Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Юридический институт
Кафедра международного права

УТВЕРЖДАЮ
Заведующий кафедрой
Т. Ю. Сидорова
« 16 » 06 2017 г.

БАКАЛАВРСКАЯ РАБОТА

40.03.01 юриспруденция
40.03.01.01 международное и иностранное право

Защита персональных данных: регулирование России и Германии.

Научный руководитель 16.06.17 доцент, канд. юрид. наук В.В. Терешкова
подпись, дата

Выпускник 16.06.17 В.А. Монин
подпись, дата

Красноярск 2017

Оглавление

Введение

В соответствии со ст. 23 Конституции РФ каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени[1]. На основании ст. 24 Конституции РФ сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются[2]. В связи с этим актуальность защиты персональных данных не подвергается сомнению. В случае если персональные данные используются произвольно и становятся доступными лицам, которым они не должны быть известны, гражданам наносится не только моральный вред, но и материальный ущерб.

В настоящее время, характеризуемое бурным развитием информационных технологий, на первый план встает вопрос защиты персональных данных при их накоплении, обработке и передаче с использованием средств информатизации. Для регулирования информационных правоотношений в области персональных данных законодателем принят целый ряд нормативно-правовых актов. Достаточно долгое время, кроме общих норм, закрепленных Всеобщей декларацией прав человека 1948 г., ни в международных актах, ни в национальном законодательстве разных государств никаких специальных правил о порядке получения, хранения, обработки и передачи персональных данных не было. Ситуация стала меняться с распространением компьютеров. У компаний и государственных органов стало скапливаться большое количество персональных данных, которые относительно легко могли быть разглашены и тем самым нанести моральный и материальный вред лицам, которых касаются эти данные.

Начиная с 1970-х гг. в промышленно развитых странах стало появляться соответствующее законодательство. Первый закон о защите персональных данных был принят в Германии в земле Гессен в 1970 году. До этого подобных

[1] «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ) // «Собрание законодательства РФ», 26.01.2009, № 4, ст. 23.
[2] Там же, ст.24.

законов нигде в мире не было. Закон Российской Федерации «О персональных данных» был принят гораздо позже, только в 2006 году.

Ужесточение требований к организациям, собирающим, изымающим и обрабатывающим персональную информацию, показывает важность данной темы.

Прослушивание личного телефона Ангелы Меркель, хакерские атаки на облачные хранилища с последующим раскрытием личных данных и фотографий подчеркивают необходимость и актуальность рассмотрения вопроса о защите персональных данных, важность определения пределов, в рамках которых возможно раскрытие и изъятие персональных данных, определение технических и юридических требований, и установление соразмерной ответственности за незаконный сбор, хранение, распространение, изъятие пользовательских данных. Очевидна необходимость проверки соответствия внутригосударственного регулирования международным нормам.

Степень научной разработанности темы дипломной работы

Несмотря на довольно большое количество авторов, занимающихся этой проблематикой (Агапов А.Б., Антопольский А.А., Бачило И.Л., Василенко Л.А., Волчинская Е.К., Глотов С.А., Гаврилова О.А., Казарян Э.А., Калятина В.О., Курушин В.Д., Килясханов И.Ш., Лапина М.А., Лопатин В.Н., Лушникова М.В., Маркевич А.С., Миндрова Е.К., Нисневич Ю.А., Помазуев А.Е., Рассолов М.М., Степанов Е.А., Сергиенко Л.А., Подшибихин Л.Н., Петросян М.Е., Петрухин И.Л., Фатьянов А.А.), их работы преимущественно посвящены характеристикам различных видов информационных процессов, ресурсов и технологий, обеспечению государственной и иных видов тайн и т.д. Комплексного исследования оборота и защиты персональных данных, комплексного сравнительно-правового исследования правового регулирования оборота персональных данных в РФ, Германии и ЕС не проводилось.

Объектом исследования являются общественные отношения, возникающие в сфере защиты персональных данных как на международном уровне, так и внутригосударственным правом, а также правоприменительная практика различных государств.

Предметом исследования являются международно-правовые нормы и нормы законодательства Европейского союза, Германии и Российской Федерации в сфере правовой охраны персональных данных.

Цель исследования состоит в обобщении законодательства и мировой практики по вопросам правовой охраны персональных данных, определении основных законодательных проблем в сфере правовой охраны персональных, а также выработке авторской позиции по обозначенным вопросам.

Для достижения указанных целей были сформулированы следующие задачи:

1. Проанализировать соответствующие международно-правовые нормы по защите персональных данных и установлении правового режима таких данных;
2. Проанализировать законодательство и практику Германии, РФ и ЕС в сфере защиты персональных данных
3. Выявить эффективные способы и методы защиты персональных данных.
4. Провести сравнительный анализ законодательства в сфере правовой охраны персональных данных в Германии, Европейском союзе и РФ с целью определения наиболее благоприятного режима регулирования персональных данных.

Научная новизна исследования состоит в том, что автором впервые предпринята попытка обобщения имеющегося опыта в сфере правовой охраны персональных данных, выявлены имеющиеся тенденции и противоречия в правовом регулировании и судебной практике на современном этапе, а также дана оценка сильным и слабым сторонам того или иного способа защиты персональных данных.

Методологическую основу дипломного исследования составляет сочетание как общенаучных методов познания, таких как анализ, синтез, обобщение, индукция, дедукция, исторический метод, логический метод, аналогия, системный подход, так и частноправовых методов научного

познания, в частности сравнительно-правового и формально-юридического метода, совокупность которых позволила провести полное комплексное исследование поставленных задач.

Структура дипломной работы определяется ее целью и принятым подходом к решению поставленных задач. Работа состоит из введения, двух глав, разделенных на параграфы, заключения, а также списка использованных источников.

Глава 1. Понятие и правовой режим персональных данных.

1.1. Понятие персональных данных

Персональные данные означают информацию, касающуюся конкретного или могущего быть идентифицированным лица ("субъекта данных") – именно такое определение дает Конвенция о защите физических лиц при автоматизированной обработке персональных данных[3]. Данная Конвенция является первым международным актом, которая заложила основу для формирования унифицированной работы по защите и обработке персональных данных. На основании данной Конвенции у стран-участников стали появляться внутригосударственные отраслевые законы по регулированию правового положения персональных данных, а так же принципы и условия их обработки.

В российском законодательстве дефиниция персональных данных закреплена в ФЗ «О защите персональных данных»[4] и гласит, что это любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Данное понятие, на наш взгляд, является самым широким за всю историю развития в Российского законодательства.

Впервые термин "персональные данные", тесно связанный с частной жизнью человека, появился в российском законодательстве в середине 1990-х гг. Федеральным законом "Об информации, информатизации и защите информации", персональные данные были отнесены к категории конфиденциальной информации, установлен запрет на сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного

[3] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.) (ред. от 15.06.1999 г.) // «Собрание законодательства РФ» от 3.02.2014 г. N 5 ст. 419

[4] Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 22.02.2017) "О персональных данных" // «Российская газета», 29.07.2006 № 4131

решения.[5] При этом содержание понятия "персональные данные" в названном Федеральном законе не было раскрыто. Спустя два года был издан Указ Президента РФ от 06.03.1997 N 188, которым был утвержден Перечень сведений конфиденциального характера. Согласно ему персональные данные включают в себя сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность.[6]

Позднее, ст. 2 "Модельного закона о персональных данных"[7] перечень сведений, относящихся к персональным данным, был несколько расширен, и стал включать в себя биографические и опознавательные данные, личные характеристики, сведения о семейном, социальном положении, образовании, профессии, служебном и финансовом положении, состоянии здоровья и прочие. И само понятие персональных данных понималось как информация (зафиксированная на материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним.

Под материальным носителем понимались материальные объекты (в том числе физические поля), в которых персональные данные находят свое отображение в виде символов, образов и сигналов. В данном случае видна нацеленность уже в то время на перспективу развития сетей, подобных сети «Интернет», а так же развитие систем по передаче информации с помощью физических полей. Думается, что это было обусловлено уровнем технического развития и начинающимся распространением информационных хранилищ, не требующих материального носителя («тела»).

В отраслевых законах, в зависимости от специфики регулируемых отношений, понимание персональных данных может изменяться. Так, в Трудовом кодексе РФ[8] в качестве персональных данных работника понимается информация, которая необходима работодателю в связи с трудовыми

[5] Федеральный закон от 20.02.1995 N 24-ФЗ "Об информации, информатизации и защите информации" // «Собрание законодательства РФ», 20.02.1995, № 8, ст. 609. (утратил силу)

[6] Терещенко Л. К. Правовой режим персональных данных и безопасность личности - М.: "Закон", 2013, N 6, с.47

[7] Модельный закон "О персональных данных" (принят постановлением на четырнадцатом пленарном заседании Межпарламентской ассамблеи государств - участников СНГ от 16.10.1999 г. N 14-19) // Информационная бюллетень Межпарламентской Ассамблеи государств-участников СНГ, 2000, N 23

[8] "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 01.05.2017) // "Российская газета" от 31 декабря 2001 г. N 256

отношениями и касающаяся конкретного работника. Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем» к персональным данным относит сведения о документе, удостоверяющем личность, адрес места жительства или пребывания личности[9]. В Федеральном законе «Об индивидуальном учете в системе обязательного пенсионного страхования» под персональными данными понимаются сведения, содержащиеся в индивидуальных лицевых счетах застрахованных лиц[10].

В Германии понятие «персональные данные» прошло более длительный путь развития. В 1980 году, в рекомендациях Организации экономического сотрудничества и развития (ОЭСР) по защите личной тайны и трансграничной передаче персональных данных, в понятие «персональной информации» включались такие данные как имя, дата и место рождения, гражданство, семейное положение, брак, родственники, дети, иждивенцы, образование и навыки, информация о пройденном обучении, полученных степенях, званиях и достижениях; стиль жизни и личные предпочтения, потребительские предпочтения, увлечения, спорт, личное поведение в быту; финансовые ресурсы, доход, собственность, недвижимость; финансовые идентификаторы: детали банковских счетов и пароли доступа к ним.

С развитием глобальных информационных технологий, понятие «персональные данные» пополнилось сетевыми идентификаторами: паролями доступа, пользовательскими именами, сетевыми сертификатами, идентификаторами, присвоенными государственными органами - номером идентификационной карты, паспорта, номером социального страхования; биометрическими идентификаторами: ДНК, отпечатками пальцев, сканом сетчатки глаза; данными о расовой и национальной принадлежности, религиозных, политических и философских убеждениях, медицинскими данными; данными о взаимодействии с органами правопорядка и правосудия.

---

[9] Федеральный закон от 07.08.2001 г. №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем» // "Российская газета" от 9.08.2001 г. N 151

[10] Федеральном законе от 01.04.1996 г. №27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» // "Российская газета" от 10.04.1996 г. N 68

В соответствии с п. 1 § 3 Федерального закона «О защите информации» Федеральной Республики Германия[11], под персональными данными понимается конкретная информация о личных или материальных обстоятельствах идентифицированного или идентифицируемого физического лица. При определении персональных данным может применяться Директива 95/46/ЕС[12]. В соответствии с п. а ст.2 Директивы 95/46/ЕС, "персональные данные" означают любую информацию, относящуюся к определенному или определяемому физическому лицу ("субъекту данных"). Определяемым является лицо, которое может быть определено, прямо или косвенно, в частности, через идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

Выделяют особые категории данных, к которым относят расовое или этническое происхождение, политические взгляды, вероисповедание или философское воззрение, членство в профессиональном союзе, а также обработку данных, касающихся здоровья или интимной жизни.

Согласно Директиве Государства-члены обязаны запретить обработку таких персональных данных.

К данным, требующим защиты, согласно закону ФРГ «О защите персональных данных» (ДСГ) относятся несколько иной, и более широкий список, в том числе и особые категории данных: персональные данные к банковским счетам или кредитным картам; данные, полученные в результате профессиональной деятельности (врачебной, страховой и т.п.); меры социальной защиты; административное или уголовное преследование и наказание; расовое или этническое происхождение; политические взгляды; вероисповедание или философское воззрение; членство в профессиональном союзе; здоровье; интимная жизнь.

---

[11] § 3 Abs. 1 BDSG

[12] Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24.10.1995 г. «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // N L 281, 23.11.1995 г., стр. 31

Также, как и в российском праве, немецкое право деформирует понятие персональных данных, оно может дополняться своими специфическими объектами в зависимости от регулируемой отрасли. В данных случаях применение такого расширительного толкования используется не только во внутригосударственном праве, а так же на уровне международных актов. Это обусловлено необходимостью выделения составных частей персональных данных для более полного и конкретного регулирования в различных областях применения Директив.

