Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический институт
институт

Кафедра международного права
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____Т.Ю. Сидорова
подпись инициалы, фамилия

«___» _____ 2021 г.

БАКАЛАВРАСКАЯ РАБОТА

40.03.01 Юриспруденция, 40.03.01.01 Международное и иностранное право
код – наименование направления

Защита персональных данных в сети Интернет: сравнительный анализ
тема

Руководитель _____ к.ю.н., доцент кафедры В.В. Терешкова
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ И.В. Зрилин
подпись, дата инициалы, фамилия

Красноярск 2021

Оглавление

Введение

В современном обществе, где информация, ее применение и доступность оказывают большое влияние на условия жизни людей, требуется широкое использование информационных технологий, которые позволяют обрабатывать огромные объемы информации и в том числе персональную информацию или иначе – персональные данные.

Регулирование безопасности информации и, в частности, защиты персональных данных осуществляется и на национальном, и на международном уровне. Вопросы, касающиеся защиты персональных данных традиционно рассматриваются как одна из сфер права на уважение частной жизни человека.

Правовым стартом для защиты персональных данных послужила Конвенция о защите физических лиц при автоматизированной обработке персональных данных 1981 г[1]. Конвенция, подчеркнув «приверженность свободе информации невзирая на границы и… уважение частной жизни и свободное распространение информации между народами», в качестве цели обозначила достижении большего единства между его членами, основанного, в частности, на уважении принципа господства права, а также соблюдении прав человека и основных свобод…с учетом увеличения трансграничного потока персональных данных».

Применительно к сети «Интернет», прежде всего вопрос о персональных данных стоит рассматривать в контексте использования интернет-покупок и социальных сетей. Последние уже перестали быть просто средством для общения и обменом повседневной информацией, а стали площадками, с помощью которых работают, знакомятся, учатся, занимаются бизнесом и благотворительной деятельностью.

В то же время субъекты персональных данных при использовании Интернет-ресурсов, в частности социальных сетей, самостоятельно указывают или оставляют о себе большое количество данных, относящихся к

[1] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981), [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/

персональным. Это может быть номер телефона, адрес с указанием места жительства, информация об учёбе или работе, место совершения покупок и прочее[2]. Такие данные и даже удалённые личные сообщения и переписки хранятся на серверах социальных сетей, могут быть истребованы правоохранительными органами на основании постановления суда. Это разделило общество на сторонников, которые утверждают, что это необходимость для обеспечения безопасности людей, и противников, считающих, что таким образом нарушается их право на тайну переписки[3].

Поэтому вопрос о безопасности личных данных пользователей сети «Интернет», которые зачастую должны оставаться недоступными посторонним лицам (таким же пользователям и даже операторам), представляется актуальным. Количество преступлений в этой сфере с каждым годом растет, и национальное законодательство просто не успевает за темпами движения прогресса. Все это говорит об актуальности данного вопроса, поскольку с каждым днем социум все больше внедряет в свою жизнь различные технологии, в том числе и технологии, связанные с Интернетом.

Объект исследования – отношения, возникающие между различными субъектами при осуществлении сбора, обработки, хранении и защиты персональных данных. Упор сделан на нормативный материал, что позволит изучить объект исследования с более объективной точки зрения.

Цель настоящего исследования заключается в рассмотрении механизма защиты персональных данных, выявлении ее специфических характеристик, анализе процедуры сбора, обработки и хранения персональных данных, а также поиска правовых и технических пробелов в данной сфере.

В связи с этим были поставлены такие задачи как:

---

[2]Бегларян М.Е., Пичкуренко Е.А. Безопасность персональных данных в современной России [Электронный ресурс]: Уголовная политика в сфере обеспечения здоровья населения, общественной нравственности и иных социально-значимых интересов, материалы 4-ой Международной научно-практической конференции. 2015. С. 24-28 – Режим доступа: http://elibrary.ru/, С. 24

[3]Беззубиков Д.А., Морозов М.В. Проблема защиты персональных данных в сети Интернет [Электронный ресурс]:Дневник науки. 2019. № 4 (28) – Режим доступа: http://elibrary.ru/, С. 127

1. Определить понятие и раскрыть признаки персональных данных;

2. Провести анализ существующих угроз безопасности персональных данных;

3. Охарактеризовать национальное и международное законодательство, и судебную практику, регулирующих защиту персональных данных;

4. Определить основные методы, меры и средства, с помощью которых осуществляется защита;

5. Рассмотреть применение этих методов и нормативных актов с целью соблюдения конкретных принципов защиты данных;

6. Исследовать рамки ответственности за нарушение правил работы с персональными данными.

Методологическую базу исследования составили всеобщие методы (диалектика и метафизика), общенаучные методы (анализ, синтез, системный и функциональный методы, логический), специальные методы (формально-юридический, сравнительно-правовой, историко-правовой).

Теоретическую базу исследования составили труды: А.Г. Абрамова, И.Л. Бачило, Д.А. Беззубиков, Д.В. Ворожбит, А.А. Григорьев, Р.В. Донец, М.О. Дудко, А.Б. Киселева, Д.К. Скалеух, К.В. Струков, А.Д. Фролова и др.

Нормативно-правовую базу исследования составили международно-правовые акты, международная судебная практика Европейского суда по правам человека и Суда Европейского союза, национальное законодательство Российской Федерации и других стран, судебная практика РФ и др.

Работа состоит из введения, двух глав, заключения и списка использованных источников.

Глава I. Информационная безопасность и персональные данные

1.1. Угрозы безопасности персональных данных и их виды

При функционировании любой информационной системы большую роль в ее эффективности играет ее защищенность. Если при получении, передаче, обработке, хранении и использовании информация о персональных данных защищена от случайного доступа или другой более серьезной угрозы, то можно с уверенностью говорить о безопасности персональных данных. Что же представляют собой угрозы безопасности персональных данных в целом? Для определения угроз персональным данным необходимо, прежде всего, установить, что подпадает под понятие «персональные данные».

Европейский суд по правам человека определяет персональные данные как «любую информацию об определенном или поддающемся определению физическом лице»[4].Это определение берет начало из Конвенции о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981 (Конвенция № 108)[5].

Также, Европейский суд по права человека в качестве персональных данных признает сведения о состоянии здоровья, ДНК, политической деятельности, судимости, местонахождении, а также сведения, содержащиеся в банковских документах, и любые сведения о лице, собранные и хранящиеся в различных базах данных[6], как устные, так и письменные сообщения или изображения[7]. Даже слюна, волосы или клетки человеческой ткани относятся к числу информации, являющейся персональными данными, так как они

---

[4] Аманн (Amann) против Швейцарии [Электронный ресурс]:Постановление Европейского Суда по правам человека от 16.02.2000 – Режим доступа: http://www.consultant.ru/, пункт 65

[5] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981), [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/, статья 2

[6] Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence, [Электронный ресурс]: сайт Европейского суда по правам человека – Режим доступа: https://www.echr.coe.int/, пункты 139-151

[7] Фон Ганновер (Принцесса Ганноверская) (Von Hannover) против Германии, [Электронный ресурс]: Постановление Европейского Суда по правам человека от 24.06.2004– Режим доступа: http://www.consultant.ru/

содержат генетическую информацию о человеке и позволяют идентифицировать конкретное лицо.

В иных случаях в определение входят только совокупность идентификаторов, например, имя, идентификационный номер, сведения о местоположении, идентификатор в режиме онлайн, признаки идентичности указанного физического лица, связанные с его физическим, психическим, экономическим, культурным или социальным состоянием[8].

В российском законодательстве персональные данные определяются как любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[9].

Российское законодательство включает в это понятие также ФИО, дату рождения, адрес местожительства или регистрации, социальное, имущественное, семейное положение, сведения о доходах, образовании, профессии, данные паспорта и т.п. Но в то же время, эти данные будут являться таковыми только в случае, если по ним можно прямо или косвенно определить конкретное физическое лицо.

Выделяют в специальную категорию персональных данных информацию о национальной и расовой принадлежности субъекта, о религиозных либо философских убеждениях, информацию о здоровье и интимной жизни субъекта, судимости.

При этом не всегда данная информация должна быть сокрыта под предлогом защиты персональных данных. Имеются исключения, которые называют общедоступными персональными данными, например, сведения о доходах работников органов государственной и муниципальной власти либо персональные данные, открыто выставленные самим субъектом[10].

---

[8] О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС [Электронный ресурс]: Регламент № 2016/679 Европейского парламента и Совета Европейского Союза(Принят в г. Брюсселе 27.04.2016)– Режим доступа: http://www.consultant.ru/, пункт 1 статьи 4

[9] О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ – Режим доступа: http://www.consultant.ru/, статья 3

[10] О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ – Режим доступа: http://www.consultant.ru/,статья 8

В российской судебной практике относят к числу персональных данных также информацию о Индивидуальном налоговом номере и СНИЛС[11], адресе электронной почты, если она связана с телефонному номеру (в противном случае не признается[12]), об уголовных делах в отношении определенных субъектов[13], о трудовой деятельности судьи[14], паспортных данных кроме случае, когда серия и номер паспорта идентифицируют бланк документа, а не физическое лицо[15], а также фотографии физического лица[16] и данные об IP-адресе[17].Некоторые российские юристы относят туда же личную подпись и электронную подпись[18].

Субъектами персональных данных являются физические лица. Это следует из определений, приведенных выше. Однако также отметим, что суды, в частности Европейский суд по правам человека, может рассматривать дело о нарушении интересов юридического лица, например, касательно обеспечения защиты личных данных и частной жизни работников[19].

---

[11] Апелляционное определение Санкт-Петербургского городского суда от 11.10.2017 по делу № 2-2998/2017, [Электронный ресурс]: сайт Санкт-Петербургского городского суда – Режим доступа: http://sankt-peterburgsky.spb.sudrf.ru/

[12] Решение Заельцовского районного суда г. Новосибирска № 2-1770/2018 ~ М-987/2018 М-987/2018 от 27 июня 2018 г. по делу № 2-1770/2018 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/

[13] Определение Верховного Суда РФ от 20.02.2019 № 303-ЭС19-56 по делу № А59-1219/2018 [Электронный ресурс]: сайт Судебные и нормативные акты РФ – Режим доступа: https://sudact.ru/

[14] Решение Верховного Суда РФ от 11.03.2013 № АКПИ13-61 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/

[15] Постановление Тринадцатого арбитражного апелляционного суда от 21 июня 2010 г. по делу № А56-4788/2010 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/

[16] Решение Октябрьского районного суда г. Красноярска № 2-3904/2019 2-3904/2019~М-966/2019 М-966/2019 от 26 августа 2019 г. по делу № 2-3904/2019 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/

[17] Решение Арбитражного суда Челябинской области по делу № А76-29008/2015 от 11.02.2016 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/

[18]Бачило И.Л. [Электронный ресурс]: Государство и право XXI в. Реальное и виртуальное. М. 2012. 280 с – Режим доступа: http://www.garant.ru/, С. 183

[19] «Бернх Ларсен холдинг АС» и другие (Bernh Larsen Holding AS and Others) против Норвегии [Электронный ресурс]: Постановление Европейского суда по правам человека от 14.03.2013 – Режим доступа: http://www.garant.ru/, пункт 107

Вопрос о защите персональных данных юридических лиц рассматривался в Судом ЕС. В деле Товарищество «Фолькер и Маркус Шеке» и Хартмунт Айферт против Земли Гессен (Volker und Markus Schecke GbR und Hartmut Eifert v. Land Hessen) Суд указывает, «юридические лица могут требовать защиту статей 7 и 8 Хартии Европейского Союза об основных правах от 2000 г[20], в связи с такой идентификацией только в том случае, если официальное название юридического лица идентифицирует одного или нескольких физических лиц[21].

Иными словами, положения о защите персональных данных относятся к юридическим лицам, если конкретного субъекта можно определить по названию этого юридического лица[22].

Далее возникает несколько вопросов: от каких именно угроз необходимо защищать персональные данные? Что вызывает данные угрозы? Какова их классификация?

Положения российского законодательства имеют свое определение термина «угрозы безопасности персональных данных». Угрозы безопасности персональных данных – это совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных[23].

