вторичную» идентификацию, сверяя фотографию в паспорте с внешностью его

[1] Российская газета. 2010. 30 июля.

предъявителя можно установить, принадлежит ли паспорт предъявителю. В случае положительного ответа личные данные отождествляются». Таким образом, к существующим проблемам идентификации в информационных системах относятся

1. Ручная обработка информации
2. Личное присутствие субъекта

Будущее стандарта идентификации в информационных системах представляется в машинном формировании и обработке заявок и удаленной идентификации посредством использования уже имеющихся у пользователей идентификаторов и проверки сведений пользователя самой информационной системой через запросы в соответствующие базы данных.

Проблема идентификации в информационных системах стояла еще при обсуждении проекта ФЗ №152 в 2006 г. Так в интервью депутата Госдумы Александра Чуева информационному агентству «REGNUM» были затронуты вопросы идентификации физических лиц.

1. «Владимир Путин в своем заключении на законопроект рекомендовал исключить положения о присвоении каждому физическому лицу идентификаторов персональных данных и о создании государственного регистра населения, содержащего эти идентификаторы.

2. «Это (идентификаторы) очень опасная вещь, потому что если номер человеку присваивается извне, то фактически это возможность ограничить права и свободы человека извне. Если вдруг этого номера у вас не окажется либо этот номер потеряется, либо система учета даст сбой, либо под этим номером окажутся не ваши, а чужие персональные данные, то вы будете абсолютно беспомощны в изменении этой ситуации - ведь номер себе присваивали не вы сами, а кто-то извне».[1]

[1] «Идентификатор персональных данных – это возможность ограничить права человека извне»: интервью депутата Госдумы Александра Чуева ИА REGNUM [Электронный ресурс]. URL: https://regnum.ru/news/602047.html (дата обращения: 20.06.2017).

Стремление законодателя к идентификации вызвано улучшением административного взаимодействия граждан с государством, однако само понятие идентификации не было отражено не в одной из редакций ФЗ №152. В дефинитивной части ФЗ №152 при определении ПД от термина «идентификация», общепринятого в российском и международном информационном праве. Вместо него использованы понятия «определенное лицо» и «определяемое лицо».[1]

Решение проблемы идентификации лежит в технической плоскости (появление инструментов, позволяющих выполнять такую идентификацию максимально просто для пользователя Интернета и с максимальной безопасностью для обеих сторон коммуникации) и правовой (признание подобных действий).

В ряде стран государство пошло по пути выдачи гражданам страны ключей электронных подписей, а за счет объединения с соответствующими электронными идентификационными картами каждый гражданин получил, по сути, возможность идентифицировать себя в электронных коммуникациях. Такой подход был избран в Бельгии, Испании, Франции, Эстонии и др. В некоторых странах государство привлекает граждан к приобретению электронных подписей путем предоставления им бесплатных ключей подписи (Дания, Австрия, Испания), не навязывая его в принудительном порядке.

Сегодня можно назвать лишь три развитые страны мира, которые используют универсальный идентификатор личности (Швеция, Бельгия, США).[2] Анализируя зарубежный опыт, при использовании универсальных карт, выделяются проблемы

[1] Соколова О. С. Проблемы реализации Федерального закона «О персональных данных». Современное право. М., 2006. С. 37-41.

[2] Брауде-Золотарёв, М. Ю., Сербина, Е. С., Негородов, В. С., Волошкин, И. Г. Персональные данные в государственных информационных ресурсах. М.: Издательский дом «Дело» РАНХиГС, 2016. 56 с.

1. Нарушения права на неприкосновенность частной жизни. (Создание регистра населения, консолидация в одном источнике данных о здоровье, интимной жизни, вероисповедании и т.д.)

2. Угрозы утечки или кражи ПД (открытый доступ государственных служащих, привлекательность скопления большого количества актуальных ПД субъектов для злоумышленника).

3. Высокие издержки контроля над использованием ПД.

В РФ была попытка выдачи универсальной электронной карты (УЭК), которая позволяла бы получать все государственные и муниципальные услуги, оказываемые в электронной форме согласно законодательству РФ. Однако согласно ст. 4 Федерального закона от 28.12.2016 № 471-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» проект был завершен. В период выдачи УЭК с 2012 по 2015г. наблюдались массовые случаи отказа населения от УЭК. Всего в этот период УЭК получили лишь 0,33% всего населения.

Для сравнения, количество банковских карт, выданных кредитными организациями за аналогичный период (с 01.01.2013 по 1.07.2015), составляет 42,6 миллиона единиц.[1]

Основные результаты исследования таковы отказа от УЭК таковы:

1. УЭК предоставляет своему владельцу минимальный функционал (в том числе по сравнению с банковскими, региональными социальными картами).

2. УЭК пользуется чрезвычайно низкой востребованностью у граждан.

[1] Принят закон, упраздняющий УЭК [Электронный ресурс]. URL: http://d-russia.ru/prinyat-zakon-uprazdnyayushhij-uek.html (дата обращения: 07.06.2017).

3. Выпуск и поддержание инфраструктуры УЭК влечет затраты, несопоставимые с социальным и экономическим эффектами ее использования.

4. Обязательность изготовления в 2017 году для всех граждан Российской Федерации повлечет значительные затраты для региональных бюджетов (40-90 миллиардов рублей), при этом велик риск неэффективного использования бюджетных средств вследствие массового отказа граждан от уже выпущенных УЭК или неиспользования их по различным причинам.[1]

В случае появления нового универсального идентификатора в РФ, представляется, что он должен относиться к категории ПД, требующих повышенную защиту. Использование идентификаторов должно быть жестко ограничено целями их создания и не должно трактоваться расширительно, делая возможным использование сбор и хранение идентификатора иными субъектами, кроме органов государственной власти или правомочными операторами, в иных, не оговоренных заранее, целях.

2.2. Административный контроль оборота персональных данных в социальных сетях

На сегодняшний день социальные сети являются мощнейшим инструментом для различных коммуникаций, продвижения товаров и услуг. Особое значение имеет проблема отсутствия единых стандартов защиты персональных данных в социальных сетях. Национальные законодательства различных стран предусматривают различную степень защиты персональных данных. В связи с этим у пользователя зачастую отсутствует возможность

[1] Принят закон, упраздняющий УЭК [Электронный ресурс]. URL: http://d-russia.ru/prinyat-zakon-uprazdnyayushhij-uek.html (дата обращения: 07.06.2017).

достоверно оценить уровень защиты персональных данных, на который он может рассчитывать, предоставляя свои персональные данные.[1]

Любая социальная сеть предполагает предоставление ей некоторых сведений о зарегистрированном пользователе. Если человек указывает действительные сведения о себе, то вносит в данную информационную систему свои персональные данные.[2] Важно отметить, что социальные сети дают возможность ограничений, оставляя досуп только для выбранной категории пользователей, но любой сайт, при регистрации, требует информцию в виде ФИО, адрес почты, а иногда и дату рождения и т.п.

