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

Кафедра «Конституционное и административное право»
(наименование)

40.04.01 Юриспруденция
(код и наименование направления подготовки)

Правовое обеспечение государственного управления и местного самоуправления
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему «**Защита персональных данных в праве России: конституционно-правовой аспект**»

Студент Бродская Э.Г. _____
(И.О. Фамилия) (личная подпись)

Научный руководитель к.ю.н., доцент А.Н. Станкин
(ученая степень, звание, И.О. Фамилия)

Тольятти 2020

Оглавление

Введение.....3
Глава 1. Теоретические основы персональных данных как предмета защиты конституционных прав в России.....7
1.1. Понятие и сущность персональных данных.....7
1.2. Конституционно-правовые аспекты защиты персональных данных.....13
Глава 2. Анализ методов конституционно-правовой защиты персональных данных.....22
2.1. Основные требования к доступу, хранению и передаче персональных данных.....22
2.2. Основания и процедура раскрытия персональных данных.....30
Глава 3. Пути совершенствования конституционно-правовой защиты персональных данных.....39
3.1. Основные проблемы конституционно-правовой защиты персональных данных.....39
3.2. Пути решения проблем в сфере конституционно-правовой защиты персональных данных.....51
Заключение.....60
Список используемой литературы.....63

Введение

Освоение персональных данных, в зависимости от субъективной точки зрения, можно отнести как к одному из величайших достижений человечества, так и к одной из самых больших проблем. Безусловно, начало использования персональных данных дало возможность компаниям предлагать новые решения, построенные на основе индивидуальных предпочтений потребителя, а ему – получать новый персонализированный продукт, наиболее подходящим образом удовлетворяющий желаниям.

Тем не менее использование персональных данных открывает компаниям новые возможности по воздействию и контролю над конкурентной ситуацией на рынке, ставит под угрозу тайну личной жизни и равенство людей. Стремительное развитие цифровой экономики в сочетании с низким уровнем расходов на внедрение инновационных продуктов влечет постоянное отставание государственного регулирования от экономических реалий. При этом объем данных, обрабатываемых в мировом масштабе, растет колоссальными темпами.

Вопросы правового регулирования персональных данных сегодня – одна из важнейших дискуссионных тем не только в России, но и в мировом юридическом сообществе. Несмотря на то что регулирование персональных данных на первый взгляд кажется узкоспециализированной частью государственного управления, их колоссальное экономическое влияние, прежде всего – на самые быстрорастущие секторы экономики, а также специфический характер, уже показали необходимость быстрого реагирования. Правовой аспект персональных данных, в отличие от, например, морального, изучен крайне мало: исследований, проведенных в данных сфере, в особенности в России, недостаточно для формирования многостороннего правового подхода к урегулированию их правомерного использования.

Таким образом, в современном мире вопрос конституционно-правовой защиты персональных данных особенно актуален.

Под персональными данными понимают любую информацию об определенном или поддающемся определению физическом лице. Правовое регулирование данного вопроса осуществляется множеством международных актов, а также Конституцией РФ, федеральными законами и подзаконными актами, что свидетельствует о стремлении государства в лице уполномоченных органов максимально регламентировать операции с персональными данными в целях их надежной охраны.

Современное законодательство достаточно полно регламентирует порядок сбора, обработки, хранения, передачи и использования персональных данных. За нарушение этих требований лицо может быть привлечено к материальной, дисциплинарной, административной, и даже уголовной ответственности.

Конечно, как и законодательство в любой другой сфере, нормы, касающиеся персональных данных не совершенны. Особенную сложность для регулирования представляет то обстоятельство, что технические возможности непреклонно возрастают, и успеть за этим прогрессом законодателю достаточно затруднительно. И тем не менее, на наш взгляд, в настоящее время, сделано максимально возможное для защиты персональных данных.

Несмотря на довольно большое количество авторов, занимающихся проблематикой защиты персональных данных (Алексеева Е.В., Богатыренко З.С., Бундин М.В., Важорова М.А., Вельдер И.А., Веселова А.Б., Ветров Д.М., Волчинская Е.К., Дятленко В.В., Выскребцев Б.С., Гаврюшина Н.И., Ганижев А.Я., Горев А.И., Гуляева Е.Е., Еремин А.Р., Федосин А.С., Зайцева Л.В., Идрисов И.Д., Кадацкая Т.А., Крушина А.С., Маркевич А.С., Пилипенко С.Г. и другие), их работы преимущественно посвящены характеристикам различных видов информационных процессов, ресурсов и технологий, обеспечению государственной и иных видов тайн и т.д.

Материалы трудов многих из перечисленных авторов будут использованы в данной работе.

Объектом исследования являются общественные отношения, возникающие в сфере конституционно-правовой защиты персональных данных, а также правоприменительная практика.

Предметом исследования являются международные правовые нормы и нормы законодательства Российской Федерации в сфере правовой охраны персональных данных.