---

[20] Об основных правах [Электронный ресурс]: Хартия Европейского Союза от 07.12.2000 – Режим доступа: http://www.garant.ru/, статьи 7 и 8

[21] Товарищество «Фолькер и Маркус Шеке» и Хартмунт Айферт против Земли Гессен (Volker und Markus Schecke GbR und Hartmut Eifert v. Land Hessen) [Электронный ресурс]: Решение Суда Европейского союза от 09.11.2010 2013 – Режим доступа: https://eur-lex.europa.eu/

[22] Абрамова А.Г. Международно-правовая защита персональных данных в сети Интернет: общие положения [Электронный ресурс]: Регион и мир. 2020. Т. 11. № 5. С. 51-58 – Режим доступа: http://elibrary.ru/, С. 52

[23] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 15.02.2008) [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/, раздел 1

Для определения способов, методов, направления и анализа рисков защиты необходимо классифицировать угрозы информационной безопасности. Поскольку формализовать описание всего множества угроз практически невозможно, ввиду сложности компьютерных систем и их зависимости от различных случайных факторов, то определяется не полный единый перечень угроз, а перечень классов угроз на основе отдельных признаков:

1. по видам возможных источников угрозы безопасности персональных данных (угрозы, возникшие ввиду умышленных или неосторожных действий внутренних или внешних лиц сети, возникшие ввиду внедрения аппаратных закладок и программ);

2. по способам реализации угроз (угрозы, связанные с несанкционированным доступом к персональным данным; с утечкой персональных данных по техническим каналам, связанные со специальным воздействием на систему персональных данных);

3. по виду несанкционированных действий, осуществляемых с персональными данными (угрозы, приводящие к нарушению конфиденциальности, приводящие к несанкционированному изменению, блокированию или уничтожению персональных данных);

4. по используемой уязвимости (угрозы, реализуемые с использованием уязвимости системного или прикладного программного обеспечения; уязвимостей протоколов сетевого взаимодействия и каналов передачи данных; уязвимости в технической защите и т.д.)[24].

При пользовании сети Интернет для приобретения товаров, работ или услуг через интернет-магазины, важно учитывать, что в данном случае

[24] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 15.02.2008) [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/, раздел 3

наиболее вероятными угрозами являются: утечка информации по техническим каналам и несанкционированный доступ к персональным данным[25].

Угрозы утечки информации по техническим каналам включают:

- утечку акустической (речевой) информации, которая возможна при наличии голосового ввода персональных данных или функций воспроизведения средствами акустики

- утечку видовой информации при просмотре с помощью оптических средств с экранов мониторов и технической обработке видео, графической и буквенно-цифровой информации и т.п[26].

Угрозы несанкционированного доступа состоят из:

- перехвата в процессе загрузки операционной системы идентификаторов или паролей

- модификации базовой системы ввода/вывода, перехват управления загрузкой

- уничтожения, копирования, перемещения, форматирования носителей информации и операционной системы или прикладной программы, с помощью специально разработанных программ просмотра и модификации реестра.[27]

В зависимости от предмета посягательства можно разделить угрозы безопасности персональных данных на следующие виды:

1. Взлом паролей (все персональные данные, сокрытые таким способом, попадают в руки к злоумышленникам);

2. Взлом электронной почты(зачастую аккаунты социальных сетей связаны с адресом электронной почты, поэтому взлом почтыувеличивает шансы злоумышленника на взлом паролей в социальных сетях).

3. Взлом банковских данных через интернет-магазин или другой сервис с онлайн-транзакциями, где пользователь сохранил данные своих банковских карт в личном кабинете.

---

[25] Киселева А.Б., Ильина Л.А. Анализ угроз безопасности персональных данных в интернет-магазинах [Электронный ресурс]: Аллея науки. 2017. Т. 1. № 8. С. 652-655 – Режим доступа: http://elibrary.ru/, С. 653

[26]Там же, С. 654

[27] Там же, С. 655

4. Загрузки на устройство вредоносного программного обеспечения, способного незаметно получать личную информацию, проводить слежку за действиями пользователя, осуществлять скрытую видео- и аудиозапись через устройство[28].

Отметим, что полностью надежных и защищенных систем персональных данных не существует. Вместе с тем, система защиты персональных данных увеличивает время доступа к информации прямо пропорционально своей сложности.

В эпоху развитых технологий одним из главных источников угрозы безопасности персональных данных является сама сеть «Интернет». Поэтому ввиду разнообразия форм общения в сети Интернет, на международном уровне больше внимания стало уделяться защите данных при работе и оказании услуг в сетях, поскольку объем информации при таких условиях вырастает до неограниченных масштабов.

Становится все сложнее осуществлять эффективный контроль над терабайтами информации, в том числе терабайтами персональных данных. Это становится одной из важнейших угроз в современном мире – огромные потоки информации, содержащие персональные данные, не поддаются контролю по причине своих объемов.

В то же время, вполне законным способом сбора и обработки персональных данных пользователей в сети Интернет чаще всего является использование, так называемых, файлов-cookies.

Это текстовых файлы, устанавливающиеся на жесткие диски пользователей и потребителей во время посещения веб-сайтов. Их использование обусловлено различными целями: анализ предпочтений интернет-покупателя, запоминание платежных реквизитов, сохранение индивидуальных настроек пользователя социальной сети или мессенджера.

[28]Пыжов Н.С., Беляева А.А., Шаханова М.В. Актуальные проблемы защиты персональных данных в сети Интернет [Электронный ресурс]: Научный электронный журнал Меридиан. 2020. № 2 (36). – Режим доступа: http://elibrary.ru/, С. 90-92.

Поэтому информация, собираемая с использованием файлов-cookies, может, как содержать, так и не содержать персональные данные субъекта.

Как правило, с файлами-cookies тесно связана таргетированная реклама, методика анализа данных, целью которой является создание профиля пользователя, наиболее отзывчивого к рекламным сообщениям[29]. Иными словами интернет-маркетологи отслеживают посещения сайтов и запросы в Интернет, определяя интересы и предпочтения субъекта.

Использование такой рекламы налагает на оператора в соответствии с российским законодательством обязанность получить предварительное согласие субъекта персональных данных[30].

Отметим, что использование файлов-cookies пользователь может ограничить настройками своего интернет-браузера или отказом в их применении при посещении веб-сайта, поскольку, согласно Директиве Европарламента и Европейского Совета 2002/58/ЕС от 12 июля 2002 года, должно быть гарантировано, «что хранение информации или получение доступа к информации, уже сохраненной на терминальном оборудовании абонента или пользователя, допускается только при условии, что заинтересованный абонент или пользователь дали свое согласие, будучи обеспеченными точной и полной информацией о целях обработки информации. Данное положение не должно препятствовать любому техническому хранению или доступу к информации с единственной целью осуществления передачи сообщения по сети электронной связи, или в случае наличия необходимости оказания провайдером услуги информационного общества соответствующих услуг по явно выраженному запросу абонента или пользователя»[31].

---

[29]Targeted marketing [Электронный ресурс]: The Dictionary Netlingo – Режим доступа: http://www.netlingo.com/word/targeted-marketing.php/

[30] О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ – Режим доступа: http://www.consultant.ru/, статья 15

[31]В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи [Электронный ресурс]:Директива Европейского Парламента и Совета Европейского Союза 2002/58/ЕС от 12.07.2002 (Директива о конфиденциальности и электронных средствах связи)– Режим доступа: http://www.garant.ru/, пункт 3 статья 5

Однако некоторые веб-сайты ограничивают возможность использования своих сервисов, если пользователь ограничил применение файлов-cookies. Это приводит к принуждению на дачу согласия по сбору и хранению части информации и персональных данных субъекта, что нарушает существующие принципы по работе с персональными данными. В связи с этим в определенных случаях файлы-cookies можно отнести к косвенным угрозам безопасности и конфиденциальности персональных данных.

Отдельно выделим такой вид интернет-угрозы, как фишинг (от английского слова«fishing» – рыбалка). Она заключается в прямом обмане пользователя с целью получить его персональные данные, в частности логины, пароли, номера телефонов или банковские данные[32].

Примером может послужить направление лицу электронного письма, выполненного и стилизованного под уведомление от официального администратора интернет-сервиса, онлайн-магазина или социальной сети, в котором сообщается о необходимости подтвердить свою учетную запись или банковские данные путем сообщения персональных данных или воспользоваться прилагаемой ссылкой на веб-страницу. Данную просьбу чаще всего мотивируют подозрением лица в мошеннических действиях или возникновением сторонних угроз. Настоящие действия в зависимости от тяжести последствий получения персональных данных обманутого лица признаются мошенническим преступлением и влекут уголовную ответственность.

Таким образом, сложно переоценить роль необходимости в защите личной информации в сети Интернет. В настоящее время на международном и национальном уровне установлены нормы направленные на создание базовой защиты персональных данных, а также соблюдения основных прав человека в

[32] Ефремов М.А., Калуцкий И.В., Таныгин М.О., Рудак И.И., Безопасность персональных данных, социальные сети и реклама в глобальной сети internet [Электронный ресурс]: Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2017. Т. 7. № 1 (22). С. 27-33 – Режим доступа: http://elibrary.ru/, С. 30

эпоху цифровых технологий. Но для защиты предмет должен быть четко обозначен.

Судебная практика конкретизирует и постоянно расширяет перечень о том, что может относиться к персональным данным. Однако этот перечень не является исчерпывающим – к персональным данным можно отнести практически любую информацию, если только она позволяет прямо или косвенно определить, идентифицировать конкретное лицо. Наличие закрытого перечня облегчило бы процесс правоприменения, но в современных условиях сформировать его практически невозможно. Аналогичная ситуация сложилась и в национальном законодательстве разных стран, в том числе и в законодательстве Российской Федерации.

Определение понятия, конкретных видов и классификаций угроз персональным данным регулируется на национальном уровне. В российском законодательстве существует большое разнообразие угроз безопасности персональных данных, которые можно разделить по видам и категориям в зависимости от источников, предмета, субъекта и сферы угроз. Главными угрозами являются несанкционированный доступ, умышленная или случайная несанкционированная передача персональных данных иным лицам (утечка), потеря и уничтожение персональных данных. Некоторые угрозы персональным данным в сети Интернет носят косвенный характер или создаются опасность только при наличии ряда условий, как например, чужие файлы-cookie, которые можно использовать с нарушением законодательства стран в сфере обработки персональных данных, а можно похитить или купить на черном интернет-рынке, тем самым заполучив полный доступ к информации ничего не подозревающего субъекта.

Иные угрозы основываются не на технической сфере, но на доверии и страхах пользователей сети, вынуждая обманным путем лицо самостоятельно раскрыть свои персональные данные без принуждения.

Защитить персональные данные от такого количества угроз без надлежащего правового регулирования не представляется возможным. В связи

с этим, возникает вопрос: как и какие акты регулируют защиту персональных данных на международном и национальном уровне?

1.2. Правовое регулирование безопасности персональных данных

Государства уже несколько десятилетий уделяют большое внимание защите относительно новой и постоянно развивающейся сфере человеческой жизни, совершенствуя правовое обеспечение безопасности персональных данных.

Ещё во второй половине 20-го века, до развития интернет-технологий, пришло понимание, что защита персональных данных требует внимания на законодательном уровне. Добиться полной, эффективной и комплексной защиты можно только совместными усилиями государств, создающих международные акты, поскольку оборот и обработка информации, в том числе персональных данных, все больше выходит за пределы отдельных стран.

В 1981 г. принята Конвенция № 108. Россия стала участницей Конвенции в 2006 году[33]. При создании этой Конвенции государства-члены исходили из факта увеличения трансграничного потока персональных данных, подвергающихся автоматизированной обработке, и свободы информации по распространению между народами, невзирая на границы[34].

Предмет регулирования Конвенции № 108 – защита персональных данных – уже на тот момент был тесно связан с положениями статьи 8 ЕКПЧ о праве каждого человека на уважение его личной и семейной жизни, его жилища и его корреспонденции. Конвенция № 108закрепляет для договаривающихся сторон обязанность по созданию надлежащего национального законодательства в сфере защиты персональных данных и принятию надлежащих мер с целью соблюдения установленных принципов в отношении каждого гражданина на

---

[33] О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс]: Федеральный закон от 19.12.2005 № 160-ФЗ – Режим доступа: http://www.consultant.ru/

[34]Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981), [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/, преамбула

территории государств-членов[35] и недопущения случайного или несанкционированного доступа, уничтожения, распространения персональных данных или их случайной потери[36].

Конвенция закрепила принципы обработки и защиты персональных данных:

a) справедливая и законная основа для сбора и обработки данных;

b) хранение для определенных и законных целей, запрещено использование иным образом, несовместимым с этими целями;

c) собираемые и обрабатываемые данные являются адекватными, относящимися к делу и не чрезмерными для целей их хранения;

d) точность данных и, когда это необходимо, их обновление;

e) данные сохраняются в форме, позволяющей идентифицировать субъекты данных, не дольше, чем это требуется для целей хранения этих данных[37].

Конвенция № 108 послужила основой последующего развития правового регулирования защиты персональных данных в эпоху, когда почти каждый человек получил возможность выхода в сеть Интернет. В связи с этим сохранность и конфиденциальность персональных данных по всему миру подвергаются еще большему вмешательству со стороны социальных сетей, мессенджеров, интернет-сайтов и т.д.