Часто пользователь социальной сети, кроме «обычных» данных при регистрации и действиях в соц. Делает общедоступной «особо чувствительную» информацию. К ней, согласно п. 1 ст. 10. ФЗ №152 относятся специальные категории персональных данных, т.е данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Объем сбора информации о пользователе очень обширный. На примере социальной сети «Вконтакте», согласно п. 4.2 правил защиты информации о пользователях сайта VK.com, включает:

1. Данные о технических средствах (устройствах), технологическом взаимодействии с Сайтом (в т.ч. IP-адрес хоста, вид операционной системы пользователя, тип браузера, географическое положение, поставщик услуг Интернета, данные из адресной книги, данные, полученные в результате доступа к камере, микрофону и т.п. устройств), и последующих действиях Пользователя на Сайте.

---

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

[2] Защита персональных данных в социальных сетях [Электронный ресурс] URL: http://www.itsec.ru/articles2/pravo/zaschita-personalnyh-dannyh-v-sotsialnyh-setyah (дата обращения: 10.06.2017).

2. Информацию, автоматически получаемую при доступе к Сайту с использованием закладок (cookies);

3. Статусы, записи в микроблоге «Стена», фотографии, аудиозаписи, видеозаписи, комментарии, записи в обсуждениях групп.

4. Информацию о вступлении в группу / выходе из группы, добавлении других Пользователей в список друзей, размещении фотографий, принятии участия / отказа от участия во встречах, добавлении видеозаписей).

5. Информацию, полученную в результате действий других пользователей на Сайте (в частности, отметки, сделанные на видеозаписях и фотографиях другими Пользователями).[1]

Эта информация содержит большинство действий пользователя на сайте, такой массив данных при попадании в чужие руки, может нанести огромный вред пользователю. На долю хищения персональных данных пришлось 64% всех утечек данных, зафиксированных в первом полугодии 2016 года – или 621 инцидент, в результате которых было украдено более 294 миллионов записей данных (53% всех похищенных или потерянных записей данных).[2] Как сообщает РИА Новости, примерно 60% пользователей социальных сетей в России как минимум однажды теряли доступ к аккаунтам в результате действий злоумышленников, из них у 25% профайлы были взломаны неоднократно.[3]

В связи с этим, администрация социальной сети «Вконтакте», согласно п. 8 Правил защиты информации о пользователях сайта рекомендует пользователям «ответственно подходить к решению вопроса об объеме информации о себе, размещаемой на Сайте»[4].

---

[1] Правила защиты информации о пользователях сайта VK.com [Электронный ресурс]. URL: https://vk.com/privacy (дата обращения: 04.05.2017).

[2] Утечки данных в 2016 году – предварительные итоги года [Электронный ресурс]. URL: https://habrahabr.ru/company/gemaltorussia/blog/314352/ (дата обращения: 04.05.2017).

[3] Eset: аккаунты соцсетей 60% пользователей рунета взламывались хакерами [Электронный ресурс]. URL: http://www.securitylab.ru/news/442581.php (дата обращения: 08.05.2017).

[4] Там же.

Интересно, что пользователь, согласно при регистрации в социальной сети соглашается на то, что отражаемые на персональной странице учетные данные будут считаться общедоступными. Несмотря на то что ПД пользователей находятся в открытом доступе, ФЗ №152 в соответствии с п.1 ст.5 предусматривает недопущение обработки ПД, несовместимой с целями сбора персональных данных. Администрация Сайта vk.com, согласно п. 5.8 «Правил пользования Сайтом ВКонтакте» обрабатывает персональные данные Пользователя в целях предоставления Пользователю доступа к использованию функционала Сайта, в том числе в целях получения Пользователем персонализированной (таргетированной) рекламы; проверки, исследования и анализа таких данных, позволяющих поддерживать и улучшать функционал и разделы Сайта, а также разрабатывать новый функционал и разделы Сайта.

Однако, как показывает практика, персональные данные пользователей социальной сети используются часто используются сторонними компаниями для продвижения товаров или анализа рынка потребителей. Так «Вконтакте» подала иск к компании Double Data и Национальному бюро кредитных историй. Последние, по мнению соцсети, используют информацию пользователей для оценки кредитоспособности и продажи банкам.[1] Тенденция использования общедоступных данных из социальных сетей наблюдается и в других социальных сетях. К примеру, страховая компания Admiral Insurance разработала алгоритм расчета благонадежности водителей, анализируя персональную страницу клиента в Facebook. В компании Facebook назвали такое приложение нарушением приватности и отказались предоставить Admiral Insurance доступ к данным пользователей.[2] Аналогичная ситуация происходит с социальной сетью Twitter, которая

[1] «В Контакте» подала иск на компанию за сбор данных для банков [Электронный ресурс] URL: http://www.rbc.ru/technology_and_media/31/01/2017/58901c239a7947304d9de7 (дата обращения: 02.06.2017).

[2] Facebook запретил страховой компании анализировать публикации клиентов [Электронный ресурс]. URL: https://apparat.cc/news/facebook-blocks-admiral-insurance/ (дата обращения: 02.06.2017).

также требовала прекратить собирать и обрабатывать открытые данные её пользователей. Результат судебного разбирательства «ВКонтакте» может поставить под угрозу существование многих сервисов, собирающих данные пользователей в социальных сетях. Примечательно то, что даже судебные приставы используют, данные пользователей социальных сетей для поиска должников, согласно документу: «Методические рекомендации по использованию сети Интернет в целях поиска информации о должниках и их имуществе» (утв. ФССП РФ 30.11.2010 № 02-7) (ред. от 16.03.2011).[1] Следует помнить, что к данным пользователя может получить доступ любой другой пользователь социальной сети. На сегодняшний день, единственной мерой обеспечения безопасности своих ПД, можно считать самостоятельное регулирование объема выкладываемой личной информации.

Кроме выполнения обязательств перед пользователями, администрация социальных сетей обрабатывает ПД клиентов так же в целях получения пользователем персонализированной (таргетированной) рекламы. Вопрос о таргетированной рекламы плотно связан с ПД пользователей. С помощью таргетинга маркетологи собирают информационные электронные базы данных о клиентах для создания профилей пользователей, которые будут наиболее восприимчивы к их сообщениям.[2] Следует отметить, что многие рекламные компании, предлагающие услуги по созданию таргетированной рекламы, указывают на наличие партнерских отношений с ведущими почтовыми сервисами и сайтами социальных сетей, предусматривающими предоставление последними сведений о пользователях. Передача информации третьим лицам также может быть предусмотрена пользовательскими соглашениями конкретных сервисов.

По этому поводу интересно мнение доктора юридических наук О.В Калятина. Он отмечает, что рекламные объявления, размещаемые на

[1] Бюллетень Федеральной службы судебных приставов. 2011. № 1.

[2] Targeted marketing // The Dictionary Netlingo. [Электронный ресурс]. URL: http://www. netlingo.com/word/targeted-marketing.php (дата обращения: 29.05.2017).

интернет сайтах, организованы таким образом, что при создании cookie для каждого лица формируется уникальный идентификационный номер, что позволяет владельцу рекламного объявления накапливать информацию об активности определенного лица в Интернете в целом.[1]

При том все вышесказанное противоречит главным принципам обработки персональных данных:

1. Недопущение объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

2. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

2.3. Проблемы трансграничного оборота персональных данных

Говоря о развитии системы защиты прав субъектов персональных данных в условиях трансграничного информационного обмена, следует учитывать особенности развития современного информационного общества, а также существующие традиции и правоприменительную практику отдельных государств.[2] Наличие особых требований к трансграничной передаче данных является составной частью практически любого современного законодательного акта, посвященного персональным данным.