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

Задачи исследования. Для достижения указанных целей были сформулированы следующие задачи:

1. Изучить понятие и сущность персональных данных;

2. Рассмотреть правовые аспекты персональных данных;

3. Раскрыть основные требования к доступу, хранению и передаче персональных данных;

4. Изучить основания и процедуру раскрытия персональных данных;

5. Определить основные проблемы конституционно-правовой защиты персональных данных;

6. Выявить пути решения проблем в сфере конституционно-правовой защиты персональных данных.

Методология исследования. Методологическую основу 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.

Теоретическую основу исследования составили работы по общей теории права, а также современные достижения науки конституционного, трудового, гражданского, административного, уголовного, международного права.

Нормативной базой работы являются международные правовые акты, отечественное законодательство, указы Президента, постановления Правительства, ведомственные акты.

Научная новизна исследования состоит в том, что автором впервые предпринята попытка обобщения имеющегося опыта в сфере конституционно-правовой защиты 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 конституционно-правовой защиты персональных данных.

Структура работы определяется ее целью и принятым подходом к решению поставленных задач. Работа состоит из введения, трех глав, разделенных на параграфы, заключения, а также списка использованной литературы.

Глава 1. Теоретические основы персональных данных как предмета защиты конституционных прав в России

1.1. Понятие и сущность 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.

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-участниц стали появляться внутригосударственные отраслевые законы по регулированию правового положения персональных данных, а также принципы и условия их обработки.

«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» [14, с. 64].

Согласно исследованию Гуляевой Е.Е., «под персональными данными понимается конкретная информация о личных или материальных обстоятельствах идентифицированного или идентифицируемого физического

лица. 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» [13].

По мнению Гаврюшиной Н.И., российское 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 также на уровне международных актов. Это обусловлено необходимостью выделения составных частей персональных данных для более полного и конкретного регулирования в различных областях применения [10].

Изучив определения разных авторов и сравнив законодательное определение персональных данных, можно выделить ряд обязательных черт, им присущих, подпадающих под охрану законодательства:

«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» [20, с. 213].

В научной 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, распространяться только на этот специальный случай, 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.

Принцип целевого назначения распространяется 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.

Соотношению «правило-исключение» следует принцип прозрачности. «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» [11].

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»). 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.

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» [62].

К тому же при автоматизированной обработке персональных данных необходимо выбрать или разработать такие критерии, которые определяют наличие только такого ограниченного количества персональных данных, которое необходимо 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.

«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 на 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, который 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» [61].

Однако нельзя рассматривать систему законодательства анализируя только специальные нормативно-правовые акты, необходимо использовать комплексный подход. Основой внутригосударственной нормативно-правовой базы является Конституция.

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.

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.

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. Часть таких актов носит рекомендательный характер.

Так, например, Просветовой О.Б. было предложено определение автоматической обработки персональных данных, впоследствии нашедшее закрепление в федеральном законодательстве. Анализируя комплекс актов, можно отметить тенденцию все к большей унификации, и все большему соответствию законодательства Российской Федерации международным нормам, в целях эффективной защиты персональных данных.

Таким образом, 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 и аргументирование необходимости правового закрепления защиты таких данных. Научные труды являются вектором развития законодательства и правоприменения в будущем.

1.2. Конституционно-правовые аспекты защиты персональных данных

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

«Перечень сведений конфиденциального характера впервые появился в Указе Президента РФ от 06.03.1997 № 188. Согласно ему, персональные данные включают в себя сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность» [24].

Позднее, ст. 2 «Модельного закона о персональных данных» 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» [9].

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 также 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»).

На сегодняшний момент в регулировании отношений в сфере персональных данных системообразующими актами являются Федеральный закон «О защите персональных данных» от 27 июля 2006 г. № 152-ФЗ и Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В 2017 г. в Российской Федерации была принята Программа «Цифровая экономика», направленная на развитие инновационного потенциала страны. Персональные данные стоят на первом месте в качестве «сквозных технологий», то есть в качестве прорывных цифровых технологий. Более того, персональные данные упоминались в принятой в 2013 г. Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 гг. Однако ни в Программе «Цифровой экономики», ни в Стратегии не говорится о том, что представляют из себя персональные данные.

Так, ФЗ о Персональных данных (ст. 3) вводит это понятие как любой информации, относящейся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Однако принятые 6 июля 2016 г. Федеральный закон «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» № 374-ФЗ, а также Федеральный закон № 375-ФЗ (далее – «Пакет Яровой») обязывают операторов связи и организаторов распространения информации хранить не только персональные данные, но и метаданные, передаваемые пользователями. Таким образом, Пакет Яровой в большой мере распространяется на метаданные данные, в то время как ФЗ о Персональных данных – лишь отчасти.

Статья 11 ФЗ № 152 определяет биометрические персональные данные как сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность, а также используются оператором для установления личности субъекта персональных данных.