Так, в Директиве 2002/58/ЕС[13] выделяются такие составные части, как данные трафика, данные местоположения и сообщения:

1. под данными трафика понимаются данные, обработанные в целях осуществления передачи сообщения по сети электронной связи или в целях формирования счета за пользование услугами электронной связи;
2. под данными местоположения понимаются любые данные, обработанные в сети электронной связи или службой предоставления услуг электронной связи, отражающие географическое местоположение конечной станции пользователя общедоступных услуг;
3. под сообщением понимается любая информация, которой обмениваются или которая передается между ограниченным кругом лиц посредством общедоступных услуг электронной связи. В это понятие не включается информация, передаваемая в рамках широкого оповещения общественности по сети электронной связи, за исключением случаев, когда передаваемая информация может иметь отношение к определенному пользователю или абоненту, получающему эту информацию.

Проведя аналогию и сравнив законодательное определение персональных данных, можно выделить ряд обязательных черт, им присущих, подпадающим под охрану законодательством:

[13] Директива Европейского Парламента и Совета Европейского Союза 2002/58/ЕС от 12.07.2002 г. «в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи» // N L 201, 31.07.2002 г., с. 37

Первое, что необходимо отметить, - это то, что субъектами персональных данных могут выступать только физические лица. Контактные данные и реквизиты юридического лица, а также иные сведения, по которым можно его определить, не подпадают под понятие персональных данных.

Во-вторых, соответствующие сведения должны обладать определенным идентифицирующим потенциалом для того, чтобы признаваться персональными данными. Некоторые виды сведений являются уникальными в своем роде, что позволяет однозначно установить на их основе определенное физическое лицо, например паспортные данные.

В-третьих, не имеет значения, соответствуют данные действительности или нет, являются они точными или полными, вымышленными или достоверными. Даже недостоверные или неточные сведения могут прямо или косвенно указывать на определенное лицо, что является достаточным основанием для признания их персональными данными.

Если те или иные сведения подпадают под понятие персональных данных, их обработка должна осуществляться в соответствии с установленными требованиями.[14]

b. Правовой режим персональных данных.

Правовому режиму присущи следующие основные признаки. Он устанавливается в законодательстве и обеспечивается государством. Правовой режим имеет цель специфическим образом регламентировать конкретные области общественных отношений, выделяя во временных и пространственных границах те или иные субъекты и объекты права. Он представляет собой особый порядок правового регулирования, состоящий из юридических средств и характеризующийся определенным их сочетанием, и создает конкретную степень благоприятности либо неблагоприятности для удовлетворения интересов отдельных субъектов права.

---

[14] Баринова Е.В. Правовой режим персональных данных // Научное сообщество студентов: Междисциплинарные исследования: сб. ст. по мат. XI междунар. студ. науч.-практ. конф. № 8 (11). URL: https://sibac.info/archive/meghdis/8(11).pdf (дата обращения: 16.04.2017)

Правовые режимы придают адекватность и эластичность юридической форме, позволяют ей более четко улавливать различия неоднородных социальных связей, точнее реагировать и учитывать особенности разных субъектов и объектов, временные и пространственные факторы, включенные в сферу действия права.

Однако законодатель определяет правовой режим персональных данных иным способом.

Так, согласно п.1 ст.4 "Модельного закона о персональных данных"[15], к нему относятся нормативно установленные правила, определяющие условия доступа, хранения, уточнения, передачи, блокирования, обезличивания и уничтожения персональных данных.

Основу правового режима персональных данных признают такие положения: персональные данные, находящиеся в ведении держателя, относятся к конфиденциальной информации; по желанию субъекта для его персональных данных может быть установлен режим общедоступной информации (био-, библиографические справочники, телефонные книги, адресные книги, частные объявления и т.д.); с момента смерти субъекта персональных данных правовой режим персональных данных подлежит замене на режим архивного хранения или иной правовой режим, предусмотренный национальным законодательством; правовой режим для персональных данных, полученных в результате деятельности правоохранительных органов, устанавливается в соответствии с национальным законодательством; защита персональных данных умершего лица может осуществляться другими лицами, в том числе наследниками, в порядке, предусмотренном национальным законодательством о защите чести, достоинства, деловой репутации, личной и семейной тайн.

Режим конфиденциальности персональных данных снимается в случаях обезличивания персональных данных, требований субъекта в отношении своих

[15] Модельный закон "О персональных данных" (принят постановлением на четырнадцатом пленарном заседании Межпарламентской ассамблеи государств - участников СНГ от 16.10.1999 г. N 14-19) // Информационная бюллетень Межпарламентской Ассамблеи государств-участников СНГ, 2000, N 23

персональных данных, не противоречащих национальному законодательству и включения персональных данных в общедоступные базы данных.

Правовой режим персональных данных невозможно рассматривать раздельно от защиты таких данных. В немецкой теории и законодательстве выделяются определенные принципы правовой охраны персональных данных.

Исходным пунктом всех принципов защиты данных является законная основа посягательства. Освобождение от репрессивного запрета может быть достигнуто путем соответствующего Конституции закона или другого нормативного акта. Предусмотренная защита нижеследующих основополагающих принципов подразумевает в себе, кроме того, право отказа от защиты. Это происходит таким образом, что субъект данных разрешает это посягательство. Такое разрешение согласно Федеральному закону о защите данных должно предоставляться им добровольно[16], распространяться только на этот специальный случай[17], действительно выражать волю субъекта данных при его полном понимании фактических обстоятельств дела и без малейших сомнений.

Соотношению «правило-исключение» следует принцип целевого использования. Этот принцип означает, что персональные данные могут собираться только для определенных и законных целей и не могут использоваться иным образом, несовместимым с этими целями[18].

Принцип целевого назначения простирается на принцип целевого хранения. Персональные данные не могут сохраняться или обрабатываться дольше, чем это необходимо для реализации легитимных целей. Эти принципы действуют также в сфере личной жизни. Дальнейшее развитие этого принципа представляет право на забвение, ст. 17 GVE.

Соотношению «правило-исключение» следует принцип прозрачности. Принцип прозрачности сформулирован в декларативной части 38 Директивы

[16] § 4a Abs. 1 S. 1 BDSG; Art. 7a) RL. 95/46.
[17] § 4a Abs. 1 S. 2 BDSG.
[18] Art. 6 Abs. 1 b RL 95/46.

95/46/EC[19]: «Принимая во внимание, что обработка данных должна быть справедливой, субъект данных должен иметь возможность узнать о существовании операций по обработке и, если данные получены от него, получить точную и полную информацию об обстоятельствах сбора». Принцип прозрачности для мобильных средств хранения и обработки персональных данных уточняется в п. 3 § 6c Федерального закона о защите данных, согласно которому процессы передачи данных, которые активируют обработку данных на носителе информации, должны четко распознаваться субъектом данных[20].

Защита данных – это не только защита от посягательств, но и предоставление гарантии при передаче данных. Этой цели служат меры предосторожности, которые известны под наименованием Privacy by Design (принцип "проектируемая конфиденциальность")[21]. Каждый, кто работает с персональными данными третьих лиц, должен нести ответственность за использование соответственных технологий.

Принцип обязательности связан с догматикой ограничения основных прав. Право на информационное самоопределение гарантировано не безгранично, законодатель может его ограничить в целях защиты общественных интересов.[22] При этом законодатель действует согласно принципу пропорциональности. Из этого следует, что посягательство должно быть необходимым для цели применения. Обязательность в праве защиты данных является более жёсткой, чем излишний административный запрет. Сбор, обработка и использование персональных данных допустимы только в том случае, если это необходимо для правомерного исполнения заданий органа, использующего такие данные, для тех целей, для которых они в каждом отдельном случае обрабатываются. К тому же при автоматизированной обработке персональных данных необходимо выбрать или разработать такие

[19] Директива Европейского Парламента и Совета Европейского Союза 95/46/EC от 24.10.1995 г. «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // N L 281, 23.11.1995 г., стр. 31

[20] § 8 Abs. 2 HDSG

[21] Schaar, P., Privacy by Design, Режим доступа: http://www.bfdi.bund.de/SharedDocs/Publikationen/%22PrivacyByDesign%22.pdf?__blob=publicationFile. (дата обращения: 19.04.2017)

[22] BVerfG, Urteil vom 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83-, BVerfGE 65, 1 (43 ff.).

критерии, которые определяют наличие только такого ограниченного количества персональных данных, которое необходимое для достижения цели.

Таким образом вытекает следующий принцип защиты данных - это принцип уменьшения и минимизации данных, который конкретизирует принцип обязательности и распространяется на все органы, использующие такие данные.

Контроль и надзор за обработкой персональных данных должен быть независимым и быть в состоянии эффективно защищать персональные данные. Из этого вытекают нарастающие функциональные и организаторские требования к соблюдению и усовершенствованию контроля.

Принципы установлены ст. 6 Директивы 95/46/ЕС, которая гласит, что Государства-участники примут меры, чтобы персональные данные: обрабатывались корректно и законно (a); собирались для объявленных, явных и законных целей, и в дальнейшем не обрабатывались каким-либо образом, несовместимым с этими целями. Дальнейшая обработка данных для исторических, статистических или научных целей не считается несовместимой с данными принципами при условии, что государства-участники обеспечат соответствующие гарантии (b); были адекватными, относящимися к делу и не избыточными в отношении целей, для которых они собираются и/или в дальнейшем обрабатываются (c); были точными и - если необходимо - актуальными; должны быть предприняты любые обоснованные шаги, чтобы неточные или неполные данные, применительно к целям, для которых они собирались или для которых они впоследствии обрабатывались, удалялись или уточнялись (d); хранились в форме, позволяющей идентификацию субъектов данных не долее, чем это необходимо для целей, с которыми данные собирались или впоследствии обрабатывались. Государства-участники установят необходимые гарантии для персональных данных, хранимых более длительные сроки в исторических, статистических или научных целей (e).

Проведя анализ правового режима персональных данных, мы приходим к выводу, что вышеуказанные принципы создают необходимое социальное

состояние и высокую степень благоприятности для удовлетворения интересов субъектов персональных данных и защиты таких данных.

1.2 Сравнительный анализ правового регулирования

Во многих странах вопрос об обеспечении защиты персональных данных стал актуален намного раньше, чем в России. Именно поэтому институт защиты персональных данных в других странах является более развитым.

Одним из первых документов в вопросе регулирования правового положения персональных данных и их защите является Конвенция Совета Европы о защите личности в связи с автоматической обработкой персональных данных[23].

В Европейской конвенции «О защите личности в связи с автоматической обработкой персональных данных» рассматривается порядок сбора, хранения, способы физической защиты персональных, а также принципы доступа к таким данным. Определен порядок обеспечения реализации прав человека на уважение частной жизни и свободу информации, которые зафиксированы в 8 и 9 статьях Конвенции о защите прав человека и основных свобод[24].

В статье 8 Европейской конвенции «О защите прав человека и основных свобод» рассматриваются права на уважение частной и семейной жизни. Согласно конвенции, каждый человек имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции и не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случая, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности, или защиты прав и свобод других лиц.

Согласно положениям конвенции, каждый человек имеет право на свободу мысли, совести и религии. Это право включает свободу менять свою религию или убеждения и свободу исповедовать свою религию или убеждения

[23] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.) (ред. от 15.06.1999 г.) // «Собрание законодательства РФ» от 3 февраля 2014 г. N 5 ст. 419

[24] Конвенция о защите прав человека и основных свобод ETS N 005 (Рим, 4 ноября 1950 г.) (ред. от 11.06.1994г.) // «Собрание законодательства РФ», 18 мая 1998 г., N 20

как индивидуально, так и сообща с другими, публичным или частным порядком, в богослужении, обучении, отправлении религиозных и культовых обрядов.

Одной из ключевых особенностей в данном вопросе, согласно Конвенции, заключается в том, что свобода исповедовать свою религию или убеждения подлежит лишь ограничениям, которые предусмотрены законом и необходимы в демократическом обществе в интересах общественной безопасности, для охраны общественного порядка, здоровья или нравственности или для защиты прав и свобод других лиц.

Можно выделить три основные тенденции международно-правового регулирования института защиты персональных данных, относимого к процессам автоматизированной обработки информации.

Первая тенденция - декларирование права на защиту персональных данных, как неотъемлемой части фундаментальных прав человека, в актах общегуманитарного характера, принимаемых в рамках международных организаций.