Кроме того, регулирование защиты персональных данных осуществляется со стороны ООН, Совета Европы и Европейского союза и иных

---

[35]Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981), [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/,статья 4

[36]Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981), [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/, статья 7

[37] Там же, статья 5

межгосударственных органов путем принятия международных актов и подписания международных договоров[38].

К настоящему времени правовое регулирование в данной сфере осуществляется комплексом актов, которые разнятся по юридической силе: часть из них обязательна для исполнения, часть носит рекомендательный характер.

В рамках ЕС принята Директива 95/46/ЕС Европарламента и Европейского Совета «О защите физических лиц при обработке персональных данных и о свободном перемещении таких данных» от 24.10.1995[39].

Главное сферой регулирования данной Директивы стала обработка персональных данных независимо от того, автоматизирована ли такая обработка или нет. Как и Конвенция № 108, Директива закрепляла обязанность участников по созданию национального законодательства в сфере защиты персональных данных, отвечающего требованиям Директивы.

Основным регулирующим актом в ЕС является Регламент «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС» от 27.04.2016 № 2016/679, также известный как Общий регламент защиты персональных данных Европейского Союза, принятый в 2016 году и вступивший в силу в 2018 году[40].

Данный Регламент отменил действие прежней Директивы 95/46/ЕС Европарламента и Европейского Совета «О защите физических лиц при

---

[38] Фомина Л.Ю. Международные стандарты защиты персональных данных в условиях информационного общества [Электронный ресурс]: Международное право. 2019. № 4. С. 50-59 – Режим доступа: https://cyberleninka.ru/, С. 50

[39] О защите физических лиц при обработке персональных данных и о свободном перемещении таких данных [Электронный ресурс]: Директива 95/46/ЕС Европарламента и Европейского Совета от 24.10.1995 – Режим доступа: http://www.garant.ru/

[40] О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС [Электронный ресурс]: Регламент Европейского Парламента и Совета Европейского Союза № 2016/679 от 27.04.2016– Режим доступа: http://www.garant.ru/

обработке персональных данных и о свободном перемещении таких данных» от 24.10.1995[41].

Общий регламент достиг цели по сведению положений двадцати семи национальных регулирований защиты данных в единый регламент, улучшил правила передачи корпоративных данных за пределы ЕС[42].

Кроме того, Общий регламент установил, что новые правила, регулирующие защиту персональных данных, применялись ко всем юридическим лицам, не входящим в ЕС, и не имеющим каких-либо представительств в ЕС, при условии, что ими осуществляется обработка данных граждан Европейского Союза. Это является одним из самых больших изменений в новом регулировании защиты персональных данных[43].

В рамках Европы регулирование также осуществляется через принятие специальных законодательных актов. В частности был принят ряд специальных актов, регулирующих защиту персональных данных в конкретных сферах[44].

---

[41]Талапина Э.В. Защита персональных данных в цифровую эпоху [Электронный ресурс]: Труды Института государства и права РАН. 2018. Т. 13. № 5. С. 117–150 – Режим доступа: http://elibrary.ru/

[42] Постникова Е.В. Некоторые аспекты правового регулирования защиты персональных данных в рамках внутреннего рынка Европейского союза [Электронный ресурс]: Право. Журнал Высшей школы экономики. 2018. № 1. С. 234–254 – Режим доступа: http://elibrary.ru/

[43] Чурилов А.Ю. Принципы Общего регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации [Электронный ресурс]: Вестник Омской юридической академии. 2019. № 1. С. 29–35 – Режим доступа: http://elibrary.ru/

[44] Об универсальной услуге и правах пользователей в отношении сетей и услуг электронной связи [Электронный ресурс]: Директива 2002/22/ЕС Европейского Парламента и Совета от 07.03.2002 (Директива об универсальной услуге) – Режим доступа: http://www.garant.ru/;В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи [Электронный ресурс]: Директива Европейского Парламента и Совета Европейского Союза 2002/58/ЕС от 12.07.2002 (Директива о конфиденциальности и электронных средствах связи) – Режим доступа: http://www.garant.ru/;О защите физических лиц при обработке персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний и о свободном обращении таких данных, а также об отмене Рамочного Решения Совета Европейского Союза № 2008/977/JHA [Электронный ресурс]: Директива Европейского парламента и Совета Европейского союза от 27 апреля 2016 г. № 2016/680 – Режим доступа: http://www.garant.ru/;О защите физических лиц при обработке персональных данных, осуществляемой учреждениями, органами, службами и агентствами Союза, и о свободном обращении таких данных, а также об отмене Регламента (ЕС) 45/2001 и Решения 1247/2002/ЕС [Электронный ресурс]: Регламент Европейского парламента и Совета Европейского Союза от 23 октября 2018 г. № 2018/1725 – Режим доступа: http://www.garant.ru/

В качестве значимого источника регулирования защиты персональных данных выделяются решения Европейского суда по правам человека, поскольку создаваемая судом практика по этим вопросам становится рекомендациями для государств при защите личной информации граждан в Интернете.

ЕСПЧ в решениях по делам о нарушении тайны личной жизни и в том числе конфиденциальности персональных данных, указывает, что обработка персональных данных должна быть справедливо и законной, основываться на информировании затрагиваемых субъектов персональных данных.

На национальном уровне, на котором происходило развитие защиты персональных данных ввиду обязывания со стороны международных актов, можно отметить, что уже после того, как в 1983 году Конституционный Суд Федеративной Республики Германия отметил потребность в национальных законодательных актах, регулирующих защиту персональной информации, в стране был принят Федеральный закон «О защите личных данных»[45]. На настоящий момент он считается одним из наиболее совершенных в сравнении с законодательными актами других стран в этой сфере[46].

Во второй половине 20-го века многие страны, такие как Финляндия, Нидерланды, Великобритания, Франция, Венгрия, также приняли на национальном уровне собственные акты, регулирующие защиту личной информации, относящейся к персональным данным[47].

Вопросы информационной безопасности в Российской Федерации закреплены на конституционном уровне. Статья 23 Конституции РФ устанавливает неприкосновенность частной жизни, личной и семейной тайны,

---

[45] О защите личных данных (Bundesdatenschutzgesetz) [Электронный ресурс]: Федеральный закон Германии от 20.12.1990 – Режим доступа: http://www.gesetze-im-internet.de/

[46]Скалеух Д.К. Зарубежный опыт правового регулирования защиты персональных данных в сети Интернет [Электронный ресурс]: Актуальные проблемы экономики, управления и права. Сборник научных статей по материалам Всероссийской научно-практической конференции, посвященной Дню Конституции Российской Федерации. Ростов-на-Дону. 2020. С. 362-367. – Режим доступа: http://elibrary.ru/, С 362

[47]Скалеух Д.К. Зарубежный опыт правового регулирования защиты персональных данных в сети Интернет [Электронный ресурс]: Актуальные проблемы экономики, управления и права. Сборник научных статей по материалам Всероссийской научно-практической конференции, посвященной Дню Конституции Российской Федерации. Ростов-на-Дону. 2020. С. 362-367. – Режим доступа: http://elibrary.ru/, С 362

тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Пункт 4 ст. 29 указывает на свободу искать, получать, передавать, производить и распространять информацию любым законным способом.

После ратификацииКонвенции № 108 в 2006 г принят Федеральный закон № 152-ФЗ «О персональных данных»[48], основой которого и стала Конвенции № 108. Федеральный закон регулирует отношения, которые связанны с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации[49].

Целью закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну[50].

Федеральный закон определяет государственный орган, контролирующий обработку персональных данных – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций[51].

Однако закон не приспособлен к регулированию защиты персональных данных именно в сети «Интернет». Так, согласно положениям Закона[52], действия по созданию ложной учетной записи в социальной сети на имя

---

[48] О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ – Режим доступа: http://www.consultant.ru/

[49]Там же, пункт 1 статьи 1

[50]О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ – Режим доступа: http://www.consultant.ru/, статья 2

[51] Сочнев А.В. Защита персональных данных в сети «Интернет» [Электронный ресурс]: Молодежь и XXI век. 2016. Материалы VI Международной молодежной научной конференции. В 4-х томах. 2016. С. 164-167 – Режим доступа: http://elibrary.ru/, С. 165

[52] О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ – Режим доступа: http://www.consultant.ru, пункт 3 статьи 3

другого человека с использованием минимума его персональных данных (ФИО) будут относиться к обработке персональных данных (в частности, использование и хранение). Другая норма Закона[53] строго регламентирует, что обработка персональных данных без согласия субъекта не допускается. Но в силу объективных обстоятельств будет практически невозможно отследить факт нарушения вышеуказанных положений в связи со спецификой природы сети «Интернет»[54].

Нельзя не отметить, что помимо Федерального закона, в Российской Федерации для правового регулирования вопроса о защите личной информации граждан на национальном уровне принят ряд подзаконных актов»[55].

Таким образом, защита персональных данных, в том числе и в сети Интернет во многом зависит от надлежащего и полного правового регулирования как на национальном, так и на международном уровне.

В мире издано множество нормативных и подзаконных актов, затрагивающих и общие и специальные сферы защиты персональных данных. Основой послужила Конвенция № 108, изданная в 1981 году. В ней закрепили основные принципы защиты информации, которые применимы и на

---

[53]О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ – Режим доступа: http://www.consultant.ru, пункты 1 и 2 статьи 10

[54] Сочнев А.В. Защита персональных данных в сети «Интернет» [Электронный ресурс]: Молодежь и XXI век. 2016. Материалы VI Международной молодежной научной конференции. В 4-х томах. 2016. С. 164-167 – Режим доступа: http://elibrary.ru/, С. 166

[55]Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: Постановление Правительства Российской Федерации от 01.11.2012 № 1119 – Режим доступа: http://www.garant.ru/;Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации [Электронный ресурс]: Постановление Правительства Российской Федерации от 15.09.2008 № 687 – Режим доступа: http://www.garant.ru/;Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных [Электронный ресурс]: Постановление Правительства Российской Федерации от 06.07.2008 № 512 – Режим доступа: http://www.consultant.ru/; Об утверждении Положения о персональных данных государственного служащего Российской Федерации и ведении его личного дела [Электронный ресурс]: Указ Президента Российской Федерации от 30 мая 2005 г. № 609 – Режим доступа: http://www.consultant.ru/;Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 14.02.2008) [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/

сегодняшний день, а также обязательства для стран-участников по созданию национальной законодательной базы.

Защита персональных данных регулируется комплексом актов, которые разнятся по юридической силе: часть из них обязательна для исполнения, часть носит рекомендательный характер. Однако Европейский союз прошел долгий путь по развитию собственного правового регулирования в указанной сфере. Как итог: единый общий акт сменил десятки директив и регламентов, что позволило ЕС унифицировать и привести воедино практически все общие положения, связанные с защитой персональных данных.

Кроме того, значительное влияние на развитие нормативного регулирования в этой сфере имеет судебная практика Европейского суда по правам человека, поскольку вопрос защиты тесно связан с правом на уважение частной жизни человека.

Анализ количества решений ЕСПЧ за последние 30 лет указывает, что в законодательстве ряда стран есть ряд правовых пробелов, требующих урегулирования. К сожалению, в том числе российское законодательство, состоящее из единственного федерального закона и ряда подзаконных актов технической направленности, не успевает за ростом активности граждан в Интернете, осуществляя регулирование в данной сфере актами, плохо применимыми к деятельности в сети Интернет. Похожая ситуация наблюдается и в других не европейских странах.

Это указывает на то, что общие положения как национального, так и международного уровня, касательно защиты персональных данных сложно назвать достаточными для обеспечения эффективного уважения частной жизни в сети Интернет. Международный характер сети Интернет, большое разнообразие вариантов ее использования и применения требуют существенного изменения и дополнения регулирования со стороны, как государств, так и самих пользователей. Поэтому у законодателей остается еще много направлений, в которых необходимо провести соответствующее нормативно-правовое регулирование, в том числе и на международном уровне.

Глава II. Основные методы и средства защиты персональных данных

2.1. Обеспечение достоверности и сохранности персональных данных

Большую роль играет степень важности той или иной информации – от этого зависит, какие методы защиты должны применятся. Данные о дате рождения в социальной сети и данные о количестве денежных средств на электронном банковском счете охраняются разными методами с разной степенью защиты.

Статья 5 Общего регламента защиты персональных данных Европейского союза[56] и Конвенции № 108[57], а также Федерального закона «О персональных данных»[58] устанавливают ряд общих принципов по обработке любых персональных данных. Среди них особо выделяются такие принципы как (достоверность) персональных данных, их сохранность и конфиденциальность.

В связи с применением разных методов защиты персональных данных, достигается соблюдение вышеупомянутых принципов по защите персональных данных, в том числе в сети Интернет.

Внимание государств к защите персональных данных, прежде всего, выражается в разработке систем мер безопасности этих данных, содержащих различные методы. На основании категорий для защиты персональных данных меры рассматривают как внутренние и внешние.