Одно из изменений ФЗ № 152, вступивших в силу 1 сентября 2015 года, оказалось наиболее спорным: законодатель систематизировал перечень действий в отношении персональных данных, которые должны производиться исключительно на территории Российской Федерации, и какие могут быть произведены за рубежом (п. 5 ст. 18 ФЗ № 152). В

[1] Дубровин О.В., Ковалева И.Ю. Защита персональных данных в сети Интернет: пользовательское соглашение // Вестник ЮУрГУ. Серия: Право. 2014. № 2. С. 64-70.

[2] Доклад заместителя руководителя Роскомнадзора Р.В. Шередина «О проблеме защиты персональных данных». «Инфофорум-Гонконг-2012» [Электронный ресурс]. URL: https://pd.rkn.gov.ru/press-service/subject4/news3007/ (дата обращения: 01.06.2017).

соответствии с п.3 ст.11 ФЗ № 152 трансграничной передачей ПД - передача ПД на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Одновременно с изменениями в ФЗ № 152, были сделаны поправки в ФЗ № 149, касающиеся создания реестра сайтов-нарушителей законодательства (ч.4 ст. 15.6 ФЗ № 149). Такая правовая норма дает право блокировки ресурса, имеющего базы данных российских пользователей за границей.

Как считает исследователь А. И. Савельев, подобное толкование нововведений закона фактически означает невозможность трансграничной передачи таких данных, хотя формально ФЗ № 152 и ФЗ № 149 не содержат никаких положений, касающихся отмены или изменения порядка их трансграничной передачи, которая к тому же прямо предусматривается в международных соглашениях, стороной которых является Россия. В частности, п. 2 ст. 12 Конвенции №108 что «сторона не будет запрещать или ставить под специальный контроль информационные потоки ПД, идущие на территорию другой Стороны, исходя исключительно из соображений защиты неприкосновенности личной сферы».[1]

Исследователь Иванов А.А. так же критикует поправки в ФЗ № 152 на предмет соответствия ст. 23 и ч. 4 ст. 29 Конституции РФ, он считает, что ФЗ № 152 ограничивает право гражданина на трансграничную передачу персональных данных, в случае, если он дал свое согласие на такую передачу.

Сегодня, учитывая поправки в ФЗ № 152 , можно запретить российским пользователям доступ к подавляющему большинству интернет-ресурсов, происходящих из иностранных государств, в том числе таких как Facebook, Livejournal, Instagram, Twitter и многие другие. На сегодняшний день

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

крупные зарубежные компании находятся в процессе перевода баз данных в РФ, либо вообще отказываются от исполнения требований закона, например Facebook.[1] Избирательность применения правовых санкций нарушает конституционный принцип равенства всех перед законом. Ярым показателем избирательности правоприменения, служит применение законодательства о ПД к отдельным интернет ресурсам. К примеру, согласно Решению Таганского районного суда (Город Москва) от 04 августа 2016 года По делу № 02-3491/2016[2] была заблокирована социальная сеть Linkedin, главным поводом блокировки которой стало нарушение п.5 ст. 18 ФЗ №152, обязывающего оператора ПД хранить ПД граждан РФ с использованием баз данных, находящихся на территории РФ.

У правовых исследователей бытует мнение, что блокировка портала Linkedin является апробированием нововведений в законодательство о локализации баз данных. Ограничение доступа к данному порталу на основании нарушения п.5 ст. 18 ФЗ №152 является первым судебным прецедентом. Учитывая то, что более крупные социальные сети, например Twitter, планируют полностью перенести базы данных в РФ только к 2018 г., блокировка Linkedin кажется, мягко говоря, несправедливой.

Обращаясь к Европейскому законодательному опыту регулирования локализации БД, показательна история Директивы от 15.03.2006 № 2006/24/ЕС.[3] Данная Директива устанавливала жесткие правила хранения информации для операторов. Данные должны были храниться не менее минимум шести месяцев и не более двух лет (сроки определялись

---

[1] Серьгина Е., Болецкая К. Facebook не хочет переносить персональные данные в Россию [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/articles/2015/08/26/606235-facebook-ne-hochet-perenosit-personalnie-dannie-rossiyu (дата обращения: 10.06.2017).

[2] Решение Таганского районного суда (Город Москва) от 04.08.2016 по делу № 02-3491/2016 [Электронный ресурс]. URL: http://docs.pravo.ru/document/view/87232058/100222486/ (дата обращения: 13.06.2017).

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) // Официальный журнал ЕС. Секция N L 201. 2002. 31 июля. С. 37.

государствами-членами при транспозиции Директивы в национальное законодательство).

Главными тезисами из обзора Европейской комиссии Директивы по сохранению данных электросвязи являлись:

1. Нормы ЕС в отношении сохранения данных в первую необходимы для правоохранительных органов, защиты потерпевших и систем уголовного правосудия.

2. Трудности для поставщиков услуг электросвязи и, в частности, для менее крупных операторов.

3. Сохранение данных сопряжено со значительными ограничениями права на неприкосновенность частной жизни.[1]

В итоге Суд Европейского союза признал Директиву недействительной, так как ее положения не отвечают критерию пропорциональности и не содержат необходимых ограничений, которые бы препятствовали злоупотреблениям со стороны правоохранительных органов.

Сегодня, в точности повторяя неудачный Европейский опыт, законодатель РФ установил ограничения трансграничной передачи данных, локализовал серверы баз ПД, ввел обязательный срок шесть месяцев для хранения текстовых сообщений, голосовой информации, изображений, звуков, видео, и иных электронные сообщения пользователей сети Интернет. (пп. 2 п. 3 ст. 10.1 ФЗ № 149)

Исследователь Савельев А.И считает, что при локализации баз данных в РФ возникает еще один центр концентрации ПД, что повышает риск их утечки или компрометации, а несение дополнительных затрат на локализацию данных может повысить стоимость интернет-сервисов или привести к тому, что такие сервисы и вовсе станут недоступными для российских пользователей. Вряд ли это можно назвать заботой о субъектах

[1] Европейская комиссия оценивает Директиву по сохранению данных электросвязи [Электронный ресурс]. URL: https://www.itu.int/net/itunews/issues/2011/03/pdf/201103_45-ru.pdf (дата обращения: 13.06.2017).

персональных данных. В определенной степени, получается, что государство расширяет доступ компетентных органов к персональным данным в отсутствие юрисдикционных сложностей.[1]

В соответствии с неофициальными заявлениями Роскомнадзор не намерен активно преследовать организации за несоблюдение правил локализации в начальный период их действия. Однако юридически такая возможность существует.

Толкование норм вступившего в силу Закона, подтвержденное неофициальными разъяснениями регуляторов, не запрещает передачу данных за пределы России. Действительно, персональные данные смогут обрабатываться за рубежом, и законодатель не ставил перед собой задачи полностью изолировать персональные данные россиян. Основной целью Закона является обеспечение хранения и актуализации данных в России, а не на иностранных серверах.