«Биометрические данные характеризуются особенной чувствительностью, так как они неразрывно связаны с носителем, поэтому законодатель устанавливает особое требование для их защиты. Если по общему правилу согласие на обработку персональных данных может быть дано в любой позволяющей подтвердить факт его получения форме, то для обработки биометрических данных используется императивная норма об обязательном письменном согласии субъекта» [18].

На практике часто возникает вопрос о том, какую именно информацию можно отнести к биометрической. В связи с этим Роскомнадзор в августе 2013 года опубликовал на своем официальном сайте разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки, в которых поясняет, что к «биометрическим данным относятся физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта».

В выпущенном в 2015 году научно-правовом комментарии к Закону № № 152-ФЗ «Роскомнадзор меняет свою позицию на противоположную в части отнесения фото- и видеоизображений к биометрической информации из-за того, что при визуальной оценке фотография или видеоизображение человека, который является близнецом или чье внешнее сходство с определяемым человеком очевидно, а также в случае осуществления

пластических операций, не позволит произвести достоверную идентификацию субъекта.

Таким образом, можно сделать вывод, что обработкой по-настоящему биометрических персональных данных занимаются только те работодатели, которые в виду секретности своей деятельности организуют сложную проходную систему на территорию организации, включающую, например, сканирование сетчатки глаза или считывающую отпечаток пальца для определения личности конкретного работника» [13].

«Кроме того, Федеральный закон от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» устанавливает довольно широкий перечень, работников, подлежащих обязательной дактилоскопической регистрации: военнослужащие, граждане РФ, проходящие службу в органах внутренних дел, органах государственной налоговой службы, органах по делам гражданской обороны, органах и подразделениях службы судебных приставов, таможенных органах, Государственной противопожарной службе и другие» [18].

На наш взгляд, отсутствие единообразного толкования термина биометрические данные, а соответственно, и понимания того, какие данные о человеке могут считаться биометрическими, является актуальной проблемой, которую предстоит решить на законодательном уровне.

Отдельно стоит сказать о видах обработки персональных данных – как уже было сказано, их два: автоматизированная обработка персональных данных и обработка персональных данных без использования средств автоматизации.

Определение автоматизированной обработки содержится в Законе о персональных данных, как обработки персональных данных с помощью средств вычислительной техники (пункт 4 статья 1 Закона № 152-ФЗ).

Обработка без использования средств автоматизации регламентирована постановлением Правительства РФ от 15.09.2008 № 687 “Об утверждении Положения об особенностях обработки персональных данных,

осуществляемой без использования средств автоматизации” (далее - Постановление № 687).

«На основании указанного Постановления обработкой персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Кроме того, настоящее определение неавтоматизированной обработки персональных данных вступает в противоречие с установленным в 152-ФЗ определением автоматизированной обработки. Исходя из принципа верховенства норм, можно сделать вывод, что в скором времени законодатель должен исправить такое несоответствие» [23].

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

Федеральный закон от 07.08.2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем. и финансированию терроризма» (далее Закон № 115-ФЗ) к персональным данным относит сведения о документе, удостоверяющем личность, адрес места жительства или пребывания личности.

В Федеральном законе от 01.04.1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» (далее Закон № 27-ФЗ) под персональными данными понимаются сведения, содержащиеся в индивидуальных лицевых счетах застрахованных лиц.

Основу конституционно-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» [9].

«Режим конфиденциальности персональных данных снимается в случаях обезличивания персональных данных, требований субъекта в отношении своих персональных данных, не противоречащих национальному законодательству и включения персональных данных в общедоступные базы данных» [9]. Правовой режим персональных данных невозможно рассматривать отдельно от защиты таких 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».

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» [13, с. 110].

Стоит также обратить внимание, что в законе уделено мало внимания вопросам, касающимся обработки персональных данных в информационных системах. Помимо специализированного закона, практическое значение имеют правила и требования в иных отраслевых федеральных законах, где на общие принципы и условия работы с персональными данными накладывается специфика регулирования именно такой отрасли права.

В этой сфере довольно много подзаконных 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.

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. Часть таких актов носит рекомендательный характер.

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

Анализ законодательства позволяет сделать вывод о том, что сбор и обезличивание, хоть и относятся к обработке персональных данных, имеют существенные отличия в части порядка их регулирования.

Кроме перечисленных основных источников регулирования сферы защиты персональных данных, имеется большое количество подзаконных актов, регулирующих отдельные стороны данного вопроса, заострять внимание на которых не представляется необходимым.

Таким образом, если те или иные сведения подпадают под понятие персональных данных, их обработка должна осуществляться в соответствии с установленными требованиями.

Проведя анализ конституционно-правового режима персональных данных, мы приходим к выводу, что вышеуказанные нормы создают необходимое социальное состояние и высокую степень благоприятности для удовлетворения интересов субъектов персональных данных и защиты таких данных.

Кроме того, необходимо соблюдать требования, предъявляемые к его содержанию статьей 9 Закона № 152-ФЗ, в частности согласие должно быть конкретным, информированным и сознательным, а также предоставляться по воле и в интересах их субъекта.