К первым относятся: проведение различных профилактических работ с сотрудниками о предупреждении разглашения персональных данных; выявление, предупреждение и устранение нарушений по защите персональных данных; ограничение числа работников с доступом к данным.

---

[56] О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС [Электронный ресурс]: Регламент Европейского Парламента и Совета Европейского Союза № 2016/679 от 27.04.2016 – Режим доступа: http://www.garant.ru/, статья 5

[57] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981), [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/, статья 5

[58] О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ – Режим доступа: http://www.consultant.ru/, статья 5

Ко вторым относят: назначение сотрудника, ответственного за организацию обработки персональных данных; введение различных технических средств охраны информации[59].

Система безопасности включает в себя как программно-технические, так и организационно-административные методы. В литературе можно встретить другую классификацию, включающую программные, физические, аппаратные, организационные методы[60].

Физические методы реализуются через создание службы охраны, систем защиты окон и дверей, установки сигнализаций и видеонаблюдения, поскольку физические методы защиты направлены на физическое препятствование доступу к персональным данным[61].

Программно-технические или же программные и аппаратные методы выражены в реализации за счет использования различных по типу устройств и компьютерных программ. Они способны предотвращать проникновение в системы и сети, или, если проникновение все же случилось, препятствуют доступу к данным, в том числе с помощью маскировки данных, контроля доступа, шифрования информации, удаления остаточных данных (временных файлов) и т.д.

Организационно-правовые методы затрагивают правовой аспект защиты персональных данных: как правовое регулирование на национальном и международном уровне путем разработки и внедрения нормативно-правовых актов и регламентов, так и создание и исполнение правил работы с персональными данными, устанавливаемых конкретной организацией или социальной сетью.

---

[59] Геращенко О.М., Капралова Н.Н. Защита персональных данных в информационных системах методом обезличивания [Электронный ресурс]: Уголовно-исполнительная система сегодня: взаимодействие науки и практики. Материалы юбилейной XX Всероссийской научно-практической конференции. 2020. С. 255-257 – Режим доступа: http://elibrary.ru/, С. 256-257

[60]Сыргашева Т.Н. Методы и средства защиты персональных данных [Электронный ресурс]: NovaUm.Ru. 2018. № 16. С. 353-354. – Режим доступа: http://elibrary.ru/, С. 353

[61]Там же

Например, вовремя регистрации на веб-сайте или в социальной сети субъект ставит отметку о своем согласии на обработку предоставленных им персональных данных[62]. Тем самым субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе[63]. Отметим, что отечественная судебная практика возлагает бремя доказывания о наличии такого согласия на оператора[64].

Применение организационно-правовых методов позволяет собирать и обрабатывать персональные данные с соблюдением принципа точности и актуальности, а также защитой от неоправданного использования, утери, разрушения.

Достоверность, точность и актуальность данных может быть нарушена ввиду помех, технических сбоев, ошибок программ или людей (персонала, пользователей), поскольку, как указывалось в параграфе 1.1, на настоящее время по миру через сеть Интернет собирается, обрабатывается, передается, анализируется и используется огромнейший массив персональных данных, за верностью которого сложно осуществлять полный контроль.

Организационными методами повышения достоверности и сохранности персональных данных можно считать:

1) учет и хранение информационных массивов персональных данных;

2) контроль качества работы операторов, системных администраторов и обслуживающего персонала;

3) организация труда операторов, системных администраторов и обслуживающего персонала, обеспечивающая уменьшение возможностей

---

[62]Ворожбит Д.В. Особенности защиты персональных данных пользователей Интернет-ресурсов [Электронный ресурс]: Работы членов студенческого научного общества СЮИ ФСИН России. Сборник статей. Самара. 2019. С. 34-38., – Режим доступа: http://elibrary.ru/, С. 35

[63] О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ – Режим доступа: http://www.consultant.ru/, пункт 1 статьи 9

[64] Решение Заельцовского районного суда г. Новосибирска № 2-1770/2018 ~ М-987/2018 М-987/2018 от 27 июня 2018 г. по делу № 2-1770/2018 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/

нарушения им требований к достоверности и сохранности персональных данных.

Большинство ошибок являются синтаксическими (связаны с опечатками в массивах данных), семантическими (связаны с нарушением смыслового значения, логичности и непротиворечивости друг другу) и прагматическими (связаны с актуальностью, необходимостью и целесообразностью собираемых и обрабатываемых персональных данных)[65].

Европейский суд многократно рассматривал дела, в которых нарушено право заявителя на частную жизнь (статья 8 ЕКПЧ) именно по причине несоблюдения принципа достоверности (точности) обрабатываемых и хранящихся персональных данных.

В деле Ротару против Румынии, о заявителе государственными службами систематически копилась информация о его жизни, в частности о его учебе, политической деятельности и судимости, часть которой была собрана более пятидесяти лет назад. Указанная публичная информация оказалась недостоверной и повредила репутации заявителя.

Суд указал, что «систематический сбор и хранение публичной информации службами безопасности в отношении отдельных лиц представляет собой вмешательство в частную жизнь данных лиц, даже если сбор такой информации касался исключительно профессиональной или общественной деятельности лица»[66].

По указанному делу Суд пришел к выводу, что «законодательство регулирующее сбор и архивирование данных не содержит необходимых гарантий»[67].Государство не обеспечило соблюдение принципа достоверности (точности) собираемых и хранимых персональных данных заявителя; На ответственных органах не лежит обязанность по проверке и уточнению

---

[65] Петров Е.О., Бажин К.А. Защита персональных данных [Электронный ресурс]: Кафедра информационной безопасности. ТюмГУ. Тюмень. 2009 – Режим доступа: https://www.bestreferat.ru/referat-397328.html/

[66] Ротару (Rotaru) против Румынии [Электронный ресурс]: Постановление Европейского Суда по правам человека от 04.05.2000 – Режим доступа: http://www.garant.ru/, п. 43-44

[67] Там же

хранящихся данных (особенно тех, что были собраны в отдаленном прошлом) с целью избежания нарушения прав граждан.

В российском судебной практике принцип достоверности (точности) персональных данных нашел применение при определении судами, что можно относить к персональным данным.

К примеру, российские суды указывают, что информация в сети Интернет не представляет собой сведения о персональных данных лица в случае, когда она не соответствует принципу точности, в частности, «если при регистрации пользователя в социальной сети владелец данного интернет-сервиса не проверяет правильность и точность указанных данных об имени, фамилии, отчестве, дате рождения. Соответственно, указанная информация (ФИО, дата рождения) не является персональными данными, подлежащими защите в соответствии с Федеральным законом «О персональных данных»[68].

Иными словами, суды определили, что любые неподтвержденные данные не могут считаться персональными и не подлежат соответствующей защите.

К сфере обеспечения достоверности (точности) и сохранности персональных данных можно отнести вопрос о корреспондирующим правам обязанностям по уточнению и удалению определенной информации и персональных данных по требованию их субъекта (последнее – так называемое, право на забвение или «цифровая смерть»), поскольку исполнение этих обязанностей операторами ведет к соблюдению принципа точности и, как может сперва показаться, нарушению принципа сохранности персональных данных. Впервые это право было закреплено в Директиве 95/46/ЕС от 24.10.1995[69].

---

[68] Постановление Тринадцатого арбитражного апелляционного суда от 01.06.2015 № 13АП-10709/2015 по делу № А56-75017/2014 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/

[69] О защите физических лиц при обработке персональных данных и о свободном перемещении таких данных [Электронный ресурс]: Директива 95/46/ЕС Европарламента и Европейского Совета от 24.10.1995 – Режим доступа: http://www.garant.ru/

Решающим моментом для начала регулирования права на забвение в сети Интернет стало решение Суда ЕС[70]. Суд указал, что «деятельность поисковой системы по поиску, автоматической индексации, временному хранению, ранжированию информации и предоставлению доступа к ней является деятельностью по обработке персональных данных и субъект персональных данных праве требовать, чтобы соответствующая информация не была доступна для широкой публики путем ее включения в индекс поисковых результатов»[71].

Право на забвение подразумевает под собой право субъекта требовать уничтожения неактуальной, неверной или неточной информации о себе из информационной системы или сети Интернет[72].

На европейском уровне этот вопрос аналогично урегулирован в разделе 3 Общего регламента защиты персональных данных Европейского союза[73], где закреплены подобные права субъекта и обязанности оператора по уточнению и/или уничтожению данных, что и в российском законе.

В российском законодательстве обязанность по уточнению или уничтожению персональных данных при определенных условиях закреплена в статье 21 Федерального закона «О персональных данных», согласно которой при неточности персональных данных, невозможности обеспечить правомерность обработки персональных данных, достижении цели обработки или отзыве субъектом персональных данных своего согласия на обработку,

---

[70]Чагин И.Б., Юрковский А.В. К вопросу о механизме реализации права на забвение в сети Интернет [Электронный ресурс]: Академический юридический журнал. 2018. № 3 (73). С. 41-47 – Режим доступа: http://elibrary.ru/, С.41

[71]Google Spain S Land Google Inc. vs Agenda Espacola de Protecciynde Datos (AEPD) and Mario Costeja Gonzalez [Электронный ресурс]: Решение Суда ЕС от 13.05.2014 – Режим доступа: http://curia.europa.eu/juris/

[72] Струков К.В. Право на забвение в сети Интернет: понятие и перспективы развития [Электронный ресурс]: Actual science. 2017. Т. 3. № 2. С. 55-57 – Режим доступа: http://elibrary.ru/, С.55

[73] О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС [Электронный ресурс]: Регламент Европейского Парламента и Совета Европейского Союза № 2016/679 от 27.04.2016 – Режим доступа: http://www.garant.ru/, статьи 16 и 17

оператор обязан соответственно уточнить персональные данные, уничтожить такие персональные данные, прекратить обработку и уничтожить данные[74].

Например, в деле Шимоволос против Российской Федерации персональные данные и информация о перемещении и задержании правозащитника была внесена в базу данных, созданную на основании министерского приказа, который не был опубликован[75].

Суд усмотрел нарушение статьи 8, так как «создание и ведение базы данных, содержащей имя заявителя, и порядок её функционирования регулировались ведомственными приказами, которые никогда не были опубликованы и никаким иным образом не были доступны общественности. Следовательно, общественность не могла знать, почему лицо было внесено в эту базу данных, как долго хранилась информация о нем, какая информация там фигурировала, каким образом она хранилась и использовалась, и кто имел над ней контроль»[76].

Европейский суд расценил это как достаточные основания для обоснованности требований заявителя по удалению его персональных данных из базы данных. Тем самым заявитель реализовал свое право на уничтожение неточной и неверной информации, а государство не исполнило соответствующую обязанность.

Подводя итог, отметим, что существует большое количество методов, собранных в различные классификации и группы с целью наилучшего, эффективного и адекватного применения средств защиты персональных данных. Они включают в себя разнообразные меры, но преследуют единую цель – защиту персональных данным путем соблюдения установленных в законах и международных актах принципов, таких как достоверность или точности персональных данных, их сохранность и конфиденциальность.

---

[74]О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ – Режим доступа: http://www.consultant.ru/, статья 21

[75]Шимоволос против Российской Федерации [Электронный ресурс]: Постановление Европейского суда по правам человека от 21.06.2011 – Режим доступа: http://www.consultant.ru/

[76]Там же, пункт 83

Принципы достоверности (точности) и сохранности персональных данных рассматриваются как в национальных, так и в международных актах бок о бок. Их нарушение является недопустимым за небольшим числом исключений, предусмотренных законами или определенных судами. Например, в целях борьбы с терроризмом или иными подобными целями.

Как международная, так и российская судебная практика полна примеров рассмотрения дел, в которых судами рассматривается вопрос о нарушении прав лица ввиду несоблюдения принципа точности (достоверности) содержания персональных данных.

Отдельной категорией споров являются обоснованные требования субъектов персональных данных по удалению информации о себе. Так называемое право на цифровую смерть предусмотрено в российском Федеральном законе и Общем регламенте ЕС в качестве исключения из принципа сохранности данных. В таком случае уничтожение персональных данных не будет считаться нарушением принципа сохранности, установленного в настоящее время международными и национальными актами, поскольку оно происходит с согласия и/или по требованию самого субъекта.

2.2. Обеспечение конфиденциальности персональных данных

Статья 7 Федерального закона «О персональных данных» устанавливает обязанность операторов не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных[77]. Следовательно, конфиденциальность предполагает необходимость предотвращения разглашения персональной информации третьим лицам.

Очень важно поддерживать сложный баланс между конфиденциальностью и открытостью данных. Именно поэтому одним из важнейших принципов является конфиденциальность данных. В случае

[77] О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ – Режим доступа: http://www.consultant.ru/, статья 7

нарушения конфиденциальности существует вероятность изменения с целью дезинформации, случайного или преднамеренного уничтожения, а также несанкционированного использования персональных данных, что может привести к самым различным проблемам и ущербу субъектов персональных данных.