Второй тенденцией является закрепление и регулирование права за защиту персональной информации в актах регулятивного характера Европейского Союза, Совета Европы, отчасти Содружества Независимых Государств и некоторых региональных международных организаций. Этот класс норм – наиболее универсальный и непосредственно касается прав на защиту персональных данных в процессах автоматизированной обработки информации.

Третья тенденция подразумевает включение норм об охране конфиденциальной информации (в том числе, и персональной) в международные договоры.

Первый способ – исторически появился раньше остальных. В современном мире информационные права и свободы являются неотъемлемой частью фундаментальных прав человека.

Всеобщая декларация прав человека 1948 г.[25] провозглашает: «Никто не может подвергаться произвольному вмешательству в личную и семейную жизнь, произвольным посягательствам на тайну его корреспонденции» и далее: «Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств». Международный пакт о гражданских и политических правах 1966г. в этой части повторяет декларацию. Конвенция 1950 г.[26] детализирует это право: «Каждый человек имеет право на свободу выражения своего мнения. Это право включает свободу придерживаться своего мнения, получать и распространять информацию и идеи без вмешательства со стороны государственных органов и независимо от государственных границ».

Указанные международные документы закрепляют информационные права человека.

С момента своего появления первые нормы о защите персональных данных рассматривались в контексте права на неприкосновенность частной жизни. Реалии времени, стремительное развитие информационных технологий, активный сбор и обработка персональных данных как в сфере частной жизни, так и в публичных отношениях индивидов с организациями и властными структурами заметно меняют содержание правовой категории персональных данных Данная категория стремительно вырывается за пределы частной жизни.[27]

В настоящее время на международном уровне сформировалась устойчивая система взглядов на информационные права человека. В обобщенном плане это - право на получение информации, право на частную жизнь с точки зрения охраны информации о ней, право на защиту информации как с точки зрения безопасности государства, так и с точки зрения безопасности бизнеса, включая финансовую деятельность.

---

[25] Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.) // "Российская газета" от 10 декабря 1998 г.

[26] Конвенция о защите прав человека и основных свобод ETS N 005 (Рим, 4 ноября 1950 г.) (ред. от 11.06.1994г.) // «Собрание законодательства РФ», 18 мая 1998 г., N 20

[27] Вуколова, Т. Законодательство о персональных данных в Германии и России. Сравнительно-правовое исследование //Интеллектуальная собственность. Авторское право и смежные права. -2016. - № 4. - с. 22

Второй способ - более детального регулирования права на защиту персональной информации связан со все возрастающей в последние годы интенсивностью обработки персональной информации с помощью автоматизированных компьютерных информационных систем. В последние десятилетия в рамках ряда международных организаций был принят ряд международных документов, развивающих основные информационные права в связи с интенсификацией трансграничного обмена информацией и использованием современных информационных технологий. Среди таких документов можно назвать следующие:

Совет Европы в 1980 г. разработал Европейскую конвенцию о защите физических лиц в вопросах, касающихся автоматической обработки личных данных[28]. В Конвенции определяется порядок сбора и обработки данных о личности, принципы хранения и доступа к этим данным, способы физической защиты данных. Конвенция гарантирует соблюдение прав человека при сборе и обработке персональных данных, принципы хранения и доступа к этим данным, способы физической защиты данных, а также запрещает обработку данных о расе, политических взглядах, здоровье, религии без соответствующих юридических оснований.

В Европейском Союзе вопросы защиты персональных данных регулируются целым комплексом документов. В 1979 г. была принята Резолюция Европарламента «О защите прав личности в связи с прогрессом информатизации». Резолюция предложила Совету и Комиссии Европейских сообществ разработать и принять правовые акты по защите данных о личности в связи с техническим прогрессом в области информатики. В 1980 году приняты Рекомендации Организации по сотрудничеству стран-членов Европейского Союза «О руководящих направлениях по защите частной жизни при межгосударственном обмене данными персонального характера».

В настоящее время вопросы защиты персональных данных детально регламентируются директивами Европарламента и Совета Европейского

[28] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.) (ред. от 15.06.1999 г.) // «Собрание законодательства РФ» от 3.02.2014 г. N 5 ст. 419

Союза. Это Директивы № 95/46/ЕС[29] и № 2002/58/ЕС[30] Европейского парламента и Совета Европейского Союза от 24 октября 1995 года «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных», Директива № 97/66/ЕС Европейского парламента и Совета Европейского Союза от 15 декабря 1997 года, касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций и другие документы.

Новое поколение европейского законодательства о защите персональных данных связано с Директивой 2002/58/ЕС об обработке персональных данных и защите конфиденциальности и личной тайны в сфере электронных коммуникаций, дополняющей действие Директивы 95/46/ЕС Основной целью нового документа является обеспечение защиты прав и свобод пользователей средств электронной связи в отношении их персональных данных и защита права на личную тайну (статья 7), а также минимизация обработки персональных данных и стимулирование использования анонимных данных там, где это возможно (статья 9).[31]

Существенное влияние на формирование института защиты персональных данных оказал Суд Европейских сообществ. В мае 2003 года было вынесено первое решение по данному вопросу. На повестке дня в австрийском деле Rechnungshof стоял вопрос о том, возможно ли публиковать данные о заработной плате публичных служащих. Суд четко определил, что положения Директивы ЕС имеют отношение и к обработке персональных данных публичном секторе.

В ноябре 2003 года в шведском деле Lindqvist Суд постановил, что основные положения Директивы ЕС - принципы защиты персональных данных - имеют прямое отношение и к Интернет-сайтам. В частности, речь шла о том,

---

[29] Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24.10.1995 г. «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // N L 281, 23.11.1995 г., стр. 31

[30] Директива Европейского парламента и Совета Европейского Союза № 2002/58/ЕС, Режим доступа: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1490611521075&uri=CELEX:32002L0058 (дата обращения - 29.03.2017).

[31] Вуколова, Т. Законодательство о персональных данных в Германии и России. Сравнительно-правовое исследование //Интеллектуальная собственность. Авторское право и смежные права. -2016. - № 4. - с. 27

что многие положения о трансграничной передаче данных несколько не соответствуют реалиям Интернета и нуждаются в корректировке.

Акты Европейского Союза характеризуются детальной проработкой принципов и критериев автоматизированной обработки данных, прав и обязанностей субъектов и держателей персональных данных, вопросов их трансграничной передачи, а также ответственности и санкций за нанесение ущерба.

В рамках Организации по экономическому сотрудничеству и развитию (ОЭСР) действуют «Основные положения о защите неприкосновенности частной жизни и международных обменов персональными данными», которая была принята 23 сентября 1980 года. В преамбуле этой Директивы говорится о необходимости разработать Основные положения, которые могли бы помочь унифицировать национальные законы о неприкосновенности частной жизни и, обеспечивая соблюдение соответствующих прав человека, вместе с тем не допустили бы блокирования международных обменов данным. Настоящие положения применяются как в государственном, так и в частном секторе к персональным данным, которые либо в связи с процедурой их обработки, либо в связи с их характером или контекстом их использования несут в себе угрозу нарушения неприкосновенности частной жизни и индивидуальных свобод. В ней определена необходимость обеспечения персональных данных должными механизмами защиты от рисков, связанных с их потерей, уничтожением, изменением или разглашением, несанкционированным доступом.

Межпарламентской ассамблеей государств – участников СНГ 16 октября 1999г. принят Модельный Закон «О персональных данных»[32].

Третий способ закрепления норм о защите персональных данных - закрепление их правовой охраны в международных договорах.

[32] Модельный закон "О персональных данных" (принят постановлением на четырнадцатом пленарном заседании Межпарламентской ассамблеи государств - участников СНГ от 16.10.1999 г. N 14-19) // Информационная бюллетень Межпарламентской Ассамблеи государств-участников СНГ, 2000, N 23

Статьи об обмене информацией включаются в международные договоры о правовой помощи, об избежании двойного налогообложения, о сотрудничестве в определенной общественной, культурной сфере.

По ст. 25 Договора между Российской Федерацией и США «об избежании двойного налогообложения и предотвращении уклонения от налогообложения в отношении налогов на доходы и капитал»[33] государства обязаны предоставлять информацию, составляющую профессиональную тайну. Договор между Российской Федерацией и Республикой Индией «о взаимной правовой помощи по уголовным делам» содержит статью 15 «Конфиденциальность»: запрашиваемая сторона может потребовать сохранения конфиденциальности переданной информации. Практика заключения международных договоров показывает стремление договаривающихся государств соблюдать международные стандарты защиты персональных данных.

В Российской Федерации долгое время политике в области защите персональных данных не уделялось должного внимания. Одним из немногих законодательных актов, ранее регулирующих процесс обработки персональных данных, являлся Указ Президента РФ "Об утверждении перечня сведений конфиденциального характера"[34].

Только после подписания Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных в 2001 году были изданы основные законодательные акты, которые регулируют организацию процессов, связанных с защитой персональных данных на современном этапе. Сейчас список документов в данной области достаточно обширен, однако сохранились пробелы в обеспечении защиты персональных данных.

В Германии ситуация с регулированием персональных данных была диаметрально противоположной. Первый закон «О персональных данных»

---

[33] Договор между Российской Федерацией и Соединенными Штатами Америки об избежании двойного налогообложения и предотвращении уклонения от налогообложения в отношении налогов на доходы и капитал. От 17.06.1992

[34] Указ Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера" // «Собрание законодательства РФ» от 10.03.1997 г. N 10, ст. 1127

появился в федеральной земле Гессен в 1970 году[35], данный нормативно-правовой акт был не только первым на территории Германии, но и первым в мировой практике. Несмотря на запрет сообщать о полученных персональных данных третьим лицам, закон, однако, не содержал требований получать согласие субъекта персональных данных на обработку таких данных.

Федеральный закон о персональных данных появился на 7 лет позднее, в 1977 году. Но и он не содержал всех необходимых положений для защиты субъекта персональных данных в ФРГ. В настоящее время на территории ФРГ действует Закон "О персональных данных" от 20 декабря 1990 года. Однако нельзя рассматривать систему законодательства анализируя только специальные нормативно-правовые акты, необходимо использовать комплексный подход.

Основой внутригосударственной нормативно-правовой базы является Конституция. Так, Конституция Российской Федерации определяет основу регулирования правоотношений в области персональных данных, устанавливая, что без согласия лица не допускаются сбор, хранение, использование и распространение информации о его частной жизни.[36] Основной закон ФРГ закрепляет не только право на свободное распространение информации и основы защиты персональных данных, но и сразу же указывает на возможные допущения по сбору таких данных без согласия субъекта персональных данных.[37]

Специальные федеральные законы устанавливают принципы осуществления обработки информации ограниченного доступа, в частности персональных данных, обязанности оператора, осуществляющего такую обработку, а также права субъекта персональных данных. Данными законами регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов (земель), иными государственными

[35] § 1 Abs. 2 HDSG
[36] Тараканова С.С. Правовой режим персональных данных, режим доступа: http://www.samoupravlenie.ru/4905.php (дата обращения: 01.05.2017)
[37] Art. 13 Abs.2 GG

органами, органами местного самоуправления, иными муниципальными органами, юридическими и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, 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, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

Согласно тексту такого специального закона[38] (и российского, и немецкого), основной его целью 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.

Помимо специализированного закона, практическое значение имеют правила и требования в иных отраслевых федеральных законах, где на общие принципы и условия работы с персональными данными накладываются специфика регулирования именно такой отрасли права[39].

В этой сфере довольно много подзаконные актов, которые могут расширять или сужать перечень данных, подлежащих защите и относящихся к персональным данным, устанавливать правила применения норм, закрепленных в федеральных законах и давать указания своим структурным подразделениям по действиям, необходимым для защиты персональных данных[40].

---

[38] Такими законами являются Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 22.02.2017) "О персональных данных" // «Российская газета», 29.07.2006 № 4131; BDSG // BGBl. I S. 2954, 2955, 20. Dezember 1990.

[39] К таким законодательным актам можно отнести: Федеральный закон от 19 декабря 2005 г. N 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных"; Федеральный закон Российской Федерации 30 декабря 2001 г. № 197-ФЗ "Трудовой кодекс Российской Федерации (14 глава)"; Федеральный закон Российской Федерации от 3 декабря 2008 г. N 242-ФЗ "О государственной геномной регистрации в Российской Федерации"; Федеральный закон Федеративной Республики Германия от 9 мая 1998г "Об усилении борьбы с организованной преступностью".