В российском законодательстве дефиниция персональных данных закреплена в Законе № 152-ФЗ и гласит, что это любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Данное понятие является самым широким за всю историю развития Российского законодательства.

Кроме перечисленных основных источников регулирования сферы защиты персональных данных, имеется большое количество подзаконных актов, регулирующих отдельные стороны данного вопроса, заострять внимание на которых не представляется необходимым.

Уяснив понятие персональных данных, источники правового регулирования их охраны и защиты, необходимо обратить внимание на более детальное изучение самого механизма охраны персональных данных, о чем и пойдет речь в следующей главе работы.

Таким образом, если те или иные сведения подпадают под понятие персональных данных, их обработка должна осуществляться в соответствии с установленными требованиями.

Проведя анализ правового режима персональных данных, мы приходим к выводу, что вышеуказанные нормы создают необходимое социальное состояние и высокую степень благоприятности для удовлетворения интересов субъектов персональных данных и защиты таких данных.

Глава 2. Анализ методов конституционно-правовой защиты персональных данных

2.1. Основные требования к доступу, хранению и передаче персональных данных

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» [9].

«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 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» [13].

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.

«Обработка персональных данных в трудовых отношениях представляет собой постоянный процесс, который начинается с момента решения соискателя предложить свою кандидатуру определенному работодателю и предоставления ему необходимых сведений для приема на работу, осуществляется в течение всего периода работы в компании:

- на этапе испытательного срока, в ходе оценки выполняемой работы,
- начислении заработной платы,
- прохождении обучения, переводах, командировках, отпусках,
- увольнении и продолжается после расторжения трудового договора до тех пор, пока работодатель не прекратит свою деятельность или сроки хранения документов не истекут.

В процессе обработки персональных данных работников к работодателю применяется ряд требований, которые он обязан выполнить. Это связано с тем, что именно работодатель осуществляет такую обработку и несет ответственность за безопасность полученных от работника данных.

Одним из требований является опубликование документа, определяющего политику работодателя в отношении обработки персональных данных» [63].

«Такой документ больше направлен на внешнюю среду компании, однако в политике целесообразно рассмотреть порядок обработки персональных данных соискателей, желающих устроиться на работу к работодателю. Особенность политики компании в отношении обработки персональных данных заключается в необходимости обеспечения неограниченного доступа к документу.

Например, можно опубликовать соответствующую политику на официальном сайте компании или организовать стенд в приемной» [28].

«Кроме того, работодателю необходимо издать локально-нормативный акт по вопросам обработки персональных данных работников, содержащим также их права, обязанности, порядок передачи персональных данных работников в пределах компании и другие моменты.

Такой локально-нормативный акт может выступать в качестве самостоятельного документа или быть приложением правил внутреннего трудового распорядка. В любом случае издание такого локально-нормативного акта происходит в порядке статьи 372 ТК РФ и подлежит ознакомлению каждым работником.

Тем самым работодателем будет выполнено требование пункта 10 статьи 86 ТК РФ в части совместной выработки с представителями работников мер по защите их персональных данных.

В пункте 3 статьи 86 ТК РФ указано, что все персональные данные работника следует получать у него самого. Однако бывают случаи, когда работодатель имеет право обрабатывать персональные данные работников в рамках контроля за исполнением ими рабочих обязанностей, делая запросы в другие организации.

Так, суд признал правомерным запрос работодателя в районный суд с уточнением о наличии дел с участием работника, и находился ли он в здании суда в запрашиваемый срок, поскольку, запрашивая информацию о месте нахождения работника в рабочее время, работодателем осуществлены полномочия по контролю за трудовой дисциплиной.

Кроме того, сведений о цели посещения истцом районного суда в запросе и в представленной информации не имеется, а значит по своему характеру и объему информация, которая была запрошена работодателем и представлена судом, не является персональными данными по смыслу, заложенному в статье 3 152 ФЗ» [28].

Из права работника на полную информацию о его персональных данных и обработке этих данных вытекает обязанность работодателя предоставить работнику такую информацию в установленные законом сроки.

«В ходе обработки работодатель обязан принять ряд мер, направленных на выполнение своих обязанностей в области защиты персональных данных работника, в том числе назначить ответственного работника за организацию обработки персональных данных и включить в его должностную инструкцию положения, регламентирующие права, обязанности и ответственность данных лиц, возникающую при работе с персональными данными работников;

- за счет собственных средств обеспечить защиту персональных данных работника от неправомерного их использования или утраты;

- осуществлять внутренний контроль соответствия обработки персональных данных Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, а также ознакомить работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, требованиями к защите персональных данных, проводить обучение указанных работников.

Проверку реализации перечисленных мер и наличие документации, связанной с защитой персональных данных, осуществляет Роскомнадзор как орган, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства.