Отдельно выделяют метод защиты персональных данных от нарушения конфиденциальности, называемый обезличивание персональных данных.

Обезличивание персональных данных – это действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных[78].

В соответствии с приказом Роскомнадзора от 05.09.2013 №996 «Об утверждении требований и методов по обезличиванию персональных данных»[79] можно выделить несколько методов обезличивания персональных данных, где каждый из них отличается особым набором свойств и характеристик, например:

– введение идентификаторов, отличающееся тем, что данные остаются полными, структурированными, целостными, но при этом не анонимными;

– изменение состава или семантики данных, при которой теряется полнота и целостность;

– декомпозиция, по характеристикам схожая с введением идентификаторов, т.к. лишена только анонимности.

– перемешивание, считающееся самым лучшим методом обезличивания данных, поскольку при перемешивании сохраняются полнота, целостность, структурированность, применимость в любой момент, а также соблюдается анонимность[80].

---

[78] О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ – Режим доступа: http://www.consultant.ru/, статья 7, пункт 9 статьи 3

[79] Об утверждении требований и методов по обезличиванию персональных данных [Электронный ресурс]: Приказ Роскомнадзора от 05.09.2013 №996 – Режим доступа: http://www.consultant.ru/

[80] Геращенко О.М., Капралова Н.Н. Защита персональных данных в информационных системах методом обезличивания [Электронный ресурс]: Уголовно-исполнительная система сегодня: взаимодействие науки и практики. Материалы юбилейной XX Всероссийской

Следовательно, обезличивание персональных данных достаточно эффективно обеспечивает безопасности персональных данных, поскольку при соблюдении ряда условий позволяет сохранить их полноту и целостность, при этом, не требуя создания конфиденциальности.

Конфиденциальность достигается также за счет комплексных методов защиты (программно-технических и организационно-административных), например, комплекс организационно-правовых методов, регулирующих процессы сбора, обработки и использования персональных данных на основе нормативно-правовых актов государств, защита от утечки, криптографическая защита (в первую очередь шифрование), защита от несанкционированного доступа посторонних лиц (разграничение доступа)[81].

Одним из основных способов по разграничению доступа для защиты конфиденциальности персональных данных в сети Интернет является идентификация, аутентификация и авторизация субъекта доступа. При организации доступа к объектам персональных данных (получении доступа к программам и конфиденциальным персональным данным) осуществляется ряд совместных действий:

1. Конкретный субъект доступа определяется из множества других субъектов путем сообщения необходимых сведений (идентификация). Обычно это логин, имя, фамилия, псевдоним, номер телефона или адрес электронной почты. Такие данные могут быть не засекречены или известны только системному администратору.

2. Подтверждается личность субъекта за счет сообщения секретных сведений (аутентификация). Под секретными сведениями понимается информация, известная только субъекту доступа (пароль, пин-код, кодовое слово и т.п.), или признак, присущий только субъекту доступа (отпечаток пальца, рисунок сетчатки глаза, черты лица и иные биометрические данные).

научно-практической конференции. 2020. С. 255-257 – Режим доступа: http://elibrary.ru/, С. 255-256

[81] Акулов О.А., Медведев Н.В. Информатика: базовый курс [Электронный ресурс]: учебник для студентов вузов, бакалавров, магистров. - 4-е изд., стер. - Москва: Омега-Л, 2007 – Режим доступа: https://may.alleng.org/d/comp/comp220.htm/, С. 533

3. субъект получает право на доступ к персональным данным и распоряжение ими (авторизация).

Пример идентификации, аутентификации и авторизации можно наблюдать ежедневно – таким способом осуществляется доступ к учетной записи социальной сети или банка.

Основным исключением из принципа конфиденциальности являются персональные данные пользователей, доступ к которым имеет неограниченный круг лиц по согласию самого субъекта[82].

К вопросу о конфиденциальности персональных данных также можно отнести обязанности лиц, собирающих и обрабатывающих данные. Эти обязанности, прежде всего, направлены на защиту частной жизни.

Из части 2 названной статьи следует, что, прежде всего, цель статьи – это защита человека от произвольного несанкционированного вмешательства и доступа к персональным данным со стороны публичных властей.

В то же время действие этой статьи не ограничивается лишь необходимостью сдерживания публичных властей от вмешательства. На государство возлагаются также позитивные обязательства с целью обеспечить надлежащую защиту частной жизни, даже когда оно не участвует в сборе и обработке персональных данных.

Это означает, что включаются меры не только со стороны государственных органов, но и между отдельными лицами (так называемый горизонтальный эффект Конвенции), например, между интернет-пользователем и провайдером, обеспечивающим доступ к определенным сайтам. Иными словами, при нарушении прав на частную жизнь частного лица иным частным лицом, государство обязано учитывать баланс интересов двух лиц с целью принятия справедливого и законного решения.

---

[82]Ворожбит Д.В. Особенности защиты персональных данных пользователей Интернет-ресурсов [Электронный ресурс]: Работы членов студенческого научного общества СЮИ ФСИН России. Сборник статей. Самара. 2019. С. 34-38., – Режим доступа: http://elibrary.ru/, С. 36

Известным примером этого является дело «K.U. против Финляндии»[83]. Обстоятельства дела заключались в следующем. Неустановленное лицо разместило объявление в сети Интернет от имени несовершеннолетнего подростка без его согласия. В объявлении указывались его возраст и год рождения, приводилось подробное описание его физических характеристик, ссылка на интернет-страницу в социальной сети, где была его фотография, а также номер телефона с ошибкой в одной цифре. В объявлении утверждалось, что он ищет интимного знакомства с мальчиком своего возраста или старше.

Интернет-провайдер отказался раскрыть личность автора, сославшись на конфиденциальность. Законодательство Финляндии, действительно, запрещало операторам раскрывать личности пользователей. Это позицию поддержали и национальные суды Финляндии.

Европейский суд, напротив, отметил, что «как общественный интерес, так и защита интересов жертв преступлений, совершенных в отношении их физического или психологического благополучия, требуют наличия средства правовой защиты, позволяющего выявлять и предавать суду фактического правонарушителя»[84].

Поэтому несмотря на то, что свобода выражения мнения и конфиденциальность коммуникаций обязаны учитываться, пользователи телекоммуникаций и интернет-услуг должны иметь гарантии неприкосновенности личной жизни и свободы выражения мнения. Такие гарантии не могут быть абсолютными, и при необходимости государство должно отступать перед иными законодательными императивами, такими как поддержание порядка и предотвращение преступлений или защита прав и свобод других лиц[85].

---

[83] K.U. против Финляндии [Электронный ресурс]: Постановление Европейского суда по правам человека от 02.12.2008 – Режим доступа: http://www.garant.ru/
[84] Там же, пункт 47
[85] Там же, пункт 49

Суд подчеркнул, что «дети и другие уязвимые лица заслуживают большей государственной защиты в форме эффективного сдерживания от таких серьезных вмешательств в основные аспекты их личной жизни»[86].

Законодательная власть, таким образом, должна обеспечить основы для совмещения этих конкурирующих интересов. Соответственно, государство не смогло защитить право заявителя на уважение его личной жизни, предоставив приоритет требованиям конфиденциальности по сравнению с его физическим и нравственным благополучием[87].

В то же время, позитивные обязательства государства возникают не в каждом отдельно взятом случае, а когда нарушаются справедливое равновесие или баланс между интересами общества в целом и отдельного лица, и при этом отдельное лицо несет чрезмерное бремя в связи с вмешательством в его частную жизнь, как в случае дела «K.U. против Финляндии», поскольку дело касалось половой неприкосновенности несовершеннолетнего лица.

Однако применительно к сети Интернет государство не всегда будет отвечать за действия иных лиц, собирающих и обрабатывающих там персональные данные. Возможны случаи, кода в силу природы сети Интернет, защита от вмешательства с помощью технических ресурсов не может быть обеспечена по объективным причинам[88]. В связи с этим вторжение в частную жизнь со стороны иных лиц (а не государства) не всегда будет подпадать под нарушение статьи 8 ЕКПЧ.

Кроме баланса интересов между двумя частными лицами, необходимо учитывать баланс интересов между лицом и обществом в целом. В деле «Паломо Санчес и другие против Испании»[89], Суд указывает, что «хотя

---

[86] Абрамова А.Г. Международно-правовая защита персональных данных в сети Интернет: общие положения [Электронный ресурс]: Регион и мир. 2020. Т. 11. № 5. С. 51-58 – Режим доступа: http://elibrary.ru/, С. 56

[87] K.U. против Финляндии [Электронный ресурс]: Постановление Европейского суда по правам человека от 02.12.2008 – Режим доступа: http://www.garant.ru/, пункты 43 и 49

[88] Мусцио против Италии [Электронный ресурс]: Постановление Европейского суда по правам человека от 13.11.2007 – Режим доступа: http://www.consultant.ru/

[89] Паломо Санчес против Испании [Электронный ресурс]: Постановление Европейского суда по правам человека от 12.09.2011 – Режим доступа: http://www.garant.ru/

границы между конвенционными позитивными и негативными обязательствами государства не определены достаточно четко, применимые принципы, тем не менее, похожи. В обоих случаях следует, в частности, принимать во внимание справедливый баланс, которого необходимо достичь при уравновешивании конкурирующих интересов отдельного лица и сообщества в целом и на который распространяется действие предоставленной государству свободы усмотрения»[90].

Однако на государство не только возлагаются позитивные и негативные обязательства по обеспечению конфиденциальности персональных данных; ему также передаются права, связанные с этим вопросом

Так, Европейский суд по правам человека указывает, что государство наделено правом на свободу усмотрения в части выбора способа соблюдения требований статьи 8 ЕКПЧ.

К примеру, в деле «Бурбулеску против Румынии»[91]права заявителя на тайну частной жизни, корреспонденции и конфиденциальности данных были нарушены работодателем, контролировавшим личную переписку заявителя., которую тот вел в рабочее время. После увольнения по этой причине заявитель обратился в национальный суд, однако во всех инстанциях ему было отказано в удовлетворении исковых требований[92].

Европейский суд установил, что, как было указано выше, на государстве-ответчике лежат позитивные обязательства по защите прав заявителя, нарушенных частной компанией[93]. Но в то же время государство свободно в выборе способов соблюдения права на личную жизнь и, как следствие, на защиту данных[94].

---

[90] Паломо Санчес против Испании [Электронный ресурс]: Постановление Европейского суда по правам человека от 12.09.2011 – Режим доступа: http://www.garant.ru/, пункт 62

[91] Бурбулеску против Румынии [Электронный ресурс]: Постановление Европейского суда по правам человека от 05.09.2017 – Режим доступа: http://www.consultant.ru/

[92] Там же, пункт 109

[93] Там же, пункты 111 и 112

[94] Там же, пункт 113

Европейский Суд в таких категориях дел предоставляет широкую свободу усмотрения при оценке необходимости установления правовой базы, регулирующей условия, при которых работодатель может контролировать электронные или иные средства общения своих работников нерабочего характера, осуществляемые с рабочего места[95] (т.е. получать доступ к части персональных данных, необходимых для осуществления такого контроля).

Тем не менее, предоставляемая государствам в этом отношении свобода усмотрения не может быть безграничной, указывает Европейский суд. Внутригосударственные органы власти должны обеспечить, чтобы применение работодателем мер по контролю корреспонденции и других средств общения, независимо от степени и продолжительности этих мер, сопровождалось бы надлежащими и достаточными гарантиями против злоупотреблений[96].

При рассмотрении схожего дела Европейский суд отмечает, что «скрытое видеонаблюдение за работником на рабочем месте должно само по себе расцениваться как значительное вмешательство в его частную жизнь»[97]. Кроме того, сделанные видеозаписи были приложены работодателем в качестве доказательств в судебном процессе.

На основании того, что испанское законодательство на тот момент уже регулировало защиту персональных данных, суд указывает, что «заявительницы имели право быть предварительно и недвусмысленно, точно и однозначно уведомленными о существовании материалов, содержащих их персональные данные, или о том, что эти данные будут обработаны, об их назначении и получателях информации»[98].

---

[95] Бурбулеску против Румынии [Электронный ресурс]: Постановление Европейского суда по правам человека от 05.09.2017 – Режим доступа: http://www.consultant.ru/, пункт 119

[96] Там же, пункт 120

[97] Лопез Рибальда и другие против Испании [Электронный ресурс]: Постановление Европейского суда по правам человека от 17.10.2019 – Режим доступа: http://www.consultant.ru/, пункт 59

[98] Лопез Рибальда и другие против Испании [Электронный ресурс]: Постановление Европейского суда по правам человека от 17.10.2019 – Режим доступа: http://www.consultant.ru/, пункт 64

Как следствие, ЕСПЧ пришел к выводу, что скрытое видеонаблюдение без предварительного уведомления составило нарушение статьи 8 ЕКПЧ и конфиденциальности личных данных, поскольку эта информация была раскрыта третьим лицам. Доводы о пропорциональности данной меры законным интересам работодателя по защите своей собственности были судом отклонены, в том числе потому, что его права могли быть защищены иными, менее жесткими, мерами[99].