Наличие особых требований к трансграничной передаче данных является составной частью практически любого современного законодательного акта, посвященного персональным данным. Обеспечение трансграничной передачи данных под юрисдикцией современного законодательства о ПД заставляет субъектов информационного пространства подчиняться строгим правилам хранения и передачи информации иностранному государству. При этом свобода субъекта ПД самостоятельно распоряжаться своей личной информацией кажется ограниченной – закон лишает субъекта данных возможности по своему решению (согласию) сообщить данные лицу, которое использует их в базах данных, находящихся за рубежом.

[1] Законодательство о локализации данных и его влияние на рынок электронной коммерции в России // Закон. 2014. № 9. С. 51-68.

3. ПЕРСПЕКТИВЫ РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ.

3.1. Определение персональных данных

От того, как право регулирует общественные отношения, зависит само развитие этих отношений: право может способствовать их развитию, но может и тормозить, а если не учитывать реалий, то право может и не работать либо результат будет совсем не тот, на который мы рассчитывали. Представляется исключительно важным, чтобы законодатель выявлял и учитывал в принимаемых законодательных актах интересы различных групп субъектов, но самый оптимальный вариант - когда обеспечивается баланс интересов.

Регуляция отношений в сфере обработки персональных данных в основном подлежит рассмотрению в ФЗ №152. На основании правового анализа норм ФЗ №152, а так же анализа судебной практики по вопросам обработки персональных данных можно выявить некоторые правовые коллизии. В ФЗ №152 суть правовых коллизий составляют:

1 неточности формулировок и расхождение

2 противоречие между отдельными нормативными правовыми актами, регулирующими одни и те же либо смежные общественные отношения,

3 также противоречия, возникающие в процессе правоприменения и осуществления компетентными органами и должностными лицами своих полномочий.

Для анализа правовых коллизий ФЗ №152 следует в первую очередь обратиться к содержанию закона. ФЗ №152 построен достаточно четко и логично. Однако персональные данные включают настолько различную информацию, что сформировать единый правовой режим персональных данных для всех случаев оказывается невозможным. Принцип формальной определенности закона, сформулированный в практике Конституционного

Суда РФ, вытекает из ч. 1 ст. 1, ч. 2 ст. 4, ч. 2 ст. 6, ч. 2 ст. 15 и ч. 1 ст. 19 Конституции РФ и предполагает точность, ясность и недвусмысленность правовых норм, без чего не может быть обеспечено единообразное понимание и применение таких норм, а значит, и равенство всех перед законом.

В основном, критике авторов-правоведов подвергается дефинитивная часть закона. В части определения понятия персональных данных. Так исследователь Иванов В.И считает что действующее определение ПД, согласно которому это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПД), слишком размыто и ориентировано на субъективное усмотрение правоприменителя. Слова "любая" и "косвенно" позволяют выходить далеко за рамки общепринятых представлений о частной жизни, личной и семейной тайне и относить к ПД все что угодно. Сведения о состоянии здоровья, интимной жизни относятся к специальным категориям ПД в соответствии с ч. 1 ст. 10 ФЗ № 152.

В конкретизации нуждается само понятие "персональные данные". Слова "любая" и "косвенно", используемые в его определении, позволяют выходить далеко за рамки общепринятых представлений о частной жизни, личной и семейной тайне и относить к персональным данным все что угодно.»[1]

Так же, с мнением И.В Иванова Согласна В.А Приезжева, которая утверждает что «С точки зрения принципов права, действующих в российской правовой системе, можно усомниться в формальной определенности понятия «персональные данные». При буквальном толковании к ПД можно отнести широкий круг информации, в том числе выходящий за рамки разумно ожидаемого в данном контексте. В частности, в нем нет указания на связь между информацией и прямой или косвенной

[1] Иванов И. С. Врачебная тайна // СПС КонсультантПлюс. 2013.

определенностью или «определяемостью» физического лица. Соответственно, отсутствует однозначное понимание того, в каких случаях собираемые и обрабатываемые данные будут относиться к персональным, а в каких – нет».[1]

Так же правоведы Наумов В.Б и Архипов В.В. высказывается о том, что понятие персональных данных в законодательстве РФ определено более широко чем в международных НПА: «Есть веские основания усомниться в том, что рассматриваемое понятие получило формальную определенность. Проблема заключается в том, что косвенно к определенному физическому лицу при таком подходе может относиться абсолютно любая информация. В самом абсурдном варианте допустимо к персональным данным причислить, например, уровень солнечной активности, поскольку она влияет на здоровье человека, т.е. на здоровье определенных или определяемых физических лиц!»[2]

Изучая вопрос об определении понятия персональных данных, следует обратиться к тенденциям в определениях судов. Исследование практики показывает, что в процессах вынесения решений, суды используют узкий и широкий подход к определению понятия персональных данных. К понятию ПД суды обычно относят прежде всего, его фамилию, имя, отчество, год, месяц, дату и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессию, доходы, а также другую информацию, при которой возможно идентифицировать конкретное лицо.[3]

---

[1] Федеральный закон «О персональных данных»: научно-практический комментарий (постатейный) / под ред. А.А. Приезжевой. М.: Редакция «Российской газеты», 2015. Вып. 11. С. 100.

[2] Наумов В.Б., Архипов В.В. Понятие персональных данных: интерпретация в условиях развития информационно-телекоммуникационных технологий // Российский юридический журнал. 2016. № 2. С. 186-196.

[3] Апелляционное определение Московского городского суда от 28.01.2014 по делу № 33-5461 [Электронный ресурс]. URL: http://ourcourt.ru/mosgorsud/2014/01/28/14041.html (дата обращения: 11.06.2017).

К примеру в Апелляционном определении Московского городского суда от 06.09.2012 по делу № 11-17136[1] суд поясняет: «Ссылка ответчика на то обстоятельство, что фамилия, имя и отчество не являются персональными данными, не может быть принята во внимание, как противоречащая действующему законодательству, так как, исходя из положений п. 1 ст. 3 ФЗ "О персональных данных" от 27 июля 2006 г. N 152-ФЗ персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).[2]

Вышесказанный подход к определении понятия ПД так же отражен в решениях судов:

- Апелляционное определение Московского городского суда от 28 января 2014 г. по делу N 33-5461.[3]

- Апелляционное определение Тульского областного суда от 28 апреля 2015 г. по делу N 33-850.[4]

В тоже время, не смотря на критику дефиниции понятия персональных данных, следует отметить, что данная трактовка в ФЗ №152 применяется в соответствии с Директивой Европейского Союза и Парламента 95/46/ЕС от 24 октября 1995 г. «О защите прав частных лиц применительно к обработке персональных данных и свободном движении таких данных» и Конвенции № 108 которые обозначают под ПД любую информацию, относящуюся к определенному или определяемому физическому лицу, которое может определено прямо или косвенно, в частности, через идентификационный

[1] Апелляционное определение Московского городского суда от 06.09.2012 по делу № 11-17136 [Электронный ресурс] URL: http://ourcourt.ru/mosgorsud/2014/01/28/140421.html (дата обращения: 11.06.2017).