Статья 88 ТК РФ регулирует передачу персональных данных и устанавливает к ней следующие требования:

- при предоставлении персональных данных третьим лицам запрашивать согласие их владельца;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупреждать получателей персональных данных работника о необходимости использования полученных данных исключительно в

заявленных при передаче целях, а также соблюдать режим секретности в процессе обработки» [28].

«Более того, работодатель может запросить подтверждение соблюдения этого требования у получателей. Здесь важно отметить, что в соответствии с пунктом статьи 6 152-ФЗ в случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор, а лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Отметим, что рассмотренное требование не распространяется на передачу персональных данных работника, предусмотренную ТК РФ или иным федеральным законом; передавать персональные данные работника представителям работников в порядке, установленном ТК РФ и иными федеральными законами, причем работодателю необходимо ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

В части передачи персональных данных третьим лицам существует спорный момент по поводу предоставления трудового договора с генеральным директором акционерам общества» [28].

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» [8].

«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» [14].

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.

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.

Оживленную дискуссию вызвал пакет «антитеррористических» законопроектов, принятый 6 июля 2016 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» [18]. Все эти данные нужно будет передавать правоохранительным органам или суду, при выполнении определенной процедуры.

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 акта (далее - поручение оператора).

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом.

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» [11].

В силу Федерального закона от 26.12.1995 № 208-ФЗ «Об акционерных обществах» (далее – Закон 208-ФЗ) общество обязано обеспечить всем акционерам, независимо от типа и количества принадлежащих им акций, доступ к документам, которые данное общество обязано хранить. Согласно перечню типовых управленческих архивных документов, образующихся в процессе деятельности, организация обязана хранить трудовые договоры, следовательно, такие договоры должны предоставляться для ознакомления по требованию акционера акционерного общества.

Так, ряд судов принимают решения о предоставлении трудовых договоров с руководителями организации акционерам без согласия работника.

Однако такая позиция не представляется верной, с учетом того, что в соответствии со статьей 67 ТК РФ и статьей 3 Закона 152-ФЗ трудовой

договор является документом, содержащим персональные данные работника, а статьей 88 ТК РФ установлен запрет на передачу персональных данных работника третьей стороне.

К тому же КС РФ пришел к выводу, что положение абзаца первого пункта 1 статьи Законом 208-ФЗ об обязанности акционерного общества обеспечить акционерам доступ к своим документам направлено, среди прочего, на обеспечение информационной открытости хозяйственной деятельности акционерного общества и возможности реализации акционерами своих прав, однако при этом необходимо учитывать, что в соответствии со статьей 17 (часть 3) Конституции РФ осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц.

Таким образом, трудовые договоры с руководством общества содержат персональные данные и предоставляются акционерам только с согласия таких работников, что подтверждается более обширной судебной практикой.

В соответствии со статьями 17, 19 Федерального закона от 12.01.1996 № 10-ФЗ «О профессиональных союзах, их правах и гарантиях деятельности» для осуществления своей уставной деятельности профсоюзы вправе бесплатно и беспрепятственно получать от работодателей информацию по социально-трудовым вопросам, в том числе осуществлять контроль за соблюдением законодательства о труде в организациях, в которых работают члены данного профсоюза, а также требовать устранения выявленных нарушений (статья 370 ТК РФ).

2.2. Основания и процедура раскрытия персональных данных

В связи с изменениями от 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.

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.

Основанием раскрытия таких данных является преследование по закону, а именно по определенным категориям преступлений. К ним относятся особо тяжкие преступления из разных отраслей права.

Из уголовного кодекса можно выделить такие категории преступлений, как:

- измена родине и посягательство на основы конституционного и демократического строя на федеральном и региональном уровне, а также при угрозе безопасности государства извне;

- особо серьезные случаи нарушения общественного порядка, а именно: формирование преступных организаций, бандформирований, а также террористических организаций;

- 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).

Также законодательство выделяет 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.

Иные основания, имеются среди составов преступлений в законе о борьбе с наркотиками, о внешней торговле.

В настоящем исследовании уже неоднократно упоминалось, что нормы Трудового кодекса в области защиты персональных данных распространяются исключительно на действующих работников, с которыми заключен трудовой договор.

Однако, любой работодатель в процессе своей деятельности многократно сталкивается с необходимостью приема на работу новых сотрудников, поэтому представляется не лишним рассмотреть вопросы защиты персональных данных такой категории, как соискатели.

Так как соискатель является самостоятельным лицом, трудовой договор с которым еще не заключен его персональные данные обрабатываются по правилу статьи 6 Закона № 152-ФЗ, то есть с согласия субъекта персональных данных.

С другой стороны, исходя из смысла пункта 2 статьи 6 Закона № 152-ФЗ, обработка считается законной в случаях, предусмотренных международным договором или законом, для осуществления и выполнения возложенных законодательством РФ на оператора функций, полномочий и обязанностей.