В Постановлении по делу «Митянин и Леонов против России»[100] отмечено, что «Суд предоставляет государству широкие пределы свободы усмотрения, когда государство должно установить справедливый баланс между конкурирующими частными интересами или конкурирующими конвенционными правами…»[101]

К схожим выводам ЕСПЧ приходит и в других делах, например, Класс и другие против Германии[102],Роман Захаров против Российской Федерации[103].

Отдельного упоминания в контексте обеспечения конфиденциальности персональных данных заслуживает также вопрос о корреспондирующей соответствующему праву обязанности предоставления субъекту доступа к своим персональным данным. Какая бы информация о субъекте персональных данных не находилась в руках государства или третьего лица, субъект должен иметь к этой информации оперативный доступ, устанавливает Европейский суд, но и здесь не обходится без нарушений.

В деле Сегерстедт-Виберг и другие против Швеции заявители обратились в связи с хранением определённой информации о них в базе данных шведской

---

[99] Лопез Рибальда и другие против Испании [Электронный ресурс]: Постановление Европейского суда по правам человека от 17.10.2019 – Режим доступа: http://www.consultant.ru/

[100] Митянин и Леонов против Российской Федерации [Электронный ресурс]: Постановление Европейского суда по правам человека от 07.05.2019 – Режим доступа: http://www.garant.ru/

[101]Там же, пункт 108

[102]Класс и другие против Германии [Электронный ресурс]: Постановление Европейского суда по правам человека от 06.09.1978 – Режим доступа: http://www.garant.ru., пункт 50

[103] Роман Захаров против Российской Федерации [Электронный ресурс]: Постановление Европейского суда по правам человека от 04.12.2015 – Режим доступа: http://www.garant.ru/, пункты 232-234

службы безопасности[104]. Им также было отказано в предоставлении информации об объёме хранящихся о них данных. Суд установил нарушение статьи 8 ЕКПЧ и прав почти всех заявителей, поскольку осуществлялось хранение информации о субъектах, доступа к которой они были лишены.

Исключением стала одна из заявительниц – о ней хранилась информация, что в 1990 году её угрожали взорвать. Это было признано Судом оправданным, т.к. интересы национальной безопасности и борьбы с терроризмом преобладали над интересами заявительницы, связанными с доступом к информации о ней в базе данных службы безопасности.

По мнению некоторых авторов в российском законодательстве вопрос доступа к данным не урегулирован в полной мере, в то время как практика европейских стран в указанной части основана на четком законодательном регулировании[105].

Ведет ли отказ в доступе к нарушению прав – во многом зависит от причин, выдвинутых государством в обоснование такого решения, а также от того, можно ли считать такой отказ необходимым в демократическом обществе и соразмерным преследуемой цели. Примером этому может служить уже упомянутое дело Сегерстедт-Виберг и другие против Швеции[106].

Таким образом, конфиденциальность – один из важнейших принципов защиты персональных данных. Существуют специальные методы и меры по предупреждению нарушения именно принципа конфиденциальности персональных данных, однако при этом конфиденциальность – из самых часто нарушаемых принципов работы с персональными данными. Это подтверждает многочисленная международная судебная практика Европейского суда по

---

[104] Сегерстедт-Виберг и другие против Швеции [Электронный ресурс]: Постановление Европейского суда по правам человека от 06.06.2006 – Режим доступа: http://www.consultant.ru/

[105] Дубровин О.В., Ковалева И.Ю. Защита персональных данных в сети Интернет: пользовательское соглашение [Электронный ресурс]: Вестник Южно-Уральского государственного университета. Серия: Право. 2014. Т. 14. № 2. С. 64-70, – Режим доступа: http://elibrary.ru/, С. 67

[106] Сегерстедт-Виберг и другие против Швеции [Электронный ресурс]: Постановление Европейского суда по правам человека от 06.06.2006 – Режим доступа: http://www.consultant.ru/

правам человека. Отметим также, что национальная судебная практика Российской федерации по нарушениям в данной сфере более обширна.

При защите конфиденциальности на государства возлагаются позитивные обязательства по предотвращению вмешательства в персональные данные и созданию эффективных законодательных мер как со стороны самого государства, так и со стороны третьих лиц (когда государство не принимает непосредственного участия в сборе и обработке информации).Европейский суд исходит из того факта, что конфиденциальность обязана учитываться, однако она не может быть абсолютной. При необходимости она должна отступать перед иными законодательными императивами, такими как поддержание порядка и предотвращение преступлений или защита прав и свобод других лиц.

Это говорит о том, что необходимо принимать во внимание справедливый баланс между интересами пострадавшего лица и общества в целом. В связи с этим государства наделены свободой усмотрения в принятии решений относительно баланса интересов. Это отмечает в своих решениях Европейский суд.

С конфиденциальностью тесно связано право субъекта персональных данных на получение информации о себе – государства, соблюдая принцип конфиденциальности и сокрытия персональных данных, могут отказать в их получении непосредственно субъекту персональных данных. Европейский суди законодатели снова указывают, что это также будет являться серьезным нарушением статьи 8 ЕКПЧ, если не соблюдать баланс интересов.

2.3. Ответственность за нарушение правил работы с персональными данными

Институт юридической ответственности за нарушение правил работы с персональными данными является одним из главных способов их защиты.

Под ответственностью за нарушение правил работы с персональными данными в настоящей работе понимается ответственность, как за умышленные, так и случайные утечку, потерю, уничтожение, подмену персональных данных и несанкционированный доступ к ним.

Международные акты в области защиты персональных данных по большей части обязуют государства создавать надлежащее и эффективное национальное законодательство с целью защиты персональных данных, то и ответственность предусмотрена в основном непосредственно национальным правом разных стран.

В законодательстве Российской Федерации соответствующая ответственность предусмотрена в ФЗ «О персональных данных»[107]. Ее можно разделить на гражданско-правовую, дисциплинарную, административную и уголовную[108].

Так, если лицу причинен имущественный ущерб или моральный вред, он может потребовать привлечения к гражданско-правовой ответственности виновного лица, которое обязано возместить убытки, вред. Федеральный закон устанавливает возможность предъявления требования о взыскании компенсации за причинение морального вреда.

Согласно ст. 151 ГК РФ, если «гражданину причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в иных случаях,

---

[107] О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ – Режим доступа: http://www.consultant.ru/, статья 24

[108] Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/, статья 90

предусмотренных законом, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда»[109].

Дисциплинарная ответственность урегулирована ст. 192 Трудового кодекса РФ. В отношении сотрудника, нарушившего правила работы с персональными данными иного лица, работодатель вправе применить замечание, выговор или увольнение[110]. Трудовой кодекс устанавливает специальное основание для расторжения трудового договора по инициативе работодателя в случае разглашения охраняемой законом тайны, ставшей известной работнику в связи с исполнением им трудовых обязанностей[111].

За нарушение правил работы с персональными данными могут быть привлечены к административной ответственности как работники, так и работодатель. Кодекс РФ об административных правонарушениях содержит по этому поводу две статьи.

Статья 13.11 КоАП предусматривает состав, охраняющий общественные отношения в сфере сбора, хранения, использования или распространения информации о гражданах (персональных данных). Ответственность установлена в виде штрафа, размер которого зависит от вида нарушения и лица, совершившего или допустившего такое нарушение;

Статья 13.14 КоАП РФ регулирует охрану данных с ограниченным доступом. Так, разглашение информации, доступ к которой ограничен, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц - от четырех тысяч до пяти тысяч рублей[112].

---

[109] Гражданский кодекс Российской Федерации от 30.11.1994 № 51-ФЗ – Режим доступа: http://www.consultant.ru/, статья 151

[110]Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/, статья 192

[111] Там же, подпункт В пункта 6 части 1 статьи 81

[112]Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/,статьи13.11и 13.14

Статья 137 Уголовного кодекса Российской Федерации предусматривает наказание за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную и семейную тайну[113]. Уголовная ответственность грозит в том случае, если эти действия совершены намеренно, из корыстной или иной личной заинтересованности и повлекли за собой нарушение законных прав и свобод граждан. Причем наказание ужесточается, если виновный использовал свое служебное положение[114].

УК РФ предусматривает наказания за преступления, связанные с нарушением конфиденциальности, упомянутой ранее.

Статьи 272-274 УК РФ посвящены преступлениям, связанным, соответственно, с неправомерным доступом к компьютерной информации, созданием, использованием и распространением вредоносных программ, нарушением правил эксплуатации ЭВМ, систем и сетей на их основе[115].

В странах Европейского союза ответственность и санкции за нарушение правил работы с персональными данными предусмотрены Общим регламентом ЕС, а именно его 9 главой[116]. В частности, статья 82 Общего регламента устанавливает, что «любое лицо, которое понесло материальный или нематериальный ущерб в результате нарушения положений настоящего Регламента, имеет право на получение компенсации от контролёра или процессора за понесенный ущерб»[117].

---

[113] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru., статья 137

[114] Там же, часть 2 статьи 137

[115]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/, статьи 272-274

[116] О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС [Электронный ресурс]: Регламент Европейского Парламента и Совета Европейского Союза № 2016/679 от 27.04.2016 – Режим доступа: http://www.garant.ru/

[117]О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС [Электронный ресурс]: Регламент Европейского Парламента и Совета Европейского Союза № 2016/679 от 27.04.2016 – Режим доступа: http://www.garant.ru/,пункты1-6 статьи 82

Статья предусматривает ответственность контролера или процессора, условия освобождения их от ответственности, солидарность и возможность предъявления регрессных требований при возмещении ущерба, а также подсудность.

Вопрос о назначении штрафов за нарушение правил работы с персональным данными регулируется статьей 83 Общего регламента. В частности при решении вопроса о наложении административного взыскания и установлении его размера, в каждом индивидуальном случае необходимо принимать во внимание: характер, тяжесть, продолжительность, преднамеренность, повторность нарушения, действия виновного, степень ответственности и сотрудничества, а также категорию персональных данных.

Кроме того, Регламент предусматривает обязанность государств-членов «установить нормы относительно иных санкций, применимых за нарушения настоящего Регламента, в том числе за нарушения, которые не подпадают под административные штрафы в порядке статьи 83, а также принять все меры, для того, чтобы обеспечить их применение. Такие санкции должны быть эффективными, соизмеримыми и должны оказывать сдерживающее воздействие»[118].

На наш взгляд, в Европейский союзе достаточно полно урегулирована ответственность за нарушение правил работы с персональными данными, устанавливая крупные штрафы и санкции. Данный уровень регулирования выступает в качестве вспомогательного по отношению к национальному регулированию ответственности в европейских государствах-членах.

Примером ответственности работника за нарушение правил работы с персональными данными субъекта является дело Копланд против Великобритании[119].

---

[118]О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС [Электронный ресурс]: Регламент Европейского Парламента и Совета Европейского Союза № 2016/679 от 27.04.2016 – Режим доступа: http://www.garant.ru/,статья 84

[119] Копланд против Великобритании [Электронный ресурс]: Постановление Европейского суда по правам человека от 03.04.2007 – Режим доступа: http://www.consultant.ru

Заявительница подвергалась контролю за ее передвижениями, перепискам, использованием Интернета и телефонными звонками со стороны заместителя ректора, т.е. такого же работника, как и она (§10-12). Европейский Суд посчитал, что «сбор и хранение указанной личной информации без ведома заявительницы, представляли собой вмешательство в ее право на уважение частной жизни и корреспонденции по смыслу статьи 8 Конвенции» (§44).

В соответствии Правилами о телекоммуникации от 24.10.2000 работодатели были обязаны принимать разумные меры для информирования работников о том, что их сообщения могут быть перехвачены. Данное условие не было соблюдено, следовательно, заместитель ректора допустил нарушение правил работы с персональными данными, за что был привлечен работодателем к ответственности, установленной национальным законодательством и отстранен от должности.

Отметим, что основным источником регулирования ответственности за нарушение правил работы с персональными данными является национальное законодательство. Основные международные акты лишь обязывают государства установить ответственность в законодательстве.

Подробно рассмотренное законодательство Российской Федерации устанавливает различные виды ответственности – от гражданско-правовой до уголовной. Аналогичное регулирование ответственности предусмотрено в национальном законодательстве других стран.

Ответственность, урегулированная в рамках ЕС, позволяет государствам взыскивать административные штрафы и назначать особые санкции для неурегулированных случаев, не подпадающих под административную ответственность. Данный уровень регулирования выступает в качестве вспомогательного по отношению к национальному регулированию ответственности в европейских государствах-членах.