[40] К таким законодательным актам можно отнести: Указ Президента Российской Федерации от 6 марта 1997 г. № 188 "Об утверждении перечня сведений конфиденциального характера"; Постановление Правительства

В Германии более распространено законодательство субъектов. В большинстве субъектов (земель) имеется свой закон о защите персональных данных, и, согласно практике правоприменения, в большинстве случаев при разрешении споров и более детальном регулировании механизмов защиты используются законы именно земель, а не правовые акты федерального уровня.

Внутренние акты федеральных органов власти Российской Федерации являются важнейшей частью регулирования защиты персональных данных, поскольку регулируют работу всех структурных подразделений органа, обеспечивая исполнение всех законных предписаний и законодательных актов в сфере защиты персональных данных.[41] Часть таких актов носит рекомендательный характер[42].

Важное место в развитии защиты персональных данных занимают научные труды, поскольку изначально именно в научных кругах появились предложения о создании такого института, о выделении персональных данных

Российской Федерации от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"; Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных"; Постановление Правительства Российской Федерации 2 июня 2008 г. № 419 "О федеральной службе по надзору в сфере связи и массовых коммуникаций"; Постановление Правительства Российской Федерации от 21 марта 2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"; Постановление Правительства Российской Федерации от 01 ноября 2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"; Постановление Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

[41] К таким актам можно отнести: Приказ ФСТЭК России от 11 февраля 2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"; Приказ ФСТЭК России от 18 февраля 2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"; Приказ Роскомнадзора от 05 сентября 2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных"; Приказ ФСТЭК России от 31 августа 2010 г. N 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»; «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСБ РФ 21.02.2008 N 149/6/6-622). «Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли» (утв. ФСБ России от 10.08.2010 г. № 149/7/2/6-1203); Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год.

[42] К таким трудам можно отнести: Методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год; «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утв. ФСБ РФ 21.02.2008 N 149/54-144).

и аргументирование необходимости правового закрепления защиты таких данных. Научные труды являются вектором развития законодательства и правоприменения в будущем. Так, например, Просветовой О.Б. было предложено определение автоматической обработке персональных данных[43], впоследствии нашедшее закрепление в федеральном законодательстве.

Анализируя комплекс актов, можно отметить тенденцию все к большей унификации, и все большему соответствию законодательства международным нормам, в целях наиболее эффективной защиты персональных данных.

[43] См.: Просветова О.Б. Защита персональных данных: Автореф. дис...канд. юр. наук. Воронеж. 2005.

Глава 2. Защита персональных пользовательских данных

2.1 Доступ, хранение и передача персональных данных: юридические и технические требования

Доступ, хранение и передача, наряду с другими производимыми действиями над персональными данными объединяются в единое понятие обработка персональных данных. В специальных законах, посвященных регулированию защиты персональных данных, как правило, закреплены понятие, общие принципы и условия обработки персональных данных.

Обработка персональных данных - это любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.[44]

Российской федеральное законодательство устанавливает принципы обработки персональных данных. Обработка персональных данных должна осуществляться на законной и справедливой основе, должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Запрещено объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.[45]

Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки. При обработке персональных

[44] Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 22.02.2017) "О персональных данных" // «Российская газета», 29.07.2006 № 4131
[45] Там же

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

Законодатель вводит понятие "автоматизированная обработка персональных данных", под которой понимается обработка персональных данных с помощью средств вычислительной техники. Автоматизированная обработка персональных данных является частным случаем обработки персональных данных по отношению к действиям по обработке персональных данных как таковых. Федеральный закон не содержит специальных требований, применяемых к неавтоматизированной обработке информации, следовательно, к автоматизированной и неавтоматизированной обработке персональных данных применяются одни и те же требования.

Этот вывод также следует из разъяснений Роскомнадзора термина "база данных", в соответствии с которым база данных - любой упорядоченный массив информации вне зависимости от материального носителя. Вследствие вышеуказанного, к обработке информации предъявляются одинаковые требования вне зависимости от материального носителя баз персональных данных (электронной или бумажной, в том числе написанной от руки).

Немецкий законодатель руководствуется иным подходом. Обработка персональных данных - это действия по сохранению, изменению, передаче, блокировке, удалению данных.

Таким образом, законодательство устанавливает ключевой критерий - воздействие на данные каким-либо образом, а такое понятие, как использование, является вспомогательным понятием т.е. применением данных без непосредственного воздействия на них[46].

В отношении типов действий отметим, что если российское законодательство оперирует только одним термином - "обезличивание",

[46] § 3 Abs. 1 S. 5 BDSG.

которое также включено в понятие обработки персональных данных, то в немецком законодательстве различаются такие действия, как "анонимизация" и "псевдонимизация" данных. При этом указанные действия также обработкой персональных данных не являются. При "анонимизации" действия по идентификации личности связаны со значительными временными и финансовыми затратами, а "псевдонимизация" позволяет существенно усложнить или вовсе исключить возможность идентификации личности.

Немецкий законодатель устанавливает тождественное с российским аналогом понятие автоматизированной обработки персональных данных, так под автоматизированной обработкой персональных данных понимается сбор, обработка и использование персональных данных с использованием электронных вычислительных средств.

Выделяются особые категории данных, к которым относят расовое или этническое происхождение, политические взгляды, вероисповедание или философское воззрение, членство в профессиональном союзе, а также обработку данных, касающихся здоровья или интимной жизни. Согласно Директиве 95/46/ЕС[47] Государства-члены обязаны запретить обработку таких персональных данных.

В Российской Федерации способы защиты персональных данных вызывают оживленные дискуссии, поводами к которой являются поправки[48] в Федеральный закон "О персональных данных": законодатель систематизировал перечень действий в отношении персональных данных, которые должны производиться исключительно на территории Российской Федерации, и какие могут быть произведены за рубежом.

Согласно нововведениям на территории Российской Федерации должны осуществляться: запись, систематизация, накопление, хранение, уточнение (обновление, изменение) и извлечение персональных данных граждан

[47] Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24.10.1995 г. «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // N L 281, 23.11.1995 г., стр. 31

[48] Федеральный закон от 21.07.2014 г. N 242-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях" // "Российская газета" от 23.07.2014 г. N 163

Российской Федерации. Такие действия, как: сбор, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение, могут осуществляться не на территории Российской Федерации. Данные указания фактически обязывают к переносу баз данных с информацией о российских гражданах, находящихся за рубежом, на территорию Российской Федерации, что в свою очередь связано со значительными временными и финансовыми издержками.

При этом, например, немецкое законодательство не создает необходимости производить определенные действия исключительно на территории ФРГ. Анализ Закона ФРГ "О персональных данных" позволяет установить, что требования закона базируются на принципе адекватной защиты, в соответствии с которым обязательного получения разрешения для сбора, передачи и обработки персональных данных в страны с адекватной защитой не требуется, и наоборот: обработка и передача информации в страны, не обеспечивающие адекватную защиту, требуют наличия такого согласия.

Доступ и сбор персональных данных

Доступ и сбор персональных данных осуществляется только с согласия субъекта таких данных. Это требование является одним из основополагающих и важнейших принципов обработки персональных данных, закрепленный не только на национальном, но и на международном уровне. При отсутствии такого согласия, к оператору применяются меры ответственности

В немецком законодательстве устанавливаются лишь общие требования к такому согласию. Согласие предоставляется на добровольной основе, для определенной цели сбора, обработки или использования, а также в связи с определенными потребностями и обстоятельствами. Практическое значение имеют последствия непредоставления такого согласия. Согласие предоставляется в письменной форме, если обстоятельства не требуют предоставления согласия в иной форме. Предоставление согласия на использование персональных данных в научных целях требует обязательной письменной формы. В отношении специальной категории данных

устанавливается обязательность указания типа таких данных в согласии на обработку.

Положения о содержании согласия об обработке персональных данных в российском законодательстве урегулированы более подробно в статье 9 Федерального закона "О персональных данных". Федеральный закон устанавливает, что согласие предоставляется на основании волеизъявления субъекта персональных данных или его законного представителя. Что касается формы согласия, то оно предоставляется в любой, позволяющей подтвердить факт его получения, форме. Таким образом, российское законодательство не устанавливает обязательных требований к письменной форме, однако обязательство доказывания наличия согласия возлагается на лицо, осуществляющее обработку данных. Таким образом, российское законодательство, так же как и немецкое, устанавливает презумпцию вины оператора персональных данных.

Устанавливается примерное содержание согласия о персональных данных. Оно должно включать личные данные субъекта (представителя) персональных данных; личные данные оператора, получающего согласие субъекта персональных данных; цель обработки персональных данных; перечень персональных данных, на обработку которых дается согласие субъекта персональных данных; перечень действий с персональными данными, на совершение которых дается согласие; общее описание используемых оператором способов обработки персональных данных; срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом; подпись субъекта персональных данных.

Федеральный закон "О персональных данных" в части 8 статьи 9 устанавливает, что персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия определенных оснований. Такими основаниями могут служить: обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с

федеральным законом; персональные данные сделаны общедоступными субъектом персональных данных и т.п.

В Федеральном законе, по нашему мнению, допущена некоторая юридико-техническая неточность. В части 1 статьи 9 Федерального закона "О персональных данных" указывается, что персональные данные могут быть предоставлены как субъектом персональных данных, так и его представителем. В части 6 статьи 9 Федерального закона "О персональных данных"[49] установлено, что согласие на обработку персональных данных может быть предоставлено представителем только в случае недееспособности лица.

Однако в части 8 устанавливается ограничение получения персональных данных от лица, не являющегося субъектом персональных данных. В число указанных ограничений не внесена оговорка о том, что недееспособность также является основанием предоставления согласия от представителя недееспособного лица. Таким образом, может возникнуть ситуация, при которой оператор может отказать представителю в обработке персональных данных в связи с отсутствием такого основания в Федеральном законе. Изложение законодательной нормы в такой форме может привести к правовой неопределенности, повлечь ограничение реализации правового интереса гражданина, а так же основных прав и свобод.

С точки зрения юридической техники, в начале статьи стоят более общие положения, а потом указываются частные случаи. Законодатель отдельно выделил пункт, посвященный недееспособным лицам. Это может выступить основанием к ограничительному толкованию положений ст. 9 ФЗ и свести получение согласия через представителя до этого единичного случая. Тогда применение ч. 8 данной статьи, в которой также упоминается получение согласия через представителя, становится непонятным. Следовательно, необходимо или исключить часть 6, или дополнить ее положением о представителях по доверенности.

[49] Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 22.02.2017) "О персональных данных" // «Российская газета», 29.07.2006 № 4131

Для автоматизированной обработки персональных данных обязательно уведомление об обработке персональных данных в адрес уполномоченного органа, наличие назначенного ответственного за обработку персональных данных в государственном органе, муниципальном органе, у юридического или физического лица. Для автоматизированной обработки персональных данных действует презумпция вины. В то время как для неавтоматизированной обработки персональных данных таких требований в Законе ФРГ "О персональных данных" не установлено. Однако из этого не следует, что неавтоматизированная обработка данных законодателем не регулируется. При неавтоматизированной обработке персональных данных ответственность наступает в общем порядке по нормам Германского гражданского уложения и может быть как договорной, так и деликтной - при наличии вины. Например, в отношении неавтоматизированного сбора персональных данных в медицинских целях в параграфе 28 Закона ФРГ "О персональных данных" устанавливаются специальные требования в части соблюдения врачебной тайны. Ответственность за несоблюдение таких требований предусмотрена в Уголовном кодексе ФРГ[50].

Хранение персональных данных

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом[51].

[50] § 203 Abs. 1,3 StGB

[51] Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 22.02.2017) "О персональных данных" // «Российская газета», 29.07.2006 № 4131

При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, оператор «обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации» - указывается в Федеральном законе №242 от 21 июля 2014 года.[52]

Суть закона заключается в запрете юридическим лицам, которые работают с персональными данными граждан РФ, собирать и хранить эти данные за рубежом – они обязаны локализовать базы данных на территории России. Закон этот вносит важные изменения в ФЗ № 152 «О персональных данных». Больше всего споров возникает вокруг того, что этот закон запрещает хранение персональных данных российских граждан за рубежом. Однако параллельное хранение, на первый взгляд, невозможно отследить. К тому же закон не содержит правовых инструментов, решающих эту проблему.

В российской практике сформировалось несколько видов решений, согласно которым субъект обрабатывающий и хранящий данные остается в правовом поле Российской Федерации

Первым является возможность перестроить архитектуру информационной системы и обеспечить первичную запись, хранение и актуализацию персональных данных в базах на территории России. Хранение и использование копий баз с персональными данными в зарубежных сервисах, таких как Microsoft Azure или Office365, не нарушает закон.