[2] Апелляционное определение СК по гражданским делам Московского городского суда от 06.09.2012 по делу № 11-17136 [Электронный ресурс] URL: http://base.garant.ru/57811433/ (дата обращения: 09.06.2017).

[3] Апелляционное определение Московского городского суда от 28.01.2014 по делу N 33-5461 [Электронный ресурс]. URL: http://ourcourt.ru/mosgorsud/2014/01/28/140421.htm (дата обращения: 16.06.2017).

[4] Апелляционное определение Тульского областного суда от 28.04.2015 по делу № 33-850 [Электронный ресурс]. URL: http://sudact.ru/regular/doc/WiziwJNrvRJM/ (дата обращения: 12.06.2017).

номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

Согласно разъяснениям Роскомнадзора, если совокупность данных необходима и достаточна для идентификации лица, такие данные следует считать персональными данными, даже если они не включают в себя данные документов, удостоверяющих личность.

Следует отметить, что не все суды признают данные, прямо относящиеся к физическому лицу к персональным. Так, в Определении СК по гражданским делам Приморского краевого суда от 9 сентября 2013 г. по делу № 33-7063[1], суд отметил, что «в совокупности имя, отчество, улица и номер дома не позволяют достоверно установить, о каком именно человеке идет речь на страницах форума». Разрешая заявленные требования, суд пришел к обоснованному выводу об отказе в удовлетворении исковых требований, поскольку сведения, размещенные в Интернете по ссылке не являются персональными данными истца, так как не содержат персонифицированных и детализированных данных, позволяющих определить в отношении какой квартиры, какого населенного пункта идет речь, а также отсутствует указание на фамилию, что не позволяет идентифицировать лицо, о котором идет речь».

Подход не признания данных персональными без их вместе взятой совокупности так же представлен в Постановлении Восемнадцатого арбитражного апелляционного суда от 24 сентября 2014 г. N 18АП-10690/14[2]

«Не каждый из этих элементов сам по себе подпадает под защиту Закона, а только если они в отдельности или в совокупности помогают

[1] Определение СК по гражданским делам Приморского краевого суда от 09.09.2013 по делу № 33-7063 [Электронный ресурс]. URL: http://www.garant.ru/products/ipo/prime/doc/116641647/ (дата обращения: 28.06.2017).

[2] Постановление Восемнадцатого арбитражного апелляционного суда от 24.09.2014 N 18АП-10690/14 [Электронный ресурс]. URL: http://base.garant.ru/60345203/ (дата обращения: 11.06.2017).

идентифицировать конкретное лицо» и в Определении Санкт-Петербургского городского суда от 26 марта 2013 г. N 33-3815/13, а так же в Апелляционном определении Московского городского суда от 28 января 2014 № 33-5461/14.[1]

Очевидно, что в рассмотренных решениях судов заложено логическое противоречие. Оно выражается в дифференцируемой трактовке понятия ПД судами. В рассмотренных выше делах, суд приходит к выводу о том, что если совокупная информация об имени, адресе не каждый из этих элементов сам по себе не подпадает под определение ПД и не позволяет идентифицировать конкретное лицо.

Этот же подход отражен в обзоре обращений граждан на портале Роскомнадзора «Фамилия и инициалы гражданина - это, несомненно, персональные данные субъекта. Однако без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных невозможно».[2]

Анализируя судебную практику можно заметить, что суды, при рассмотрении дел, часто понимают под ПД количество данных, способных идентифицировать человека. Суды ссылаются на то, что отдельные части личной информации, например, имя и фамилия, без каких-либо других идентификаторов не являются ПД. Такому подходу способствует используемый судами Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»[3], который в ст. 1 трактует понятие ПД как сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность.

---

[1] Апелляционное определении Московского городского суда от 28.01.2014 № 33-5461/14 [Электронный ресурс]. URL: http://base.garant.ru/60345203/ (дата обращения: 11.06.2017).

[2] Обзор обращений граждан за II квартал 2012 года «Защита прав субъектов персональных данных» [Электронный ресурс]. URL: http://10.rkn.gov.ru/queries/lookup/people_2kv_2012/p1/ (дата обращения: 09.06. 2017).

[3] Собрание законодательства РФ. 1997. № 10. Ст. 1127.

Любопытно, что суды и Роскомнадзор в своих отчетах используют термин «идентификация». Следует отметить, что законодателем не раскрывается определение понятия идентификации. Учитывая, что законодательство о ПД не содержит определение понятия, можно предположить, что законодатель вкладывает в него обычно используемое в повседневной жизни значение.

Учитывая, что ПД определяются судами идентификационными свойствами, а идентифицируемость субъекта является необходимым условием квалификации данных в качестве персональных, представляется возможным изменить дефиницию понятия ПД в п. 1 ст. 3 ФЗ № 152 на любую информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), позволяющую оператору идентифицировать личность субъекта персональных данных.

3.2. Единый портал персональных данных

Законодательство о ПД на сегодняшний день содержит право субъекта на отзыв согласия на обработку его ПД. Процедура отзыва описана в п.5 ст. 21 ФЗ № 152. В случае отзыва субъектом ПД на обработку его ПД оператор обязан прекратить их обработку или обеспечить прекращение такой обработки и в случае, если ПД более не требуется для целей обработки ПД, уничтожить ПД или обеспечить их уничтожение (если обработка ПД осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва.

На практике, для субъекта ПД бывает очень трудно отследить потоки личной информации и отозвать их. Со стороны оператора ПД так же происходят нарушения обработки ПД, например:

1. Нарушение сроков обработки после отзыва;

2. Незаконная передача ПД субъекта другим организациям.

Чаще всего подобные нарушения встречаются в финансово-кредитных организациях и банковской сфере, так же некоторые из них неправомерно указывалось на невозможность отзыва согласия на обработку ПД.

В подтверждение вышесказанных слов показателен пример из Постановления ФАС Поволжского округа от 28.04.2012 № Ф06-2316/2012,[1] в котором в ходе проверки деятельности ЗАО «КОМСТАР-Регионы», проводимой Роскомнадзором, было установлено, что договор, заключенный с абонентом М., был расторгнут 1 июня 2011 г., задолженность ее погашена, следовательно, цель обработки достигнута 1 июня 2011 г. Однако, несмотря на указанные обстоятельства, оператор по истечении трех рабочих дней продолжал обрабатывать персональные данные М.

Неисполнение обязанностей оператора по прекращению обработки ПД после отзыва, может быть выявлено в ходе проверки, проводимой Роскомнадзором, уполномоченным осуществлять контроль и надзор соответствия обработки ПД требованиям комментируемого ФЗ № 152, и повлечь вынесение в его адрес предписания с требованием устранить нарушения.

Справедливости ради надо отметить, что дача согласия на обработку персональных данных, особенно в электронной форме не носит затруднительного характера для субъекта ПД, что нельзя сказать про процедуру отзыва ПД. К примеру, для отзыва ПД после совершения покупки в интернет-магазине трудность состоит в том, отзывает согласие сам субъект ПД, или нет. Выходит, что если дать согласие на обработку персональных данных своими конклюдентными действиями, то отзывать его, возможно, придется с помощью письменного заявления субъекта персональных данных либо электронного документа с электронной же подписью? Без сомнения,

[1] Постановление ФАС Поволжского округа от 28.04.2012 № Ф06-2316/2012 [Электронный ресурс]. URL: http://kad.arbitr.ru/Card/16837b12-beb9-476e-9a93-d8e576519c6e (дата обращения: 21.06.2017).