ЕСПЧ также указывает на привлечение к ответственности виновного лица на основании национального законодательства.

Заключение

Исходя из вышеизложенного, автор приходит к следующим выводам.

Сложившаяся сверхзависимость современного общества от сети Интернет привела к возникновению очередного витка развития проблем, вызываемых возможной незащищенностью информации, в частности, персональных данных, попадающих в сеть Интернет.

Защита персональных данных осуществляется большим количеством актов, принятым на национальном, так и на международном уровне. Принято множество нормативных и подзаконных актов, затрагивающих и общие и специальные сферы защиты персональных данных.

Основой послужила Конвенция № 108, изданная в 1981 году, в которой закреплены основные принципы защиты информации, а также обязательства для стран-участников по созданию национальной законодательной базы.

Защита персональных данных регулируется комплексом актов, которые разнятся по юридической силе: часть из них обязательна для исполнения, часть носит рекомендательный характер. Европейский союз прошел долгий путь по развитию собственного правового регулирования в указанной сфере. Единый общий акт сменил десятки директив и регламентов, что позволило ЕС унифицировать и привести воедино практически все общие положения, связанные с защитой персональных данных.

Значительное влияние на развитие нормативного регулирования имеет практика Европейского суда по правам человека по связанным с правом на уважение частной жизни человека. Анализ решений ЕСПЧ за последние 30 лет указывает, что в законодательстве ряда стран имеет ряд правовых пробелов.

К сожалению, в том числе российское законодательство, состоящее из единственного федерального закона и ряда подзаконных актов технической направленности, не успевает за ростом активности граждан в Интернете, осуществляя регулирование в данной сфере актами, плохо применимыми к деятельности в сети Интернет. Похожая ситуация наблюдается и в других странах.

На международном и национальном уровне создана базовая защита персональных данных в эпоху цифровых технологий. Но предмет защиты еще четко не обозначен. Судебная практика конкретизирует и постоянно расширяет перечень о того, что может относиться к персональным данным. Однако этот перечень не является исчерпывающим.

К персональным данным можно отнести практически любую информацию, если она позволяет прямо или косвенно определить, идентифицировать конкретное лицо. Наличие закрытого перечня облегчило бы процесс правоприменения, но сформировать его практически невозможно. Аналогичная ситуация сложилась и в национальном законодательстве большинства стран, в том числе Российской Федерации.

Определение конкретных видов и классификаций угроз персональным данным содержится в национальных законах. В российском законодательстве описано большое разнообразие угроз безопасности персональных данных, которые можно разделить по видам и категориям в зависимости от источников, предмета, субъекта и сферы угроз. Главными угрозами являются несанкционированный доступ, умышленная или случайная несанкционированная передача персональных данных иным лицам (утечка), потеря и уничтожение персональных данных. Некоторые угрозы персональным данным в сети Интернет носят косвенный характер или создаются опасность только при наличии ряда условий, как например, чужие файлы-cookie, которые можно использовать с нарушением законодательства стран в сфере обработки персональных данных, а можно похитить или купить на черном интернет-рынке, тем самым получив полный доступ к информации ничего не подозревающего субъекта.

Иные угрозы основываются не на технической сфере, но на доверии и страхах пользователей сети, вынуждая обманным путем лицо самостоятельно раскрыть свои персональные данные без принуждения.

Существует большое количество методов, собранных в различные классификации и группы с целью наилучшего, эффективного и адекватного

применения средств защиты персональных данных. Они включают в себя разнообразные меры, но преследуют единую цель – защиту персональных данным путем соблюдения установленных в законах и международных актах принципов, таких как достоверность или точности персональных данных, их сохранность и конфиденциальность.

Принципы достоверности (точности) и сохранности персональных данных рассматриваются как в национальных, так и в международных актах бок о бок. Их нарушение является недопустимым за небольшим числом исключений, предусмотренных законами или определенных судами. Например, в целях борьбы с терроризмом или иными подобными целями.

Как международная, так и российская судебная практика полна примеров дел, в которых суд признает нарушение прав лица ввиду несоблюдения принципа точности (достоверности) содержания персональных данных.

Отдельной категорией споров являются обоснованные требования субъектов персональных данных по удалению информации о себе. Так называемое право на цифровую смерть предусмотрено в российском Федеральном законе и Общем регламенте ЕС в качестве исключения из принципа сохранности данных. В таком случае уничтожение персональных данных не будет считаться нарушением принципа сохранности, установленного в настоящее время международными и национальными актами, поскольку оно происходит с согласия и/или по требованию самого субъекта.

Существуют специальные методы и меры по предупреждению нарушения именно принципа конфиденциальности персональных данных, однако при этом конфиденциальность – из самых часто нарушаемых принципов работы с персональными данными. Это подтверждает международная судебная практика. Отметим, что национальная судебная практика Российской федерации по нарушениям в данной сфере еще более обширна.

При защите конфиденциальности на государства возлагаются позитивные обязательства по предотвращению вмешательства в персональные данные и созданию эффективных законодательных мер как со стороны самого

государства, так и со стороны третьих лиц (когда государство не принимает непосредственного участия в сборе и обработке информации). Европейский суд исходит из того факта, что конфиденциальность обязана учитываться, однако она не может быть абсолютной. При необходимости она должна отступать перед иными законодательными императивами, такими как поддержание порядка и предотвращение преступлений или защита прав и свобод других лиц.

Необходимо принимать во внимание справедливый баланс между интересами пострадавшего лица и общества в целом. Государства наделены свободой усмотрения в принятии решений относительно баланса интересов.

С конфиденциальностью тесно связано право субъекта персональных данных на получение информации о себе – государства, соблюдая принцип конфиденциальности и сокрытия персональных данных, могут отказать в их получении непосредственно субъекту персональных данных. Европейский суд и законодатели снова указывают, что это также будет являться серьезным нарушением статьи 8 ЕКПЧ, если не соблюдать баланс интересов.

Однако в связи со специфичной природой сети Интернет государства не всегда способны исполнять свои позитивные обязательства и обеспечивать полную и надлежащую защиту персональных данных разных лиц.

За нарушение правил работы с персональными данными предусмотрена ответственность. Законодательство Российской Федерации устанавливает различные виды ответственности – от гражданско-правовой до уголовной. Аналогичное регулирование ответственности предусмотрено в национальном законодательстве других стран.

Ответственность в рамках ЕС включает административные штрафы и особые санкции для неурегулированных случаев, не подпадающих под административную ответственность.

Список использованных источников

Международные правовые акты

1. Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence, [Электронный ресурс]: сайт Европейского суда по правам человека – Режим доступа: https://www.echr.coe.int

2. В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи [Электронный ресурс]: Директива Европейского Парламента и Совета Европейского Союза 2002/58/ЕС от 12.07.2002 (Директива о конфиденциальности и электронных средствах связи) – Режим доступа: http://www.garant.ru

3. Конвенция о защите прав человека и основных свобод (заключена в г. Риме 04.11. 1950) [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru

4. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981), [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru

5. О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС [Электронный ресурс]: Регламент № 2016/679 Европейского парламента и Совета Европейского Союза (Принят в г. Брюсселе 27.04.2016) – Режим доступа: http://www.consultant.ru

6. О защите физических лиц при обработке персональных данных и о свободном перемещении таких данных [Электронный ресурс]: Директива 95/46/ЕС Европарламента и Европейского Совета от 24.10.1995 – Режим доступа: http://www.garant.ru

7. О праве на неприкосновенность частной жизни [Электронный ресурс]: Доклад Специального докладчика ООН от 25.10.2018 – Режим доступа:

https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/324/49/PDF/G1832449.pdf?OpenElement

8. О праве на неприкосновенность частной жизни в цифровую эпоху [Электронный ресурс]: Резолюция Генеральной Ассамблеи ООН № 73/179 от 17.12.2018 – Режим доступа: https://undocs.org/ru/A/RES/73/179.

9. Об основных правах [Электронный ресурс]: Хартия Европейского Союза от 07.12.2000 – Режим доступа: http://www.garant.ru

10. Об универсальной услуге и правах пользователей в отношении сетей и услуг электронной связи [Электронный ресурс]: Директива 2002/22/ЕС Европейского Парламента и Совета от 07.03.2002 (Директива об универсальной услуге) – Режим доступа: http://www.garant.ru

Международная судебная практика

11. «Бернх Ларсен холдинг АС» и другие (Bernh Larsen Holding AS and Others) против Норвегии [Электронный ресурс]: Постановление Европейского суда по правам человека от 14.03.2013 – Режим доступа: http://www.garant.ru

12. Google Spain S Land Google Inc. vs Agenda Espacolade Protecciynde Datos (AEPD) and Mario Costeja Gonzalez [Электронный ресурс]: Решение Суда ЕС от 13.05.2014 – Режим доступа: http://curia.europa.eu/juris/

13. K.U. против Финляндии [Электронный ресурс]: Постановление Европейского суда по правам человека от 02.12.2008 – Режим доступа: http://www.garant.ru

14. Аманн (Amann) против Швейцарии [Электронный ресурс]: Постановление Европейского Суда по правам человека от 16.02.2000 – Режим доступа: http://www.consultant.ru

15. Бурбулеску против Румынии [Электронный ресурс]: Постановление Европейского суда по правам человека от 05.09.2017 – Режим доступа: http://www.consultant.ru

16. Класс и другие против Германии [Электронный ресурс]: Постановление Европейского суда по правам человека от 06.09.1978 – Режим доступа: http://www.garant.ru

17. Копланд против Великобритании [Электронный ресурс]: Постановление Европейского суда по правам человека от 03.04.2007 – Режим доступа: http://www.consultant.ru

18. Корр (Korr) против Швейцарии [Электронный ресурс]: Постановление Европейского Суда по правам человека от 25.03.1998 – Режим доступа: https://europeancourt.ru

19. Леандер (Leander) против Швеции [Электронный ресурс]: Постановление Европейского Суда по правам человека от 26.03.1987 – Режим доступа: http://www.garant.ru

20. Лопез Рибальда и другие против Испании [Электронный ресурс]: Постановление Европейского суда по правам человека от 17.10.2019 – Режим доступа: http://www.consultant.ru/

21. Митянин и Леонов против Российской Федерации [Электронный ресурс]: Постановление Европейского суда по правам человека от 07.05.2019 – Режим доступа: http://www.garant.ru

22. Мусцио против Италии [Электронный ресурс]: Постановление Европейского суда по правам человека от 13.11.2007 – Режим доступа: http://www.consultant.ru

23. Паломо Санчес против Испании [Электронный ресурс]: Постановление Европейского суда по правам человека от 12.09.2011 – Режим доступа: http://www.garant.ru

24. Роман Захаров против Российской Федерации [Электронный ресурс]: Постановление Европейского суда по правам человека от 04.12.2015 – Режим доступа: http://www.garant.ru

25. Ротару (Rotaru) против Румынии [Электронный ресурс]: Постановление Европейского Суда по правам человека от 04.05.2000 – Режим доступа: http://www.garant.ru

26. Сегерстедт-Виберг и другие против Швеции [Электронный ресурс]: Постановление Европейского суда по правам человека от 06.06.2006 – Режим доступа: http://www.consultant.ru

27. Товарищество «Фолькер и Маркус Шеке» и Хартмунт Айферт против Земли Гессен (Volker und Markus Schecke GbR und Hartmut Eifert v. Land Hessen) [Электронный ресурс]: Решение Суда Европейского союза от 09.11.2010 2013 – Режим доступа: https://eur-lex.europa.eu/

28. Фон Ганновер (Принцесса Ганноверская) против Германии, [Электронный ресурс]: Постановление Европейского Суда по правам человека от 24.06.2004 – Режим доступа: http://www.consultant.ru

29. Шимоволос против Российской Федерации [Электронный ресурс]: Постановление Европейского суда по правам человека от 21.06.2011 – Режим доступа: http://www.consultant.ru

Национальные правовые акты разных стран

30. О защите личных данных (Bundesdatenschutzgesetz) [Электронный ресурс]: Федеральный закон Германии от 20.12.1990 – Режим доступа: http://www.gesetze-im-internet.de

31. Loi informatiqueet libertes Act № 78-17 of January 1978 on information technology, data files and civil liberties // The Commission nationale de l'informatique et des libertés. URL: http://www.cnil.fr/english/data-protection/ official- texts/

32. Гражданский кодекс Российской Федерации от 30.11.1994 № 51-ФЗ – Режим доступа: http://www.consultant.ru

33. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ [Электронный ресурс]: СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru

34. О персональных данных [Электронный ресурс]: Федеральный закон от 27.07.2006 № 152-ФЗ – Режим доступа: http://www.consultant.ru