«Так, статьей 16 ТК РФ устанавливается перечень дополнительных оснований возникновения трудовых отношений, предшествующие трудовому договору, одним из которых является конкурс на замещение соответствующей должности.

В статье 18 ТК РФ конкретизируется такое основание – трудовые отношения будут считаться возникшими, если трудовым законодательством, иными нормативными правовыми актами, или уставом организации определены перечень должностей, подлежащих замещению по конкурсу, и порядок конкурсного избрания на эти должности.

Например, в соответствии со статьей 172 ТК РФ заключению трудового договора предшествует избрание по конкурсу на замещение должности педагогического работника, относящегося к профессорско-преподавательскому составу, в организации, осуществляющей образовательную деятельность по реализации образовательных программ высшего образования и дополнительных профессиональных программ, а также переводу на такую должность.

Следовательно, не требуется согласие соискателя на обработку его персональных данных, предъявляемых с целью замещения по конкурсу вакантной должности в связи с тем, что такая обработка предусмотрена законодательством Российской Федерации» [28].

«Кроме того, согласие на обработку персональных данных от соискателя не требуется, если претендент на открытую вакансию самостоятельно разместил своего резюме в сети Интернет, тем самым сделав его доступным неограниченному кругу лиц. В таком случае по правилу пункта части первой статьи 6 Закона о персональных данных обработка персональных данных, сделанных общедоступными субъектом персональных данных, считается правомерной.

В случае, когда соискателя представляет кадровое агентство, с которым данное лицо заключил соответствующий договор, согласие на обработку работодателем также не запрашивается» [28]. Так как за защиту персональных данных соискателя отвечает соответствующее кадровое агентство, которое обязано предупредить работодателя о необходимости соблюдения конфиденциальности предоставляемой информации.

Зачастую в процессе поиска работы соискатель отправляет свое резюме понравившемуся работодателю по электронной почте. Роскомнадзор дает следующий комментарий по этому поводу: «В случае получения резюме соискателя по каналам электронной почты работодателю необходимо дополнительно провести мероприятия, направленные на подтверждение факта направления, указанного резюме самим соискателем.

К примеру, к таким мероприятиям можно отнести приглашение соискателя на личную встречу с уполномоченными сотрудниками работодателя, обратная связь посредством электронной почты и т.д.” Представляется, что в данном разъяснении речь идет о любой обратной связи на письмо соискателя. С точки зрения делового этикета такой ответ подразумевается сам по себе.

Однако, юридических предпосылок в данном контексте не прослеживается. Необходимость ответа на письмо соискателя появляется только в случае, указанном статьей 64 ТК РФ, а именно обязанность работодателя сообщить причину отказа по письменному требованию лица, которому отказано в заключении трудового договора» [28].

«В случае сбора и обработки персональных данных соискателя на основании письменной анкеты, заполняемой непосредственно кандидатом, такая анкета должна соответствовать требованиям п. 7 Постановления № 687, в частности, содержать сведения о цели обработки персональных данных, сроки обработки и перечень действий с ними, также предусматривать поле для отметки о согласии на обработку персональных данных соискателем

Такая анкета может размещаться в электронной форме на сайте работодателя – в этом случае согласие на обработку персональных данных подтверждается соискателем путем проставления отметки в соответствующем поле. Также стоит принимать во внимание указанное положение в случае, если пропускная система на территорию работодателя

организована таким образом, что каждый посетитель компании отмечается в журнале прохода посетителей и работников» [31].

«Согласно пункту 4 статьи 21 Закона 152-ФЗ при достижении цели обработки, оператор обязан ее прекратить и уничтожить персональные данные в срок, не превышающий 30 дней с даты достижения цели обработки, если иное не предусмотрено федеральными законами.

В связи с тем, что отношения соискателей и работодателя на федеральном уровне не регулируются, а договор между ними еще не заключен, работодатель при трудоустройстве одного из кандидатов должен уничтожить персональные данные остальных претендентов на вакантную должность в указанный срок.

В ряде случаев при отборе кандидатов запрашивается информация о соискателе на его предыдущих местах работы в виде характеристики или рекомендации» [31].

«Так, работодатель вправе запросить, а бывший работодатель — предоставить такую информацию на основании письменного согласия поступающего на работу лица. При этом требования законодательства не будут нарушены.

Однако, требование предоставления согласия соискателя не распространяется на случаи заключения трудового договора с бывшим государственным или муниципальным служащим.

Согласно статьей 64.1 ТК РФ работодатель при заключении трудового договора с такими гражданами в течение двух лет после их увольнения с государственной или муниципальной службы обязан в десятидневный срок сообщать о заключении трудового договора работодателю по последнему месту его службы в соответствующем порядке – эта норма призвана способствовать обеспечению контроля за соблюдением бывшими государственными и муниципальными служащими ограничений и запретов,

установленных законодательством в целях противодействия коррупции на территории РФ» [31].