Вторым вариантом законной деятельности в сфере персональных данных является хранение данных в информационной системе за рубежом в зашифрованном виде, а расшифровывать данные только в приложении, находящимся на территории России.

[52] Федеральный закон от 21.07.2014 г. N 242-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях" // "Российская газета" от 23.07.2014 г. N 163

Оживленную дискуссию вызвал пакет «антитеррористических» законопроектов, принятый 6 июля 2016 года. Полноценно закон[53], регулирующий хранение персональных данных, вступает в силу только с середины 2018 года. С этого момента закон обязывает операторов связи хранить записи звонков и любых сообщений пользователей и интернет-трафик в течение полугода. Провайдеры и интернет-ресурсы, внесенные в реестр организаторов распространения информации в сети Интернет, тоже должны хранить весь пользовательский трафик в течение шести месяцев. Кроме того, и телефонные операторы, и интернет-компании уже сейчас должны хранить мета-данные — то есть не содержимое переговоров и сообщений, а информацию о том, что они состоялись в определенное время и в определенном месте. Все эти данные нужно будет передавать правоохранительным органам или суду, при выполнении определенной процедуры.

В немецком праве тоже недавно (16 октября 2015 года) был принят аналогичный законопроект. Однако в отличие от российского аналога он устанавливает объектом сбора и хранения не содержимое коммуникации, а только мета-данные, и устанавливает меньший срок: 10 недель для мета-данных и 4 недели для данных по местонахождению субъекта персональных данных во время коммуникации.

Передача персональных данных

Передача персональных данных носит строго регламентированный порядок, и требует согласия субъекта персональных данных.

Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего

[53] Федеральный закон от 6 июля 2016 г. N 374-ФЗ "О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности" // "Российская газета" от 8 июля 2016 г. N 149

акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом.[54]

В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьями настоящего Федерального закона.

Федеральное законодательство в сфере защиты персональных данных оперирует еще одним понятием - "трансграничная передача данных". Согласно ст. 3 Федерального закона «О персональных данных» трансграничная передача персональных данных - это передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Законодатель вводит специальный подтип передачи персональных данных на территорию иностранного государства и устанавливает в ст. 12 Федерального закона для такой передачи дополнительные правила. Согласно данной статье трансграничная передача может осуществляться как в страны, обеспечивающие адекватную защиту персональных данных, так и не обеспечивающие ее. К странам с эффективной защитой относятся страны, являющиеся сторонами Конвенции о защите физических лиц при автоматизированной обработке персональных данных[55].

---

[54] Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 22.02.2017) "О персональных данных" // «Российская газета», 29.07.2006 № 4131

[55] Критериев, определяющих адекватность защиты прав субъектов персональных данных на территории иностранного государства, действующим законодательством Российской Федерации не предусмотрено.
Оператору, осуществляющему трансграничную передачу персональных данных, необходимо руководствоваться законодательством иностранного государства, на территорию которого осуществляется передача персональных данных, законодательством Российской Федерации в области защиты прав субъектов персональных данных, а также международными нормативными актами, в том числе Конвенцией о защите прав

Трансграничную передачу также возможно осуществлять в страны, не обеспечивающие адекватной защиты в случаях:

1. наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

2. предусмотренных международными договорами РФ;

3. предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

4. исполнения договора, стороной которого является субъект персональных данных;

5. защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

Закон при этом не устанавливает, какими преимуществами обладает трансграничная передача данных в страны, обеспечивающие адекватную защиту данных, и не предусматривает какой-либо упрощенный механизм передачи данных в этом случае.

В немецком законодательстве понятие трансграничной передачи данных как таковое отсутствует. Порядок передачи персональных данных за границу урегулирован Законом ФРГ "О персональных данных"[56]. В законодательстве разделены процедуры передачи персональных данных органам власти и юридическим и физическим лицам, процедуры сбора персональных данных с целью их последующей передачи: в коммерческих целях; в коммерческих

физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. ETS № 108 с учетом перечня стран, подписавших и ратифицировавших данную Конвенцию.

Вторая группа, которые могут претендовать на статус стран, обеспечивающих адекватную защиту персональных данных, это страны, имеющие общенациональные нормативные правовые акты в области защиты персональных данных и уполномоченный надзорный орган по защите прав субъектов персональных данных.

Подробнее см.: Защита прав субъектов персональных данных, режим доступа: https://rkn.gov.ru/treatments/p459/p468/ (дата обращения: 25.04.2017)

[56] § 4b, § 14, § 15, § 28 - 30a (ff) BDSG

целях в анонимной форме; в коммерческих целях для исследования мнений или рынка.

В соответствии с данными параграфами передача персональных данных допускается в страны - члены ЕС, страны - участники Соглашения о Европейском экономическом пространстве, органы ЕС, а также иные иностранные государства. При этом закон не устанавливает обязательных требований к локализации тех или иных типов персональных данных.

Передача персональных данных должна основываться на обеспечении адекватности защиты персональных данных, однако согласно положениям Закона такая адекватность оценивается с учетом всех обстоятельств, которые возникают в связи с необходимостью обработки персональных данных. В частности, характер данных, цель обработки персональных данных, продолжительность предлагаемой обработки, страны происхождения и страны назначения, правила, применимые к получателю персональных данных. Среди прочих критериев адекватной защиты в коммерческих целях передачи персональных данных являются в том числе отсутствие оснований полагать, что субъект персональных данных заинтересован в запрете обработки данных, данные были взяты из открытых источников.

2.2 Основания и процедура раскрытия персональных пользовательских данных

а. Законодательство РФ и Германии

Персональные данные относятся к категории конфиденциальной информации (документированной информации, доступ к которой ограничивается в соответствии с законодательством РФ). Они указаны и в Перечне сведений конфиденциального характера, утвержденным Указом Президента РФ № 188[57], за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральным законом случаях.

В связи с изменениями от 16 октября 2015 года в Германии, и 6 июля 2016 в России, операторы связи, провайдеры и интернет-ресурсы обязаны хранить мета-данные, а в России еще и содержание коммуникации, с целью возможного использования таких данных правоохранительными органами. Основанием в Российской Федерации для раскрытия персональных данных является необходимость их использования в антитеррористической деятельности. Однако ни конкретных оснований, ни определенной процедуры раскрытия таких данных российский законодатель еще не сформулировал. Немецкий законодатель в этом плане ушел далеко вперед, поскольку изменения от 16 октября 2015 года являются уже вторым вариантом законодательного оформления хранения персональных данных операторами и провайдерами связи.

Первоначальный вариант включал в себя схожие положения с нынешним российским законом, срок хранение также был полгода и условия сбора персональных пользовательских данных были аналогичными. Однако Закон был отменен Конституционным судом Германии. Федеральный Конституционный Суд в своем решении от 2 марта 2010, отменил §§ 113a и 113b ТКГ[58] и § 100g пункт 1 предложение 1 Уголовно-процессуального

[57] Указ Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера" // «Собрание законодательства РФ» от 10.03.1997 г. N 10, ст. 1127
[58] Telekommunikationsgesetz // 25. Juli 1996 BGBl. I S. 1120

кодекса[59], поскольку сбор и хранение трафика в соответствии с § 113a ТКГ нарушали статью 10 пункт 1 Основного закона (GG) Германии, в результате чего были так же отменены соответствующие правила, принятые для осуществления директивы 2006/24 / ЕС Европейского парламента и Совета от 15 марта 2006 года о сохранении данных, сгенерированных или обработанных в связи с предоставлением общедоступных услуг электронных коммуникаций или сетей связи общего пользования и Директивы 2002/58/ЕС о внесении изменений.

Некоторые считают и данную юридико-правовую конструкцию неконституционной. Однако имеется ряд черт, существенно отличающие нынешний закон от предыдущего, а именно: объем данных существенно снижен; установлен крайне короткий срок хранения данных.

Нынешний вариант закона Германии о хранении пользовательских данных является более «мягким», поскольку не требует хранения содержания данных трафика и коммуникации, а собирает только мета-данные – данные о времени, месте и участниках коммуникации. Закон вступает в полную силу только в 2018 году, однако уже сейчас имеются закрепленные законодателем акты, регулирующие основания и процедуру раскрытия персональных данных.

Основанием раскрытия таких данных, согласно немецкому законодательству[60], является преследование по закону, а именно по определенным категориям преступлений, их список четко регламентирован в ст.100g Уголовно-процессуального кодекса Германии. К ним относятся особо тяжкие преступления из разных отраслей права. Из уголовного кодекса Германии можно выделить такие категории преступлений[61], как: измена родине и посягательство на основы конституционного и демократического строя на федеральном и региональном уровне, а так же при угрозе безопасности государства извне; особо серьезные случаи нарушения общественного порядка, а именно: формирование преступных организаций, бандформирований, а так же

[59] Strafprozessordnung // 7. April 1987 (BGBl. I S. 1074, ber. S. 1319)
[60] § 100g StPO
[61] Strafgesetzbuch // 13. November 1998 (BGBl. I S. 3322)

террористических организаций; преступление против сексуального самоопределения: изнасилование, насильственные действия сексуального характера; распространение, хранение и приобретение детской и подростковой порнографии; убийство; преступления против личной свободы, принудительный труд, принудительная проституция, незаконная эксплуатация; преступления с экономическим подтекстом: кража группой лиц, разбойное нападение, грабеж с причинением смерти, тяжкие случаи вымогательства, «отмывание» денег и незаконных активов; иные особо тяжкие общественно опасные преступления (геноцид, развязывание войны, нарушение основных прав и свобод человека).

В законе об иностранных гражданах Германии[62] выделяют такие преступные составы, по которым возможно раскрытие персональных данных: расследование деятельности шпионов; расследование деятельности и проникновения через границу преступных организаций, террористических организаций, бандформирований, чья деятельность привела к смертям, среди населения Германии.

Иные основания, имеются среди составов преступлений в законе о борьбе с наркотиками[63], о внешней торговле[64], о надзоре за прекурсорами[65].

Из анализа вышеуказанных актов видно, что раскрытие персональных данных и данных трафика возможно только в случае преступлений, нарушающих конституционные и основополагающие устои общества и законные, особо важные интересы государства.

Условия раскрытия, а также процедура регламентируется уголовно-процессуальным кодексом. При допуске к персональным данным необходимо выполнить ряд условий, только при наличии которых возможно раскрытие таких данных.

---

[62] Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet // 30. Juli 2004 (BGBl. I S. 1950)
[63] Gesetz über den Verkehr mit Betäubungsmitteln // 1. März 1994 (BGBl. I S. 358)
[64] Außenwirtschaftsgesetz // 28. April 1961 (BGBl. I S. 481, 495)
[65] Gesetz zur Überwachung des Verkehrs mit Grundstoffen, die für die unerlaubte Herstellung von Betäubungsmitteln missbraucht werden können // 7. Oktober 1994 (BGBl. I S. 2835)

Первым условием является наличие подозрение лица в совершении или подготовке, покушении на одно из вышеперечисленных преступлений;

Второе условие - соответствие принципу соразмерности. Поскольку при раскрытии персональных данных и данных трафика ограничиваются конституционные права граждан, то необходимо всегда проверять, возможно ли такое ограничение в данном случае, сравнение последствий при раскрытии и при не раскрытии таких данных, и на основе этого принимается решение о возможности использования конфиденциальных данных в данном конкретном случае.

Третьим фактором является отсутствие возможности и перспектив расследования данного преступления без использования данной юридико-правовой формы. В данном случае применяется принцип необходимости, который отражает невозможность эффективного расследования без применения раскрытия персональных данных и данных трафика.

Российский законодатель только начинает формировать нормативно-правовую базу в сфере раскрытия персональных пользовательских данных. и, думается, что более развитая структура правовых актов Германии может быть полезным примером и являться вектором развития законодательства в области раскрытия персональных данных.

b. Нормы международного права и Европейского союза

В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи была принята Директива 2002/58/ЕС[66], закрепляющая обязанность государств-членов Европейского Союза (далее – ЕС) в своем национальном законодательстве гарантировать конфиденциальность передаваемых сообщений и относящихся к ним данных трафика посредством сети связи общего пользования и общедоступных услуг электронной связи. В частности, государства-участники должны запретить прослушивание, несанкционированное подключение,

[66] Директива Европейского парламента и Совета Европейского Союза № 2002/58/ЕС, Режим доступа: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1490611521075&uri=CELEX:32002L0058 (дата обращения - 29.03.2017).

хранение или другие виды перехвата или слежки за сообщениями и относящимися к ним данными трафика, кроме случаев получения санкционированного разрешения на осуществление этих действий в соответствии с пунктом 1 статьи 15 настоящей Директивы.