35. О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс]: Федеральный закон от 19.12.2005 № 160-ФЗ – Режим доступа: http://www.consultant.ru

36. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru

37. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru

38. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 15.02.2008) [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru

39. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: Постановление Правительства Российской Федерации от 01.11.2012 № 1119 – Режим доступа: http://www.garant.ru

40. Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации [Электронный ресурс]: Постановление Правительства Российской Федерации от 15.09.2008 № 687 – Режим доступа: http://www.garant.ru

41. Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных [Электронный ресурс]: Постановление Правительства Российской Федерации от 06.07.2008 № 512 – Режим доступа: http://www.consultant.ru

42. Об утверждении Положения о персональных данных государственного служащего Российской Федерации и ведении его личного дела [Электронный ресурс]: Указ Президента Российской Федерации от 30 мая 2005 г. № 609 – Режим доступа: http://www.consultant.ru

43. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

(утв. ФСТЭК РФ 14.02.2008) [Электронный ресурс]: Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru

44. Об утверждении требований и методов по обезличиванию персональных данных [Электронный ресурс]: Приказ Роскомнадзора от 05.09.2013 №996 – Режим доступа: http://www.consultant.ru

Российская судебная практика

45. Апелляционное определение Санкт-Петербургского городского суда от 11.10.2017 по делу № 2-2998/2017, [Электронный ресурс]: сайт Санкт-Петербургского городского суда – Режим доступа: http://sankt-peterburgsky.spb.sudrf.ru

46. Постановление Тринадцатого арбитражного апелляционного суда от 01.06.2015 № 13АП-10709/2015 по делу № А56-75017/2014 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/

47. Постановление Тринадцатого арбитражного апелляционного суда от 21 июня 2010 г. по делу № А56-4788/2010 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/

48. Решение Арбитражного суда Челябинской области по делу № А76-29008/2015 от 11.02.2016 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/

49. Решение Заельцовского районного суда г. Новосибирска № 2-1770/2018 ~ М-987/2018 М-987/2018 от 27 июня 2018 г. по делу № 2-1770/2018 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/

50. Решение Верховного Суда РФ от 11.03.2013 № АКПИ13-61 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/;

51. Определение Верховного Суда РФ от 20.02.2019 № 303-ЭС19-56 по делу № А59-1219/2018 [Электронный ресурс]: сайт Судебные и нормативные акты РФ – Режим доступа: https://sudact.ru

52. Решение Октябрьского районного суда г. Красноярска № 2-3904/2019 2-3904/2019~М-966/2019 М-966/2019 от 26 августа 2019 г. по делу № 2-3904/2019 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/

Учебная и научная литература

53. Targeted marketing [Электронный ресурс]: The Dictionary Netlingo – Режимдоступа: http://www.netlingo.com/word/targeted-marketing.php

54. Абрамова А.Г. Международно-правовая защита персональных данных в сети Интернет: общие положения [Электронный ресурс]: Регион и мир. 2020. Т. 11. № 5. С. 51-58 – Режим доступа: http://elibrary.ru

55. Акулов О.А., Медведев Н.В. Информатика: базовый курс [Электронный ресурс]: учебник для студентов вузов, бакалавров, магистров. - 4-е изд., стер. - Москва: Омега-Л, 2007 – Режим доступа: https://may.alleng.org/d/comp/comp220.htm

56. Бачило И.Л. [Электронный ресурс]: Государство и право XXI в. Реальное и виртуальное. М. 2012. 280 с – Режим доступа: http://www.garant.ru

57. Бегларян М.Е., Пичкуренко Е.А. Безопасность персональных данных в современной России [Электронный ресурс]: Уголовная политика в сфере обеспечения здоровья населения, общественной нравственности и иных социально-значимых интересов, материалы 4-ой Международной научно-практической конференции. 2015. С. 24-28 – Режим доступа: http://elibrary.ru

58. Беззубиков Д.А., Морозов М.В. Проблема защиты персональных данных в сети Интернет [Электронный ресурс]: Дневник науки. 2019. № 4 (28) – Режим доступа: http://elibrary.ru

59. Ворожбит Д.В. Особенности защиты персональных данных пользователей Интернет-ресурсов [Электронный ресурс]: Работы членов

студенческого научного общества СЮИ ФСИН России. Сборник статей. Самара. 2019. С. 34-38., – Режим доступа: http://elibrary.ru

60. Геращенко О.М., Капралова Н.Н. Защита персональных данных в информационных системах методом обезличивания [Электронный ресурс]: Уголовно-исполнительная система сегодня: взаимодействие науки и практики. Материалы юбилейной XX Всероссийской научно-практической конференции. 2020. С. 255-257 – Режим доступа: http://elibrary.ru

61. Григорьев А.А. Методы и средства защиты персональных данных в сети Интернет [Электронный ресурс]: Современные проблемы проектирования, применения и безопасности информационных систем. Материалы XVII Межрегиональной научно-практической конференции. 2017. С. 35-39 – Режим доступа: http://elibrary.ru

62. Гундерич Г.А., Ломач Я.С., Булгакова Я.А. Защита персональных данных в сети Интернет [Электронный ресурс]: сборник статей IX Международной научно-практической конференции: в 2 ч.. 2019. С. 93-96 – Режим доступа: http://elibrary.ru

63. Донец Р.В., Булгаков В.В. Защита персональных данных и частной жизни в сети интернет [Электронный ресурс]: Актуальные проблемы социально-гуманитарных наук. Сборник научных трудов по материалам Международной научно-практической конференции. В 6-ти частях. Под общей редакцией Е.П. Ткачевой. 2017. С. 58-61 – Режим доступа: http://elibrary.ru

64. Дроменко А.Ю. Информационные права граждан РФ и защита персональных данных в сети «Интернет» [Электронный ресурс]: Science Time. 2016. № 2 (26). С. 203-206. – Режим доступа: http://elibrary.ru

65. Дубровин О.В., Ковалева И.Ю. Защита персональных данных в сети Интернет: пользовательское соглашение [Электронный ресурс]: Вестник Южно-Уральского государственного университета. Серия: Право. 2014. Т. 14. № 2. С. 64-70, – Режим доступа: http://elibrary.ru

66. Дудко М.О. Правовой механизм защиты персональных данных в сети Интернет [Электронный ресурс]: Международное гуманитарное право глазами

белорусской общественности. Материалы международного научного форума. Редколлегия: Е.Ф. Довгань (гл. ред.) [и др.]. Минск, 2020. С. 87-98 – Режим доступа: http://elibrary.ru

67. Ефремов М.А., Калуцкий И.В., Таныгин М.О., Рудак И.И., Безопасность персональных данных, социальные сети и реклама в глобальной сети internet [Электронный ресурс]: Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2017. Т. 7. № 1 (22). С. 27-33 – Режим доступа: http://elibrary.ru

68. Кирпичникова А.В. Правовая проблема защиты персональных данных пользователей в сети Интернет [Электронный ресурс]: Ученые записки. сборник научных трудов. Оренбург, 2020. С. 75-79 – Режим доступа: http://elibrary.ru

69. Киселева А.Б., Ильина Л.А. Анализ угроз безопасности персональных данных в интернет-магазинах [Электронный ресурс]: Аллея науки. 2017. Т. 1. № 8. С. 652-655 – Режим доступа: http://elibrary.ru

70. Лачина Е.А., Кузнецова И.А., Носова Е.В. Проблемы защиты персональных данных в сети «Интернет» [Электронный ресурс]: Ученые записки. 2021. № 1 (37). С. 114-118 – Режим доступа: http://elibrary.ru

71. Малахов А.О. Правовые методы защиты персональных данных в сети Интернет [Электронный ресурс]: Государственное управление III тысячелетия: проблемы и перспективы. сборник научных статей IV Международной научно-практической конференции. 2017. С. 169-174 – Режим доступа: http://elibrary.ru

72. Петров Е.О., Бажин К.А. Защита персональных данных [Электронный ресурс]: Кафедра информационной безопасности. ТюмГУ. Тюмень. 2009 – Режим доступа: https://www.bestreferat.ru/referat-397328.html

73. Постникова Е.В. Некоторые аспекты правового регулирования защиты персональных данных в рамках внутреннего рынка Европейского союза [Электронный ресурс]: Право. Журнал Высшей школы экономики. 2018. № 1. С. 234–254 – Режим доступа: http://elibrary.ru

74. Пыжов Н.С., Беляева А.А., Шаханова М.В. Актуальные проблемы защиты персональных данных в сети Интернет [Электронный ресурс]: Научный электронный журнал Меридиан. 2020. № 2 (36). – Режим доступа: http://elibrary.ru

75. Сарычев А.Ю. К вопросу о защите персональных данных в сети Интернет [Электронный ресурс]: Научно-образовательный потенциал молодежи в решении актуальных проблем XXI века. 2019. № 14. С. 148-150 – Режим доступа: http://elibrary.ru

76. Скалеух Д.К. Зарубежный опыт правового регулирования защиты персональных данных в сети Интернет [Электронный ресурс]: Актуальные проблемы экономики, управления и права. Сборник научных статей по материалам Всероссийской научно-практической конференции, посвященной Дню Конституции Российской Федерации. Ростов-на-Дону. 2020. С. 362-367. – Режим доступа: http://elibrary.ru

77. Сочнев А.В. Защита персональных данных в сети «Интернет» [Электронный ресурс]: Молодежь и XXI век. 2016. Материалы VI Международной молодежной научной конференции. В 4-х томах. 2016. С. 164-167 – Режим доступа: http://elibrary.ru

78. Струков К.В. Право на забвение в сети Интернет: понятие и перспективы развития [Электронный ресурс]: Actual science. 2017. Т. 3. № 2. С. 55-57 – Режим доступа: http://elibrary.ru

79. Сыргашева Т.Н. Методы и средства защиты персональных данных [Электронный ресурс]: NovaUm.Ru. 2018. № 16. С. 353-354. – Режим доступа: http://elibrary.ru

80. Талапина Э.В. Защита персональных данных в цифровую эпоху [Электронный ресурс]: Труды Института государства и права РАН. 2018. Т. 13. № 5. С. 117–150 – Режим доступа: http://elibrary.ru

81. Талапина Э.В. Цифровая трансформация во Франции: правовые новеллы [Электронный ресурс]: Право. Журнал Высшей школы экономики. 2019. № 4. С. 164-184 – Режим доступа: http://elibrary.ru

82. Толбанова А.В. Основные меры по защите личных и персональных данных при работе в сети Интернет, [Электронный ресурс]: Безопасность городской среды. материалы межрегиональной (с международным участием) научно-практической конференции. 2016. С. 156-157 – Режим доступа: http://elibrary.ru

83. Фомина Л.Ю. Международные стандарты защиты персональных данных в условиях информационного общества [Электронный ресурс]: Международное право. 2019. № 4. С. 50-59 – Режим доступа: https://cyberleninka.ru

84. Фролова А.Д., Защита персональных данных в сети Интернет [Электронный ресурс]: Технологии XXI века в юриспруденции. Материалы Второй международной научно-практической конференции. Под редакцией Д.В. Бахтеева. 2020. С. 456-459 – Режим доступа: http://elibrary.ru

85. Хилюк А.В., Мельников Н. Проблема защиты персональных данных в Интернете [Электронный ресурс]: Сборник «неделя науки СПбПУ». Материалы научной конференции с международным участием, В 3 ч. отв. ред. А.В. Рубцова, М.С. Коган. Санкт-Петербург, 2020. С. 178-181 – Режим доступа: http://elibrary.ru

86. Хлестова Д.Р., Попов К.Г. К вопросу о защите персональных данных в сети Интернет [Электронный ресурс]: Инновационное развитие. 2017. № 7 (12). С. 20-21 – Режим доступа: http://elibrary.ru

87. Чагин И.Б., Юрковский А.В. К вопросу о механизме реализации права на забвение в сети Интернет [Электронный ресурс]: Академический юридический журнал. 2018. № 3 (73). С. 41-47 – Режим доступа: http://elibrary.ru

88. Чурилов А.Ю. Принципы Общего регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации [Электронный ресурс]: Вестник Омской юридической академии. 2019. № 1. С. 29–35 – Режим доступа: http://elibrary.ru

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический институт
институт

Кафедра международного права
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____ Т.Ю. Сидорова
подпись инициалы, фамилия
«18» 06 2021 г.

БАКАЛАВРАСКАЯ РАБОТА

40.03.01 Юриспруденция, 40.03.01.01 Международное и иностранное право
код – наименование направления

Защита персональных данных в сети Интернет: сравнительный анализ
тема

Руководитель _____ к.ю.н., доцент кафедры В.В. Терешкова
подпись, дата 18.06.21 должность, ученая степень инициалы, фамилия

Выпускник _____ 18.06.21 И.В. Зрилин
подпись, дата инициалы, фамилия

Красноярск 2021