обе эти процедуры могут быть затруднительны для рядового покупателя интернет-магазина.[1]

Зачастую сам субъект ПД не помнит, где он давал согласие на обработку ПД, либо беспечно относится к своим ПД, размещая их в общедоступных источниках. Такому субъекту ПД, будет весьма тяжело воспользоваться правом на отзыв согласия на обработку ПД. Рассматривая развитие Европейского законодательства, а именно Регламент № 2016/679 Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)» [рус., англ.] (Принят в г. Брюсселе 27.04.2016)[2] можно заметить тенденцию законодателя к упрощению бюрократических процедур в работе с персональными данными и минимизацию усилий для начала и прекращения обработки ПД. В п.3 ст.7 закрепляется право субъекта в любое время отозвать свое согласие и устанавливается «простота» отзыва согласия. «Процедура отзыва согласия должна быть такой же простой, как и процедура предоставления согласия».

Простота отзыва согласия ПД субъектом может быть возможна при создании единого портала ПД. Такой портал аккумулировал бы в себе базу данных операторов, обрабатывающих личную информацию субъектов ПД, с возможностью отзыва согласия на обработку ПД у каждого оператора. Сейчас создание такого портала обсуждается на рабочей группе в администрации президента, которую возглавляет советник президента РФ Игорь Щеголев.[3]

---

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

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Официальный журнал ЕС. Секция N L 119. 2016. 04 мая. P. 1.

[3] Алешин М. В России установят контроль за распространением персональных данных [Электронный ресурс]. URL: http://iz.ru/rubric/internet (дата обращения: 18.06.2017).

Появление такого ресурса должно решить проблему неконтролируемой обработки ПД и облегчить отзыв ПД субъектом. Идея создания портала выглядит довольно привлекательно и перспективно, однако сложность представляет механизм реализации данного проекта.

Чтобы проект портала ПД полностью выполнял свои функции в полную силу, необходимо:

1. Автоматизировать БД операторов;
2. Решить проблемы сознательного правонарушения;
3. Постоянно проверять и пополнять реестр операторов;
4. Обеспечить высокую степень защиты такого ресурса.

Понятно, что для работы ресурса необходимо перевести всю информацию в электронный вид. Это создаст дополнительную нагрузку на тех операторов, кто использует неавтоматизированную обработку ПД. Так же, тяжело движется процесс внесения юр. Лиц в реестр операторов ПД, (около 10% всех организаций находятся в списке) и функционал сайта будет бесполезен для людей, оставляющих свои ПД у неавторизованных операторов.

Множество сведений о всех субъектах РФ в одном месте, включая и особо чувствительную информацию, безусловно несет риск утечки информации. Необходимо обеспечить надежную защиту ПД на данном ресурсе, т.к. в отличие от информации в социальных сетях, в проекте планируется содержание только актуальные ПД, включая особо чувствительную информацию, попадание в чужие руки которых может нанести серьезный вред субъекту ПД.

4. МЕТОДИЧЕСКАЯ РАЗРАБОТКА

Интерактивный урок №1
«Понятие персональных данных» (45 мин)

1) Тип урока: Комбинированный урок

2) Цель урока: Сформировать представление о персональных данных

3) Задачи:

3.1 Образовательные:

- Изучить закон «О персональных данных»;
- Закрепить сущность понятия ПД;
- Формирование умений работать в «СПС Консультант»

3.2 Развивающие:

- Развитие умений анализировать информацию, обобщать и делать выводы;
- Совершенствование речевой грамотности;
- Развитие умений выявлять причинно-следственные связи.

3.3 Воспитательные:

- Формирование правовой культуры.

4) Технические средства:

- Персональные компьютеры с доступом к сети интернет, проектор, тетрадь

5) Методы

- По источнику получения информации: словесные (объяснения), практические;
- По управлению деятельностью учащихся: эвристическая беседа, алгоритмизация;
- По видам деятельности учащихся: поисковый, исследовательский.

Учебно-методическая литература:

1. Портал «Защити свои персональные данные» / [Электронный ресурс] http://персональныеданные.дети/ (дата обращения 10.05.2017)

2. Семакин И.Г., Шеина И.Ю. Преподавание информатики в средней школе. Методическое пособие. М.: Лаборатория базовых знаний, 2011

3. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 22.02.2017) "О персональных данных" // "Российская газета", N 165, 29.07.2006

Ход урока:

Структурный элемент урока	План деятельности преподавателя	План деятельности учащихся	Время этапа урока (мин.)
Организационная часть	Приветствие, проверка присутствующих учащихся, запись даты и темы в тетрадь, вступительная речь	Знакомство с преподавателем	5
Актуализация опорных знаний	Пояснение к правилам выполнения теста	Выполнение теста	5
Изучение нового материала	Знакомство с ФЗ «о персональных данных», закрепление понятия ПД, обработка ПД, безопасность ПД	Беседа с преподавателем	20

Совместная проверка результатов теста	Пояснение правильных ответов	Анализ допущенных ошибок	5
Закрепление материала	Перечисление основных тезисов урока, опрос по пройденному материалу (поощрение активно отвечающих на вопросы учеников)	Ответ на вопросы преподавателя	5
Выставление оценок	Учет активности учеников на занятии, оценивание работу каждого ученика, поощрение активистов.	Анализ работы на уроке	3
Постановка домашнего задания	Определения планов работы на следующее занятие, дача домашнего задания по пройденному материалу	Запись домашнего задания	2

Материалы для теста

1. Персональные данные состоят из:

1. ФИО, возраст, домашний адрес и номер телефона
2. Группа крови, отпечатки пальцев, медицинские диагнозы
3. Сведения об образовании, фотографии

4. Все вышеперечисленное. Персональные данные - это информация, по которой тебя можно идентифицировать.

2. Можешь ли ты контролировать размещение своих фотографий в сети Интернет, если выкладываешь их в социальные сети?

1. Да
2. Нет

3. Друг устраивает вечеринку в выходные, и все ваши друзья приглашены. Правильно ли будет разместить дату, время и место на сайте, потому что тогда у каждого будут детали этой встречи.

1. Да
2. Нет

4. Какие файлы ты разместишь в социальных сетях?

1. Все, что захочу, это смешно и интересно – моим друзьям понравится!
2. Сначала подумаю. Буду ли я чувствовать себя комфортно, если родители, учителя увидят то, что я публикую?
3. Фотографии, ФИО, адрес

5. Может ли твой друг заходить в твой аккаунт и отправлять от твоего имени сообщения?

1. Да, потому что он мой друг, и я ему доверяю
2. Нет. Имея доступ к твоему аккаунту, друг может иметь доступ не только к тем файлам, которые ты разрешил смотреть, но и ко всем остальным данным.

6. При заполнении онлайн-формы для ввода данных, которые будут опубликованы, какие данные не стоит указывать?