В свою очередь, возможность государств-членов ЕС принять законодательные меры, ограничивающие некоторые права в области защиты конфиденциальности коммуникаций, если такие ограничения представляют собой необходимую, соответствующую и пропорциональную меру в рамках демократического общества для осуществления защиты национальной (государственной) безопасности, обороны и общественной безопасности, предотвращения, расследования, обнаружения и судебного преследования преступных действий устанавливается в п. 1 ст. 15 Директивы 2002/58/ЕС[67]. В связи с этим государства-члены Европейского Союза могут, помимо прочего, принять законодательные меры, предусматривающие сохранение данных на определенный период по основаниям, предусмотренным в настоящем пункте.

Спустя практически 4 года (15.03.2006 г.) была принята Директива 2006/24/ЕС[68], целиком посвященная хранению персональных пользовательских данных.

Согласно данной Директиве государства-члены ЕС должны обеспечить хранение провайдерами общедоступных услуг электронной связи или сетей общественной связи данных, в частности, необходимых для: отслеживания и идентификации пользователей услуг; определения даты, времени и продолжительности сообщений пользователей; определения местоположения оборудования мобильной связи; идентификации коммуникационного оборудования пользователей (данные IMEI и IMSI вызывающей и принимающей сторон). Соответствующие данные должны храниться не менее 6 месяцев, но не более 2 лет.

---

[67] Директива Европейского Парламента и Совета Европейского Союза 2002/58/ЕС от 12.07.2002 г. «в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи» // N L 201, 31.07.2002 г., с. 37

[68] Директива Европейского парламента и Совета ЕС № 2006/24/ЕС, режим доступа: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0024 (дата обращения – 29.03.2017).

При этом Директива 2006/24/ЕС не распространяется на хранение самого содержания сообщений (в оригинале: «content of electronic communications»).

Несмотря на то, что после принятия Директивы 2006/24/ЕС большинство государств-членов ЕС заявили об откладывании вступления данной директивы в действие на тот или иной период, в итоге ее положения были имплементированы в законодательство некоторых государств-членов ЕС (Швеции, Великобритании, Германии, Дании и другие).

Впоследствии, в ряде государств-членов ЕС соответствующее национальное законодательство, принятое во исполнение Директивы 2006/24/ЕС, было признано неконституционным[69].

А спустя 8 лет после принятия Директивы 2006/24/ЕС Решением Европейского Суда[70] от 08.04.2014 (далее – Решение от 08.04.2014) она была в полном объеме признана недействительной на всей территории ЕС.

Можно выделить три ключевых основания признания Директивы 2006/24/ЕС недействительной.

Во-первых, Директива 2006/24/ЕС, направленная на предотвращения серьезных преступлений, не устанавливает какой-либо связи между необходимостью хранения данных и угрозой общественной безопасности. В частности, нет связи между необходимостью хранения данных и определенным периодом времени и / или конкретной географической зоной, и / или определенным кругом лиц, которые могут быть так или иначе вовлечены в серьезное преступление, или лицами, которые по другим причинам могли бы способствовать предупреждению, выявлению серьезных преступлений (параграф 59 Решения от 08.04.2014).

Во-вторых, Директива 2006/24/ЕС не устанавливает каких-либо объективных критериев, позволяющих определить пределы доступа компетентных национальных органов к сохраненным данным и их последующим использованием в целях предупреждения, выявления или

[69] BVerfG, Urteil vom 02. März 2010 - 1 BvR 256/08 - Rn. (1-345)
[70] Дело № C-293/12 и дело C-594/12, режим доступа: http://curia.europa.eu/juris/liste.jsf?num=C-293/12# (дата обращения – 29.03.2017).

уголовного преследования преступлений, которые в силу степени своей общественной опасности могут считаться достаточно серьезными, чтобы оправдать такое вмешательство [в право на уважение частной и семейной жизни и в право на защиту персональных данных] (параграф 60 Решения от 08.04.2014).

В-третьих, Директива 2006/24/ЕС не устанавливает каких-либо объективных критериев, в соответствии с которыми ограничивается число лиц, имеющих право доступа к сохраненным данным. Прежде всего, указывает Суд, доступ компетентных национальных органов к сохраненным данным не зависит от предварительного одобрения судом или независимым административным органом (параграф 62 Решения от 08.04.2014).

Европейский суд, признавая необходимость в определенных случаях хранения соответствующих данных, пришел к выводу, что Директива 2006/24/ЕС «влечет за собой широкое и особенно серьезное вмешательство в эти основные права [в право на уважение частной и семейной жизни и в право на защиту персональных данных]… без того, чтобы такое вмешательство не было строго ограничено положениями, гарантирующими, что оно возможно только тогда, когда это действительно необходимо» (параграф 65 Решения от 08.04.2014).

Отметим, что признание Директивы 2006/24/ЕС недействительной не повлияло на применение в ряде стран ЕС национального законодательства, принятого для имплементации Директивы 2006/24/ЕС еще в период ее действия.

Уже в 2016 г. Европейский Суд возвратился к вопросу о законности хранения данных пользователей в связи с запросами национальных судов Швеции и Великобритании, перед которыми были поставлены вопросы о соответствии национальных законов в данной области праву ЕС.

Так, законодательство Швеции обязывало провайдеров услуг электронной коммуникации (по тексту Решения от 21.12.2016: «providers of electronic communications services») хранить в течение 6 месяцев данные, указанные в Директиве 2006/24/ЕС. При этом для доступа к соответствующим

данным уполномоченные государственные органы не должны уведомлять провайдера и получать предварительное одобрение суда или независимого административного органа.

Законодательство Великобритании, в свою очередь, обязывало операторов общественной связи (в оригинале: «public telecommunications operator») при поступлении от уполномоченных органов запроса осуществлять хранение указанных соответствующими органами данных о пользователях в течение определенного этими же органами периода (максимум – 12 месяцев). Порядок доступа к соответствующим данным дифференцирован в зависимости от вида уполномоченного органа: одним органам для доступа требуется получение судебного одобрения, другим – нет.

Таким образом, если в законодательстве Великобритании была так или иначе учтена позиция Европейского суда, обозначенная им в Решении от 08.04.2014, то законодательство Швеции, исходя из его изложения в Решении от 21.12.2016, изменениям после 08.04.2014 не подверглось.

В итоге, Суд Европейского Союза, во многом повторив аргументы, которыми руководствовался в Решении от 08.04.2014, посвященному директиве о хранении данных, Решением от 21.12.2016 признал необходимость Директивы 2002/58/ЕС и Хартии Европейского Союза об основных правах толковаться как исключающие возможность закрепления в национальном законодательстве общего и неизбирательного сохранения всех данных о трафике и местоположении всех подписчиков и зарегистрированных пользователей всех средств электронной связи.

Директива 2002/58/ЕС и Хартия Европейского Союза об основных правах должны толковаться как исключающие возможность закрепления в национальном законодательстве возможности доступа компетентных национальных органов к сохраненным данным, когда, в частности, для такого доступа не требуется предварительное одобрение суда или независимого административного органа.

При этом Суд отметил, что статья 15 Директивы 2002/58/ЕС[71] не препятствует принятию государствами-членами ЕС законодательства, разрешающего, в качестве превентивной меры, целевое сохранение данных о трафике и местоположении в целях борьбы с серьезным преступлением, при условии, что такое хранение ограничено категориями сохраняемых данных, средствами связи, лицами и периодом хранения (параграф 108 Решения от 21.12.2016).

С учетом изложенного, представляется, что Россия сейчас находится лишь в самом начале пути поиска баланса между, с одной стороны, правом на конфиденциальность коммуникаций и, с другой стороны, необходимостью борьбы с такими угрозами общественной безопасности как, например, терроризм. Европейский Союз на этом пути уже как минимум 11 лет (если считать с даты принятия Резолюции 2006/24/ЕС) и как показывают упомянутые решения Европейского суда точка в этом вопросе тоже пока не поставлена.

[71] Стоит отметить, что в Решении Суда от 21.12.2016 много внимание уделено именно толкованию данной статьи Директивы 2002/58/ЕС. Толкуя указанные положения, Суд приходит к выводу, что хранение данных является исключением из запрета на хранение данных, приведенного в статье 5 Директивы 2002/58/ЕС, и, следовательно, такое исключение должно быть обоснованным, соразмерным предполагаемой цели, и допускается только на ограниченный период времени.

2.3 Ответственность за нарушение конфиденциальности

а. Законодательство РФ

В связи с увеличением объема собираемых персональных данных, увеличением субъектов, обрабатывающих такие данные, расширением их полномочий, а так же с наличием актов, повышающих требование к таким субъектам, необходимо более полное, строгое и эффективное регулирование ответственности за нарушение законодательства о персональных данных.

Ответственность за нарушение законодательства в сфере защиты персональных данных носит комплексный характер, так, лица, виновные в нарушении требований данного закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность в соответствии со статьёй 24 Федерального закона "О персональных данных".

Дисциплинарная ответственность устанавливается нормами главы 14 Трудового кодекса РФ. Данная глава защищает не только работников от незаконной обработки персональных данных работодателем, но так же и работодателя от некачественного и зачастую противоправного действия работников.

Так работники наделяются правом обжалования в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных, а виновные в нарушениях работники могут получить замечание, выговор или быть уволены. Увольнение по инициативе работодателя возможно за разглашение любой охраняемой законом тайны, в том числе персональных данных другого работника.

Административная ответственность является самым «популярным» видом из всех. Она закреплена в статье 13.11 Кодекса об административных правонарушениях. Со дня принятия КоАП РФ — с 30 декабря 2001 г. — и до 7 февраля 2017 г. формулировка его ст. 13.11 не изменялась. За это время только

лишь Федеральным законом № 116-ФЗ72 были увеличены размеры штрафов. Однако с 1 июля 2017 г. вступают в силу поправки, которые устанавливают вместо одного состава правонарушений в области персональных данных - семь[73].

В последние годы отмечена тенденция роста количества жалоб и обращений субъектов персональных данных (граждан) на незаконные действия операторов, осуществляющих обработку персональных данных с нарушением законодательства Российской Федерации в области персональных данных и, соответственно, количества выявленных нарушений. В пояснительной записке отмечается, что предлагаемые законопроектом составы правонарушений соответствуют тем, которые Роскомнадзор чаще всего выявляет в ходе проверок.

Нововведенные составы являются существенным изменением в структуре и в основании ответственности. Все составы введены в ст. 13.11 КоАП, которая значительно увеличилась по объему, поскольку оснований для ответственности стало существенно больше. Она включает в себя такие правонарушения: обработка персональных данных без письменного согласия субъекта; обработка информации, касающейся личной жизни, здоровья, вероисповедания и т. д.; невыполнение оператором требований к публикации в открытом доступе документа о его политике обработки персональных данных; непредставление оператором субъекту информации об обработке его персональных данных; невыполнение оператором требований субъекта об уточнении, блокировке или уничтожении его персональных данных; ненадлежащее хранение (в том числе при помощи электронных носителей) персональных данных; несоблюдение правил по обезличиванию персональных данных.

[72] Федеральный закон от 22.06.2007 № 116-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части изменения способа выражения денежного взыскания, налагаемого за административное правонарушение» // "Российская газета" от 27 июня 2007 г. N 135

[73] Федеральный закон от 7 февраля 2017 г. N 13-ФЗ "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях" // "Российская газета" от 10 февраля 2017 г. N 30

Помимо увеличения оснований, так же законодатель привносит свои изменения и в систему наказаний, не только расширяя, но и ужесточая ответственность.

В новой редакции ст. 13.11 КоАП РФ[74] существенно увеличены размеры административных штрафов. Максимальные размеры штрафов для всех категорий нарушителей предусмотрены за обработку персональных данных без письменного согласия их субъекта либо обработку персональных данных с нарушением установленных законодательством Российской Федерации в области персональных данных требований к составу сведений, включаемых в согласие.

По ряду правонаруш в праве состав протокол лица

Полномочия по возбуждению дел об административных правонарушениях в области персональных данных переданы от прокуроров должностным лицам Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Согласно введенным поправкам, Роскомнадзор получил полномочия на составление протоколов административных правонарушений (пункт 2 ст. 1 Федерального закона № 13-ФЗ внесены изменения в п. 58 ч. 2 ст. 28.3 КоАП РФ), а прокуратура лишилась подобных полномочий (пункт 3 ст. 1 Федерального закона № 13-ФЗ ст. 13.11 КоАП РФ исключена из ч. 1 ст. 28.4 КоАП РФ).