«Кроме того, не требуется согласие для уточнения или получения дополнительной информации по прежним местам работы об соискателях, подавших документы на замещение вакантных должностей государственной гражданской службы, поскольку перечень предоставляемых документов, определен федеральным законом.

Одним из важных вопросов при предоставлении информации является ее достоверность, поэтому ряд работодателей устраивают дополнительные проверки кандидатов при приеме на работу и в процессе трудовой деятельности, включая проверку на детекторе лжи (полиграфе)» [31].

«Законодательство РФ не содержит прямых запретов на такие действия в отличие от международных норм права. Хотя проверка на полиграфе носит добровольный характер и осуществляется на основании письменного согласия, представляется халатной невнимание законодателя к вопросам регулирования подобной процедуры хотя бы потому, что с проведением проверки зачастую связаны случаи незаконного наложения дисциплинарных взысканий, увольнений, и принуждения к расторжению трудового договора» [21].

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.

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.

«Сбор, хранение, изменение, передача и другие виды обработки персональных данных стали доступны всем и каждому. Кроме того, возникла проблема неконтролируемых данных, когда информация, оставленная пользователем на веб-сайте, хранится годами, часто без его ведома.

Одновременно с этим назрела потребность разработать правила, регулирующие использование персональных данных институтами, органами и учреждениями наднациональной организации, а также должностными лицами и сотрудниками таких органов» [22].

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.

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.

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.

Основанием раскрытия таких данных является преследование по закону, а именно по определенным категориям преступлений. К ним относятся особо тяжкие преступления из разных отраслей права.

Глава 3. Пути совершенствования конституционно-правовой защиты персональных данных

3.1. Основные проблемы конституционно-правовой защиты персональных данных

Конституция РФ закрепила демократический путь развития нашего государства, главная ценность которого – человек и защита его прав. Но и сегодня нерешенными остаются некоторые вопросы, в том числе обеспечение права граждан на частную жизнь и проблемы защиты личной информации.

В 2006 году был подписан Федеральный закон Российской Федерации № 152 «О персональных данных», по ужесточенным требованиям которого модернизированы базы данных, предназначенные для накопления, сохранения или выдачи персональных данных.

Детально требования по защите персональных данных прописаны в:

- Положении о безопасности информационных систем личных данных, утвержденном Постановлением Правительства России № 781 в 2007 году;

- Совместном приказе ФСБ, Мининформсвязи, ФСТЭК № 55/86/20 2008 года;

- Внутренних инструкциях ФСБ и ФСТЭК.

Указанные требования о защите персональных данных распространяются на деятельность всех учреждений и организации и направлены на предупреждение утечек конфиденциальной информации.

Существует перечень распространенных проблем защиты персональных данных, обусловленных организационными и техническими аспектами.

По Указу Президента России № 188 от 6.03.1997 г. «Об утверждении Перечня сведений конфиденциального характера», утвердившему перечень закрытых данных, подлежащих правовой защите. В силу их

конфиденциальности для их защиты требуется наличие лицензии ФСТЭК на организацию безопасности конфиденциальных данных. Аналогичные требования предъявляет ФСТЭК РФ к операторам информационных баз данных 1, 2 и 3 класса. Они распространяются на большинство коммерческих и государственных учреждений. Для применения средств криптографической защиты обрабатываемых конфиденциальных данных нужна лицензия ФСБ.

Для получения таких лицензий сотрудники организации должны обладать соответствующей квалификацией и опытом работы. Также потребуется специализированное оборудование и помещение, что сложно обеспечить в небольших компаниях.

Еще одной распространенной проблемой являются жесткие императивные требования к системам по защите персональных данных. Защита информационных систем персональных данных 1 класса приравнена к защите сведений, содержащих государственную или коммерческую тайну. Обязательное требование – защита конфиденциальных баз данных от утечек из-за электромагнитных импульсов вычислительной техники и средств связи.

Под защиту 1 класса попадают базы персональных данных, а также базы, содержащие и обрабатывающие одновременно большое количество сведений. Такие базы данных встречаются в большинстве корпораций (частных и муниципальных).

А нормативы ФСТЭК, регламентирующие порядок обработки персональных данных, обозначены грифом «Для служебного использования». Получить указанные акты могут операторы персональных данных и организации, обеспечивающие защиту персональных данных по лицензии ФСТЭК.

Одна из проблем защиты конфиденциальных сведений, которыми являются персональные данные, – это отсутствие сертифицированных компьютерных программ. Предлагаемые программы не соответствуют требованиям, предъявляемым к 1 и 2 уровням защиты персональных данных.

К примеру, сертифицированные программы по защите и управлению базами данных (открытый код MySQL) не представлены на российском рынке, а лицензионная ОС Microsoft Windows применима только для защиты информационных баз данных до 2 уровня. Нерешенной проблемой остается защита баз данных при использовании 64-разрядных ОС и операционных систем Unix и Linux.