1. Никнэйм или псевдоним

2. ФИО

3. Адрес, где ты живешь

4. Адрес, где ты учишься

* - Допускается несколько вариантов ответа

7. Какие последствия могут наступить, если ты отметишь друга на фото

5. Массовое распространение фотографии в сети, если не настроена приватность учетной записи

6. Никаких последствий не будет

7. Ничего не случится, мой друг просто станет популярнее

8. Если у тебя есть сомнения, дать ли людям, с которыми общаешься в сети больше личной информации о себе, что ты сделаешь

8. Расскажешь взрослому и попросишь совет

9. Расскажешь другу (подруге) и попросишь совет

10. Отправишь личные данные и посмотришь, что будет

11. Не отправишь личные данные

12. Допускается несколько вариантов ответа

ЗАКЛЮЧЕНИЕ

Результатом правового регулирования оборота ПД является достижение личной безопасности, характеризующейся состоянием защищенности жизненно важных интересов личности от потенциально и реально существующих угроз, или отсутствие таких угроз, где права человека и состояние их защищенности являются отражением уровня зрелости социальной политики государства, которое одной из своих задач ставит обеспечение прав и безопасности своих граждан. Решению этой задачи должна быть подчинена деятельность всех государственных институтов. Состояние защищенности и баланс интересов операторов, общества и государства во всех сферах жизнедеятельности может обеспечивать устойчивое развитие страны и способствовать достижению национальной безопасности.

Исходя из поставленных задач, в работе было проанализировано действующее законодательство РФ в области защиты ПД, а так же деятельность уполномоченного органа по защите ПД. Сделаны выводы о плодотворности формирования новых подходов к регулированию отношений в области защиты ПД и международном сотрудничество государств в регламентации информационного пространства.

Для изучения основных правовых коллизий информационного пространства РФ, в работе рассмотрены проблемы правоприменения законодательства при трансграничной передачи данных, в сфере оказания государственных услуг и социальных сетях. Сделаны выводы и о сверхимперативности, избирательности и недостаточности правовой защиты ПД в вышеуказанных отраслях.

В качестве возможных перспектив развития законодательства, в третьей главе предлагается новый вариант законодательной дефиниции термина «персональные данные» и создание единого портала ПД. Представляется, что новое определение термина ПД, при внедрении в

практику, устранит неопределенность существующего понятия, облегчит деятельность судов и операторов ПД. Единый портал ПД, в свою очередь, сделает облегченным отзыв согласия об обработке ПД, устранит процессуальную трудность, а порой и невозможность исполнения данного правомочия.

Проведенный анализ правовых норм и акцентирование множества правовых коллизий в законодательстве о ПД дает основания полагать, что, несмотря на активное старание законодателя контролировать обработку ПД в РФ, некоторые механизмы правоприменения требуют доработки или пересмотра. Пробелы правового регулирования законодательства о ПД отчасти вызваны тем, что в РФ институт ПД возник относительно недавно и находится на этапе становления.

На сегодняшний день, исходя из проведенного исследования можно выделить ряд очевидных проблем:

1. Наличие практики сознательного правонарушения операторами;
2. Несовершенство терминологии главного закона о ПД;
3. Недостаточное правовое регулирование оборота ПД в социальных сетях;
4. Правовая неграмотность граждан, беспечное распространение своих ПД.

Обеспечение высокого уровня защищенности прав граждан РФ на неприкосновенность частной жизни, личную и семейную тайну является одной из главных задач государства. Реализация данной цели лежит в планомерной, учитывающей интересы общества и операторов политике Роскомнадзора, правового просвещения и пропаганде ответственного отношения к ПД для граждан, повышению доступности и качества государственных услуг. Изучение практики Европейских государств перед внесением изменений в национальное законодательство, а так же ратификация международных договоров должно становиться естественной практикой для законодателя.

Принимая во внимание интересы общества, развитие действующей законодательной базы не должно быть в первую очередь направлено на обеспечение защиты собственно информации, а не прав граждан при обработке их ПД в информационных системах.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Нормативные правовые акты и иные документы

1. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) // Собрание законодательства РФ. 2014. № 5. Ст. 419.
2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства РФ. 2014. № 31. Ст. 4398.
3. Кодекс об административных правонарушениях Российской Федерации: Федеральный закон от 30.12.2001 № 195-ФЗ // Собрание законодательства РФ. 2002. № 1. Ст. 1.
4. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954.
5. Трудовой кодекс Российской Федерации: Федеральный закон от 30.12.2001 № 197-ФЗ // Российская газета. 2001. 31 декабря.
6. Воздушный кодекс Российской Федерации: Федеральный закон от 19.03.1997 № 60-ФЗ // Российская газета. 1997. 26 марта.
7. Жилищный кодекс Российской Федерации: Федеральный закон от 29.12.2004 № 188-ФЗ // Российская газета. 2005. 12 января.
8. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ // Парламентская газета. 2006. 03 августа.
9. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 06.07.2016) // Российская газета. 2006. 29 июля.

10. Об организации предоставления государственных и муниципальных услуг: Федеральный закон от 27.07.2010 № 210-ФЗ (ред. от 28.12.2016) // Российская газета. 2010. 30 июля.
11. О внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации: Федеральный закон от 28.12.2016 № 471-ФЗ // Российская газета. 2016. 30 декабря.
12. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 07.02.2017 № 13-ФЗ // Парламентская газета. 2017 10-16 февраля.
13. Об утверждении Перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) // Российская газета. 1997. 14 марта.
14. О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с «Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»): Постановление Правительства РФ от 16.03.2009 № 228 (ред. от 01.07.2016) // Российская газета. 2009. 24 марта.
15. Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами: Постановление Правительства РФ от 21.03.2012 № 211 (ред. от 06.09.2014) // Российская газета. 2012. 30 марта.
16. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012 № 1119 // Российская газета. 2012. 07 ноября.

17. Методические рекомендации по использованию сети Интернет в целях поиска информации о должниках и их имуществе (утв. ФССП РФ 30.11.2010 № 02-7) (ред. от 16.03.2011) // Бюллетень Федеральной службы судебных приставов. 2011. № 1.
18. Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» [рус., англ.] (Принята в г. Люксембурге 24.10.1995) (с изм. и доп. от 29.09.2003).
19. Директива 97/66/ЕС от 15.12.97 «Касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций» // Официальный журнал ЕС. Раздел С 200. 1994. 22 июля. С. 4.
20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Официальный журнал ЕС. Раздел L 119. 2016. 04 мая. P. 1.
21. Judgment in Case C-131/12 Google Spain SL, Google Inc. v Agecia Española de Proteción de Datos, Mario Costeja González [Электронный ресурс]. Режим доступа: http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065
22. Решение по делу 12-283/2011 от 21.09.2011 [Электронный ресурс]. Режим доступа: https://rospravosudie.com/court-kujbyshevskij-rajonnyj-sud-g-omska-omskaya-oblast-s/act-513897244/
23. Решение Таганского районного суда (Город Москва) от 04.08.2016 по делу № 02-3491/2016 [Электронный ресурс]. Режим доступа: http://docs.pravo.ru/document/view/87232058/100222486/
24. Апелляционное определение Московского городского суда от 28.01.2014 по делу № 33-5461 [Электронный ресурс]. Режим доступа: http://ourcourt.ru/mosgorsud/2014/01/28/140421.html