Гражданская ответственность может наступать независимо от других видов ответственности, применяться совместно с ними. Данное положение закреплено в ст. 24 Федерального закона "О персональных данных": Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, а также нарушением требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется

[74] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. N 195-ФЗ // "Российская газета" от 31 декабря 2001 г. N 256

независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков(ст. 24).

Уголовная ответственность наступает за наиболее тяжкие виды нарушений законодательства о персональных данных, к ним относятся: незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Отягчающим обстоятельством по данному виду нарушений признается данное правонарушение, совершенное с использованием своего служебного положения (ст.137 УК РФ); неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети (ст.272 УК РФ); оказание услуг по технической защите информации при отсутствии соответствующей лицензии, либо осуществление деятельности с нарушением лицензионных требований и условий, если это деяние причинило крупный ущерб гражданам, организациям или государству, либо сопряжено с извлечением дохода в крупном размере (более 1 500 тыс. руб.). Отягчающим признаком признается совершение преступления организованной группой лиц, либо сопряженное с извлечением дохода в особо крупном размере (более 6 000 тыс. руб.).[75]

При толковании данного положения мы приходим к выводу, что помимо морального вреда возможно возмещение имущественного вреда или понесенных убытков, что более детально регулируется гражданским законодательством.

При анализе вышеуказанных положений можем отметить тенденция в усиления ответственности, ужесточения санкций, ведения новых видов правонарушений и расширения полномочий надзорных органов, что указывает

[75] Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ // «Собрание законодательства РФ» от 17 июня 1996 г. N 25 ст. 2954

на понимание законодателем важности более эффективной защиты персональных данных.

Поскольку ответственность является одним из главных стимулов для исполнения законодательства, то закрепление ее основ выходит за рамки внутригосударственного права и основные права и обязанности регулируются межгосударственными актами, договорами, актами международных организаций.

b. Законодательство Германии и Европейского союза.

Несмотря на то, что привлечение к ответственности входит в компетенцию государства, положения об ответственности закрепляются и на уровне региональных организаций.

Примером может послужить законодательство Европейского Союза. Так, Директива 95/46/ЕС устанавливает основные права субъектов персональных граждан, а так же обязанность государств-участников урегулировать во внутреннем праве вопросы ответственности за нарушение законодательства о персональных данных. Основными закрепленными принципами являются: право любого лица на судебную защиту от любого нарушения прав, гарантированных ему национальным законодательством, применимым к осуществляемой обработке; право получить компенсацию от оператора за понесенный ущерб имеет любое лицо, которое понесло ущерб в результате неправомерной операции по обработке или какого-либо действия, несовместимого с национальными нормами, принятыми в соответствии с настоящей Директивой; обязанность государств-участниц в принятии надлежащих мер для обеспечения полного осуществления норм настоящей Директивы и, в частности, установлении санкций, налагаемых в случае нарушения норм, принятых в соответствии с настоящей Директивой[76].

В немецком праве гражданско-правовая ответственность так же может применяться независимо от применения или неприменения других видов

[76] Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24.10.1995 г. «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // N L 281, 23.11.1995 г., стр. 31

ответственности. В целом процедура и основания применения данного вида ответственности схожа с российским аналогом, однако в немецком праве имеется ряд интересных правил, которые, по нашему мнению, ограничивают возможность полноценного возмещения ущерба. Такими ограничениями являются: иск о возмещении ущерба может подать лишь физическое лицо, так же оно должно действовать само заинтересованное лицо; ограничивается максимальная сумма иска в размере 130 тыс. евро (в российском законодательстве такие ограничения отсутствуют).[77]

По особенностям и отличиям от российского законодательства применения административной и уголовной ответственности можно отметить, что часть диспозиций, нарушающих защиту персональных данных находится непосредственно в Федеральном Законе Германии «О персональных данных».

Так же отличается и материальный состав правонарушений, например в Германии имеются такие составы, как: нарушение обязанности назначить сотрудника, ответственного за защиту персональных данных; нарушение в информировании заинтересованных лиц в использовании их данных в рекламных целях или в торговле; нарушение процедуры обработки информации; нарушение при выдаче информации субъектам персональных данных.[78]

Противоправные действия, нарушающие законодательство о персональных данных с целью получения материальной выгоды или причинения вреда другому лицу, влекут за собой уже уголовную ответственность.

Примечательным фактом является, что, в отличии от российского права, законодательство Германии устанавливает составы преступлений, относящихся не только к публичному обвинению, но и к частному. Условия применения

[77] См.: Haftung und Sanktionen bei Datenschutzverstößen – Schadensersatz und Schmerzensgeld, режим доступа: http://www.it-rechtsanwalt.com/datenschutz/haftung-und-sanktionen-bei-datenschutzverstoessen-schadensersatz-und-schmerzensgeld-3601.php (дата обращения: 07.05.2017)

[78] См.: Haftung und Sanktionen bei Datenschutzverstößen – Ordnungswidrigkeitstatbestände und Bußgelder, режим доступа: http://www.it-rechtsanwalt.com/datenschutz/haftung-und-sanktionen-bei-datenschutzverstoessen-ordnungswidrigkeitstatbestaende-und-bussgelder-3590.php (дата обращения: 08.05.2017)

санкций за такие правонарушения, как и возможность возбуждения уголовного дела, зависят только от наличия заявления заинтересованного лица.

В немецком праве уголовная ответственность за попытку совершения и подготовку к совершению преступления наступает только тогда, когда это напрямую указано в законе. В связи с этим применение уголовной ответственности за попытку или подготовку преступления, нарушающего федеральное законодательство в сфере защиты персональных данных, является отчасти ограниченным. Думается, что для более эффективного действия законодательства в указанной сфере необходимо пресекать преступления и наказывать за данные действия/бездействия не по факту их совершения, а на стадии подготовки или попытки, дабы не допускать ущемления конституционных прав человека и гражданина.[79]

При изучении ответственности за нарушения положений о защите персональных данных можно выделить тенденцию на расширение составов преступлений и правонарушений. Такой процесс нельзя считать завершенным и окончательным, пока не снизится количество нарушений до минимума, и пока не будет найден баланс между конституционными и основополагающими правами и свободами человека и уровнем вмешательства в частную и личную жизнь, необходимую для осуществления всеобщей безопасности.

[79] См.: Haftung und Sanktionen bei Datenschutzverstößen – Straftatbestände und Strafen, режим доступа: http://www.it-rechtsanwalt.com/datenschutz/haftung-und-sanktionen-bei-datenschutzverstoessen-straftatbestaende-und-strafen-3598.php (дата обращения: 08.05.2017)

ЗАКЛЮЧЕНИЕ

Исходя из вышеизложенного, автор пришел к следующим выводам. Персональные данные защищаются правовыми нормами на международном и национальном уровне. Способы охраны в мире в целом совпадают, имея, однако, свои особенности. В ходе работы удалось определить специфику основных способов защиты персональных данных в РФ, Германии и ЕС, их преимущества и недостатки для субъектов и операторов.

1. В России в связи с недавним появлением и относительно небольшим временем применения нормы, касающиеся вопросов регулирования конфиденциальной информации персонального характера, не систематизированы и содержатся только в нескольких федеральных законах. Большое количество подзаконных и локальных внутренних актах правоприменительных органов затрудняет использование и исполнение всех предписаний. Их наличие, к сожалению, не решает тех проблем в рассматриваемой сфере, так как нормы носят общий, декларативный характер. Нам представляется необходимым дальнейшая конкретизация, с последующей систематизацией, и в итоге кодификация норм, регулирующих правовое положение персональных данных.

В Германии законодательство о персональных данных является более полным, структурированным и систематизированным, поскольку он включает в себя не только основные принципы, условия и требования защиты персональных данных, но включает в себя еще и ответственность.

Отметим тенденцию все к большей унификации правовых актов, их все большему соответствию международным нормам. В целях глобализации, наиболее тесного сотрудничества государств, а главное, в целях наиболее эффективной защиты персональных данных государствам необходимо иметь одинаково развитую законодательную базу, поскольку в мире все больше и больше появляется трансконтинентальных корпораций, повышается мобильность людей и уровень технического оснащения, которые приводит к распространению персональных данных далеко за пределы границ одного государства.

2. В постоянном процессе совершенствования законодательства и правоприменения государства создают такие правовые акты, исполнение которых представляется довольно сложной процедурой. Кроме того это затратно в плане временных и материальных ресурсов. При том никаких субсидий государство не предоставляет. Речь идет о территориальном ограничении Российской Федерацией операторов персональных данных, а именно: запись, систематизация, накопление, хранение, уточнение (обновление, изменение) и извлечение персональных данных граждан Российской Федерации разрешено только на территории Российской Федерации.

Данные законодательные нормы подводят к затруднительному положению организации, которые не способны перенести хранение и остальные вышеуказанные действия на территорию РФ, что приводит к нарушению законодательства.

В противовес российскому законодательству, законодательство Германии не создает необходимости производить определенные действия исключительно на территории ФРГ, а указывает на необходимость руководствоваться только принципом адекватной защиты. Думается, что подобная юридико-правовая форма является более эффективной. Мы предлагаем включить подобное положение в законодательство Российской Федерации.

3. Постоянные споры о необходимости выявления консенсуса между основными правами и свободами человека и их ограничением с целью защиты общественного строя и порядка вспыхнули с новой силой в Германии в октябре 2015 года, в связи с принятием положений, об обязанности хранения операторами связи, провайдерами и интернет-ресурсами данных трафика пользователя, а именно мета-данных. Еще большая волна возмущения прокатилась по России в связи с принятием поправок от 6 июля 2016 года, поскольку операторов обязали собирать не только мета-данные, но и само содержание коммуникаций между пользователями.

При анализе положений национального и международного права в совокупности с судебной практикой Европейского Союза, мы пришли к

выводу, что форма ограничения конституционных прав в РФ не соответствует принципу пропорциональности. В европейском праве более «мягкую» директиву признали не соответствующей основным международным правам человека и были вынуждены отменить. Думается, что по истечение времени то же самое произойдет и с российским законом, внесшим такие ограничения. Единственным условием, при котором указанный акт не будет отменен, является приведение его в соответствие с международным правом и Конституцией РФ. Примером может послужить правовой акт принятый в Германии поскольку процедура раскрытия персональных данных более регламентирована, а так же установлены очень короткие сроки хранения и значительно уменьшен объем хранимых данных.

4. Основным недостатком существующей юридической ответственности за нарушение норм о персональных данных является отсутствие взаимосвязанности между различными сферами оборота персональных данных. Однако в связи с расширением полномочий государства и операторов в области сбора и обработки персональных данных, доступа к ним и расширение возможностей распространения, а также наличия пробелов законодатель расширяет список правонарушений, вводит новые санкции, а так же увеличивает размеры и сроки наказания.

При анализе вышеуказанных положений отметим тенденцию усиления ответственности, ужесточения санкций, ведения новых видов правонарушений и расширения полномочий надзорных органов, что указывает на понимание законодателем важности более эффективной защиты персональных данных

Одним из последних таких изменений являются поправки в ст.13.11 КоАП РФ, в результате которых количество санкций значительно увеличилось, а следовательно, увеличилось количество сфер, урегулированных законодателем.

Право Европейского союза и Германии прошло более длительный путь развития. Система санкций и порядок применения ответственности являются более продуманными и систематизированными. Вместе с тем постоянное изменение базового законодательства в области охраны персональных данных в

Германии влечет необходимость расширения и добавления новых видов противоправных деяний.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Международные акты

1. Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10.12.1948 г.) [Электронный ресурс] - Режим доступа: http://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (дата обращения: 15.04.17).

2. Директива Европейского Парламента и Совета Европейского Союза 2002/22/ЕС от 7.03.2002 г. об универсальных услугах и правах пользователей в отношении сетей электронных коммуникаций и услуг [Электронный ресурс] – Режим доступа: https://pd.rkn.gov.ru/law/ (дата обращения: 19.04.17).

3. Директива Европейского Парламента и Совета Европейского Союза 2002/58/ЕС от 12.07.2002 г. «в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи» // N L 201, 31.07.2002, с. 37

4. Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24.10.1995 г. «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // N L 281, 23.11.1995, ст. 31

5. Договор между Российской Федерацией и Соединенными Штатами Америки об избежании двойного налогообложения и предотвращении уклонения от налогообложения в отношении налогов на доходы и капитал, 17.06.1992 [Электронный ресурс] - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_3575/ (дата обращения: 19.04.17).

6. Дополнительный протокол к Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера, о наблюдательных органах и трансграничной передаче информации ETS N 181 от 08.11.2001 г. [Электронный ресурс] – Режим доступа: https://pd.rkn.gov.ru/law/ (дата обращения: 19.04.17).