25. Апелляционное определение Московского городского суда от 06.09.2012 по делу № 11-17136 [Электронный ресурс]. Режим доступа: http://ourcourt.ru/mosgorsud/2014/01/28/140421.html
26. Апелляционное определение СК по гражданским делам Московского городского суда от 06.09.2012 по делу № 11-17136 [Электронный ресурс]. Режим доступа: http://base.garant.ru/57811433/
27. Апелляционное определение Московского городского суда от 28.01.2014 по делу N 33-5461 [Электронный ресурс]. Режим доступа: http://ourcourt.ru/mosgorsud/2014/01/28/140421.htm
28. Апелляционное определение Тульского областного суда от 28.04.2015 по делу № 33-850 [Электронный ресурс]. Режим доступа: http://sudact.ru/regular/doc/WiziwJNrvRJM/
29. Определение СК по гражданским делам Приморского краевого суда от 09.09.2013 по делу № 33-7063 [Электронный ресурс]. Режим доступа: http://www.garant.ru/products/ipo/prime/doc/116641647/
30. Постановление Восемнадцатого арбитражного апелляционного суда от 24.09.2014 № 18АП-10690/14 [Электронный ресурс]. Режим доступа: http://base.garant.ru/60345203/
31. Апелляционное определении Московского городского суда от 28.01.2014 № 33-5461/14 [Электронный ресурс]. Режим доступа: http://base.garant.ru/60345203/
32. Постановление ФАС Поволжского округа от 28.04.2012 № Ф06-2316/2012 Электронный ресурс]. Режим доступа: http://kad.arbitr.ru/Card/16837b12-beb9-476e-9a93-d8e576519c6e

Литература

1. Eset: аккаунты соцсетей 60% пользователей рунета взламывались хакерами [Электронный ресурс]. Режим доступа: http://www.securitylab.ru/news/442581.php

2. Facebook запретил страховой компании анализировать публикации клиентов [Электронный ресурс]. Режим доступа: https://apparat.cc/news/facebook-blocks-admiral-insurance/
3. Remedying Web Hijacking: Notification Effectiveness and Webmaster Comprehension [Электронный ресурс]. Режим доступа: http://dl.acm.org/citation.cfm?id=2883039
4. Targeted marketing // The Dictionary Netlingo. [Электронный ресурс]. Режим доступа: http://www. netlingo.com/word/targeted-marketing.php)
5. Брауде-Золотарёв, М. Ю., Сербина, Е. С., Негородов, В. С., Волошкин, И. Г. Персональные данные в государственных информационных ресурсах. М.: Издательский дом «Дело» РАНХиГС, 2016. 56 с.
6. В России установят контроль за распространением персональных данных [Электронный ресурс]. Режим доступа: http://iz.ru/rubric/internet
7. ВКонтакте подала иск на компанию за сбор данных для банков [Электронный ресурс] Режим доступа: http://www.rbc.ru/technology_ and_media/31/01/2017/58901c239a7947304d9de73
8. Доклад заместителя руководителя Роскомнадзора Р.В. Шередина «О проблеме защиты персональных данных». «Инфофорум-Гонконг-2012» [Электронный ресурс]. Режим доступа: https://pd.rkn.gov.ru/press-service/subject4/news3007/
9. Дубровин О.В., Ковалева И.Ю. Защита персональных данных в сети Интернет: пользовательское соглашение // Вестник ЮУрГУ. Серия: Право. 2014. №2. С. 64-70.
10. Европейская комиссия оценивает Директиву по сохранению данных электросвязи [Электронный ресурс]. Режим доступа: https://www.itu.int/net/itunews/issues/2011/03/pdf/201103_45-ru.pdf
11. Защита персональных данных в социальных сетях [Электронный ресурс]. Режим доступа: http://www.itsec.ru/articles2/pravo/zaschita-personalnyh-dannyh-v-sotsialnyh-setyah
12. Иванов И.С. Врачебная тайна // СПС КонсультантПлюс. 2013.

13. «Идентификатор персональных данных – это возможность ограничить права человека извне»: интервью депутата Госдумы Александра Чуева [Электронный ресурс] // ИА REGNUM. Режим доступа: https://regnum.ru/news/602047.html
14. Майоров А.В., Поперина Е.Н. Формирование и развитие права на неприкосновенность частной жизни // Юридическая наука и правоохранительная практика. 2012. № 3. С. 34-38.
15. Наумов В.Б., Архипов В.В. Понятие персональных данных: интерпретация в условиях развития информационно-телекоммуникационных технологий // Российский юридический журнал. 2016. № 2. С. 186-196.
16. Обзор обращений граждан за II квартал 2012 года «Защита прав субъектов персональных данных» [Электронный ресурс]. Режим доступа: http://10.rkn.gov.ru/queries/lookup/people_2kv_2012/p1/
17. Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2015 год [Электронный ресурс]. Режим доступа: https://rkn.gov.ru/docs/Otchet_ZPD_rus2015.pdf
18. Параскевов А.В., Левченко А.В., Кухоль Ю.А. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом // Научный журнал КубГАУ. 2015. № 110. С. 866-894.
19. Передня В.А. Защита персональных данных в информационно-телекоммуникационной сети международного информационного обмена // Юридический мир. 2013. № 6. С. 13-16.
20. Правила защиты информации о пользователях сайта VK.com [Электронный ресурс]. Режим доступа: https://vk.com/privacy
21. Принят закон, упраздняющий УЭК [Электронный ресурс]. Режим доступа: http://d-russia.ru/prinyat-zakon-uprazdnyayushhij-uek.html
22. Развитие законодательства о защите персональных данных [Электронный ресурс]. Режим доступа: http://www.smartmanage.ru/deels-430-1.html

23. Савельев А.И. Законодательство о локализации данных и его влияние на рынок электронной коммерции в России // Закон. 2014. № 9. С. 51-68.
24. Савельев А.И. Электронная коммерция в России и за рубежом: правовое регулирование. 2-е изд. М.: Статут, 2016. 640 с.
25. Серьгина Е., Болецкая К. Facebook не хочет переносить персональные данные в Россию [Электронный ресурс]. Режим доступа: https://www.vedomosti.ru/technology/articles/2015/08/26/606235-facebook-ne-hochet-perenosit-personalnie-dannie-rossiyu
26. Соколова О.С. Проблемы реализации Федерального закона «О персональных данных». Современное право. М., 2006.
27. Терещенко Л.К. Модернизация информационных отношений и информационного законодательства: монография. М.: Институт законодательства и сравнительного правоведения при Правительстве РФ, ИНФРА-М, 2013. 227 с.
28. Туркиашвили А.М. Защита персональных данных личности как информационная функция современного государства // Современный юрист. 2013. № 4. С. 110-123.
29. Утечки данных в 2016 году – предварительные итоги года [Электронный ресурс] Режим доступа: https://habrahabr.ru/company/gemaltorussia/blog/314352/
30. Федеральный закон «О персональных данных»: научно-практический комментарий (постатейный) / под ред. А.А. Приезжевой. М.: Редакция «Российской газеты», 2015. Вып. 11. 176 с.