7. Конвенция о защите прав человека и основных свобод ETS N 005 от 04.11.1950 г. (ред. от 11.06.1994г.) [Электронный ресурс] – Режим доступа: http://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/005 (дата обращения: 19.04.17).

8. Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981 г. (ред. от 15.06.1999 г.) // СЗ РФ 2014 г. N 5 ст. 419

9. Модельный закон «О персональных данных» (принят постановлением на четырнадцатом пленарном заседании Межпарламентской ассамблеи государств - участников СНГ от 16.10.1999 г. N 14-19) // Информационная бюллетень Межпарламентской Ассамблеи государств-участников СНГ. 2000. N 23

Нормативно-правовые акты Российской Федерации

1. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 г. N 195-ФЗ // Российская газета 2001, N 256

2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ) // СЗ РФ 2009, № 4, ст. 851

3. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 01.05.2017) // Российская газета 2001, N 256

4. Уголовный кодекс Российской Федерации от 13.06.1996 г. N 63-ФЗ // СЗ РФ 1996, N 25, ст. 2954

5. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 22.02.2017) «О персональных данных» // Российская газета 2006, № 4131

6. Федеральный закон от 20.02.1995 N 24-ФЗ «Об информации, информатизации и защите информации» // СЗ РФ, 1995, № 8, ст. 609. (утратил силу)

7. Федеральный закон от 07.08.2001 г. №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем» // Российская газета 2001, N 151

8. Федеральный закон от 01.04.1996 г. №27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» // Российская газета 1996, N 68

9. Федеральный закон от 21.07.2014 г. N 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» // Российская газета 2014, N 163

10. Федеральный закон от 06.07.2016 г. N 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Российская газета 2016, N 149

11. Федеральный закон от 22.06.2007 № 116-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях в части изменения способа выражения денежного взыскания, налагаемого за административное правонарушение» // Российская газета 2007, N 135

12. Федеральный закон от 7.02.2017 г. N 13-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // Российская газета 2017, N 30

13. Указ Президента РФ от 06.03.1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера» // СЗ РФ 1997, N 10, ст. 1127

Нормативно-правовые акты Германии

14. Außenwirtschaftsgesetz // 28. April 1961 (BGBl. I S. 481, 495)

15. Bundesdatenschutzgesetz // 20. Dezember 1990, BGBl. I S. 2954, 2955.

16. Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet // 30. Juli 2004 (BGBl. I S. 1950)

17. Gesetz über den Verkehr mit Betäubungsmitteln // 1. März 1994 (BGBl. I S. 358)

18. Gesetz zur Überwachung des Verkehrs mit Grundstoffen, die für die unerlaubte Herstellung von Betäubungsmitteln missbraucht werden können // 7. Oktober 1994 (BGBl. I S. 2835)

19. Strafgesetzbuch // 13. November 1998 (BGBl. I S. 3322)

20. Strafprozessordnung // 7. April 1987 (BGBl. I S. 1074, ber. S. 1319)

21. Telekommunikationsgesetz // 25. Juli 1996 BGBl. I S. 1120

Научная литература

Российская научная литература

22. Алексеева Е.В. Гарантии защиты персональных данных работника в современном российском законодательстве / К познанию права. 2008, № 3. С. 42-48.

23. Богатыренко З.С. Новейшие тенденции защиты персональных данных работника в российском трудовом праве / Трудовое право. 2006. № 10. С. 29-51.

24. Борисова С.А. Общие требования при обработке персональных данных работника и гарантии их защиты / Трудовое право. 2005. № 11. С. 30-36.

25. Бундин М.В. Неприкосновенность частной жизни и защита персональных данных / Инновации в государстве и праве России. 2007, № 1. С. 277-284.

26. Важорова М.А. Проблемы совершенствования системы обеспечения защиты персональных данных / Актуальные вопросы российского права и проблемы правоприменения в условиях современности. 2009. №1. С. 38-40.

27. Вельдер И.А. Практика защиты персональных данных в странах Европейского Союза: роль национальных административных и судебных органов / Интеллектуальная собственность и ее исследователь. 2005. №3. С. 171-178.

28. Веселова А.Б. Защита персональных данных работников / Трудовые споры. 2006, № 10. С. 33-46.

29. Ветров Д.М. Защита персональных данных и защита информации на предприятии. Некоторые спорные вопросы применения / Проблемы права. 2010, № 1. С. 114-121.

30. Волчинская Е.К., Дятленко В.В. Законодательство о защите персональных данных: проблемы и решения / Информационное право. 2006, № 1 (4). С. 11-16.

31. Выскребцев Б.С. Проблема реализации права работника на защиту персональных данных / Проблемы современного российского права. 2010. №6 С. 69-71.

32. Гаврюшина Н.И. Проблемы правовой защиты персональных данных / Актуальные вопросы современного российского права. 2010. № 1. С. 158-161.

33. Ганижев А.Я. Формирование информационного права и его влияние на защиту персональных данных работника / Эффективность правового регулирования общественных отношений в России. 2007. №2. С. 120-122.

34. Горев А.И. Защита прав субъектов персональных данных в информационном обществе / Международные юридические чтения. 2007, № 2. С. 117-122.

35. Гришина Е.П., Саушкин С.А. Перспективы формирования организационно-правового режима защиты персональных данных на основе международных стандартов в деятельности кадровых служб органов федеральной таможенной службы / Теоретические и практические аспекты таможенного регулирования на единой таможенной территории таможенного союза. 2009. №1. С. 131-135.

36. Гуляева Е.Е. Международно-правовые проблемы защиты персональных данных / Актуальные проблемы современного международного права. 2008. №2. С. 110-117.

37. Долгов А.С. Правовая защита персональных данных работника / Научные записки НГУЭУ. 2005. № 3. - С. 83-85.

38. Долгов А.С. Правовая защита персональных данных работника / Современные проблемы юридической науки. 2005. № 5. - С. 181-183.

39. Еремин А.Р., Федосин А.С. К вопросу государственной защиты права на неприкосновенность частной жизни в процессе автоматизированной обработки персональных данных граждан РФ / Право и общество. 2009. №1. С. 64-69.

40. Зайцева Л.В. Юридическая ответственность в области защиты персональных данных работников / Вестник НГУ. 2006. № 2. С. 84-87.

41. Идрисов И.Д. Правовое регулирование защиты и обработки персональных данных в электронной коммерции / Актуальные проблемы юридической науки и правоприменительной практики. 2008. № 1. С. 180-184.

42. Кадацкая Т.А. Защита персональных данных как одна из составляющих информационной безопасности граждан / Современный мир: безопасность и права человека. 2006. №2. С. 135-139.

43. Крушина А.С. Право на защиту персональных данных / Современные проблемы юридической науки. 2009. № 1. С. 289-290.

44. Куфтин Н.Н. Защита персональных данных как составная часть развития законодательства в информационной сфере / "Черные дыры" в Российском Законодательстве. 2007. № 5. С. 491-492.

45. Лебедева М.М. Актуальные вопросы защиты персональных данных / Право: теория и практика. 2008. № 4 (105). С. 18-20.

46. Лушников А.М. Защита персональных данных работника: сравнительно-правовой анализ / Актуальные проблемы совершенствования российского законодательства и правоприменения. 2009. №2. С. 100-108.

47. Лушников А.М. Защита персональных данных работника: сравнительно-правовой комментарий гл. 14 ТК РФ / Трудовое право. 2009. № 10 (116). С. 77-82.

48. Лютов Н.Л. Защита персональных данных: международные стандарты и внутреннее российское законодательство / Трудовое право. 2010. № 8 (126). С. 15-32.

49. Маркевич А.С. Организационная основа защиты персональных данных работника на легальном уровне / Международная научно-практическая конференция "Преступность в России: состояние, проблемы предупреждения и раскрытия преступлений". 2008. № 1. С. 248-251.

50. Михалусь А.Ф. Защита персональных данных работника / Наука и образование. 2006. № 3. С. 318-320.

51. Пилипенко С.Г., Федосин А.С. К вопросу о реализации права на защиту персональных данных при их обработке в электронной форме / Пробелы в российском законодательстве. 2009. № 3. С. 213-215.

52. Пилипенко С.Г., Федосин С.А. К вопросу о защите права на неприкосновенность частной жизни при обработке персональных данных / Актуальные проблемы современного государства и права. 2009. №7. С. 69-75.

53. Проблемы правовой защиты конфиденциальности персональных данных несовершеннолетних: вопросы теории и практики. Монография / Покаместова Е.Ю.; Под науч. ред.: Гаврилов С.Т. - Воронеж: Изд-во Воронеж. ин-та МВД России. 2008. - 146 с.

54. Просвирнин Ю.Г. Защита персональных данных / Вестник Воронежского государственного университета. 2008. № 2 (5). С. 174-188.

55. Прытков Ю. Правовое регулирование общественных отношений в сфере защиты персональных данных на территории РФ / Актуальные проблемы правовой теории и практики. 2007. № 1. С. 186-191.

56. Руденко Г.В. Правовые основы защиты персональных данных в ходе сотрудничества государств в уголовно-правовой сфере в рамках Европейского Союза / Актуальные проблемы международно-правового сотрудничества в сфере борьбы с преступностью. 2010. №1. С. 163-166.

57. Садикова И.С. Конституционно-правовые основы защиты персональных данных / Закон и право. 2009. № 12. С. 50-51.

58. Сдобнов Д.А. Защита персональных данных работника: необходимость совершенствования правового регулирования / Актуальные проблемы реформирования современного законодательства Российской Федерации. 2010. №2. С. 374-375.

59. Стефанишин С.С., Шпакова А.Л. Основания и порядок защиты персональных данных работников / Трудовые споры. 2006, № 3. С. 3-7.

60. Фахертдинова Г.Р. Защита персональных данных работника / Актуальные проблемы реформирования современного законодательства Российской Федерации. 2010. № 1. С. 377-378.

61. Хачатурян Ю. Право работника на защиту персональных данных: недостатки механизма реализации / Трудовое право. 2005. № 3. С. 77-84.

62. Хачатурян Ю.А. Право работника на защиту персональных данных / Современное право. 2006, № 1. С. 43-51.

63. Цадыкова Э.А. Гарантии охраны и защиты персональных данных человека и гражданина / Конституционное и муниципальное право 2007. № 14. С. 15-18.

64. Челнокова Г.Б. Проблемы защиты персональных данных в рамках трудовых отношений // Право и государство: теория и практика. 2007. № 9. - С. 65-70

65. Шишлов А.А. Правовое регулирование защиты персональных данных в рамках Европейского Союза // Закон и право. 2010. № 1. С. 32-33.

Практика судов иностранных государств

66. BVerfG, Urteil vom 02. März 2010 - 1 BvR 256/08 - Rn. (1-345) [Электронный ресурс] – Режим доступа: http://law.justia.com/cases/federal/appellate-courts/F2/24/365/1496726/ (дата обращения: 12.04.17).

67. № C-293/12 и C-594/12 [Электронный ресурс] – режим доступа: http://curia.europa.eu/juris/liste.jsf?num=C-293/12# (дата обращения – 29.03.2017).

Иные электронные ресурсы

Русскоязычные электронные ресурсы

68. Защита прав субъектов персональных данных [Электронный ресурс] – режим доступа: https://rkn.gov.ru/treatments/p459/p468/ (дата обращения: 25.04.2017)

Иностранные электронные ресурсы

69. Haftung und Sanktionen bei Datenschutzverstößen – Ordnungswidrigkeitstatbestände und Bußgelder [Электронный ресурс] – режим доступа: http://www.it-rechtsanwalt.com/datenschutz/haftung-und-sanktionen-bei-datenschutzverstoessen-ordnungswidrigkeitstatbestaende-und-bussgelder-3590.php (дата обращения: 08.05.2017)

70. Haftung und Sanktionen bei Datenschutzverstößen – Schadensersatz und Schmerzensgeld [Электронный ресурс] – режим доступа: http://www.it-rechtsanwalt.com/datenschutz/haftung-und-sanktionen-bei-datenschutzverstoessen-schadensersatz-und-schmerzensgeld-3601.php (дата обращения: 07.05.2017)

71. Haftung und Sanktionen bei Datenschutzverstößen – Straftatbestände und Strafen [Электронный ресурс] – режим доступа: http://www.it-rechtsanwalt.com/datenschutz/haftung-und-sanktionen-bei-datenschutzverstoessen-straftatbestaende-und-strafen-3598.php (дата обращения: 08.05.2017)