Предлагаемые лицензионные защиты персональных данных не соответствуют требованиям нормативных актов или неприменимы в условиях хранения и обработки больших объемов данных, поскольку не отвечают техническим требованиям. Так, для работы программы безопасности баз данных Secret Net необходимы аппаратные компоненты, установить которые через blade-сервер невозможно.

А программы, используемые при работе с персональными данными, проверяются перед установкой на наличие недекларированных возможностей. Для проведения указанной проверки предоставляются исходные коды программ, на что согласны далеко не все компании-производители программ для ПК, особенно иностранные.

До начала работы с информационными базами персональных данных подтверждают, соответствует ли защита требованиям, предъявляемым к 1, 2 и 3 классам. Для этого проводится аттестация системы обработки данных. Если раньше подобная процедура проводилась только в государственных учреждениях, то сегодня проверка уровня защиты персональных данных обязательна для всех организаций.

Еще одной проблемой является недостаточное количество российских компаний, специализирующихся на предоставлении услуг по технической защите конфиденциальных данных, получивших лицензию, не способных удовлетворить увеличивающийся с каждым годом спрос на техническую защиту персональных данных. А порядок лицензирования неприменим к большому количеству желающих получить аттестат на работу с персональными данными.

На современном этапе развития нашего общества необходимо отметить, что ни один из нас не может уже обойтись без сети Интернет. Информационно-телекоммуникационная сеть Интернет является сейчас одним из главных средств для свободного распространения информации, аккумулирующее практически все доступные источники информации.

В связи с этим возникает необходимость правового регулирования данной сферы, в целях обеспечения прав граждан. С одной стороны, обеспечиваемые статьей 29 Конституции Российской Федерации свобода слова, свобода получения, использования и распространения информации любым законным способом не подлежат ни ограничению, ни ущемлению.

Однако, с другой стороны очевидна необходимость защиты персональных данных граждан, права на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства.

Опираясь на исследования уровня информационной безопасности Российских компаний 2018 год, можно сказать, что 21% опрошенных компаний пострадали от утечек информации, 15% компаний удалось предотвратить кражу данных, 46% организаций не сталкивались с подобными инцидентами, а 18% респондентов не владеют подобной информацией.

Во-первых, утекала информация о клиентах и сделках (32%), во-вторых, техническая информация (26%), в-третьих, персональные данные, а также информация о партнерах (14%) и внутренняя бухгалтерия (7%). В основном виновниками таких инцидентов становились рядовые сотрудники данных компаний [6].

«Наиболее проблемным моментом, на наш взгляд, в регулировании защиты персональных данных в процессе трудовых отношений является отсутствие единообразного толкования термина биометрические данные, в частности, отнесение к ним фото- и видеоизображений работников, а соответственно, и понимания, какие данные о человеке могут являться биометрией.

На данный момент в отношении идентификации фотоизображения как биометрических данных действует единственный документ, регулирующий удостоверение личности гражданина, осуществляющего выезд и въезд на территорию РФ.

Очевидно, что применять его в трудовых отношениях не представляется возможным. Кроме того, разъяснения об отнесении фото- и видеоизображений к биометрическим данным дает проверяющий орган, в полномочия которого не входит толкование законодательства, и, соответственно, такие разъяснения носят рекомендательный характер.

На практике обозначенная проблема приводит к разночтениям законодательства, в том числе со стороны Регулятора, и, как следствие, к дополнительным штрафным санкциям в отношении работодателя, принявшего «не ту сторону» толкования.

На основании чего считаем отсутствие четкой позиции отнесения фото- и видеоизображений пробелом в современном законодательстве, который следует урегулировать» [39].

Другим проблемным моментом законодательства в области защиты персональных данных работника является отсутствие регулирования проверок на полиграфе несмотря на то, что в настоящее время РФ входит в число пяти ведущих государств мира по объемам прикладного применения полиграфа в правоохранительных целях, а коммерческое применение полиграфа осуществляется более чем в двадцати городах России.

«Как было отмечено выше, судебная практика по данному вопросу выявляет случаи незаконного наложения дисциплинарного взыскания, увольнения и принуждения к расторжению трудового договора вследствие использования тестирования на детекторе лжи.

Причем международные стандарты труда, как и национальное законодательство большинства европейских стран, содержат нормы о запрете проверок или их строгое ограничения в государственной и коммерческой сферах.

По нашему мнению, отсутствие регулирования исследований на полиграфе на территории РФ затрудняет и сдерживает применение опросов в правоохранительных целях, а также создает условия для злоупотребления.

Так, например, создание единой системы подготовки и аттестации полиграфологов, будут способствовать отмене дискредитации метода и защите прав субъектов при использовании результатов опросов» [31].

«Необходимо отметить, что в настоящее время не требуется создания новых структур в сфере разработки и внедрения инициатив в области саморегулирования, необходима активизация уже существующих организаций.

Целесообразно, в перспективе, на государственном уровне вводить институт саморегулируемых организаций информационной сферы, основной целью которых будет являться обеспечение добросовестного регулирования деятельности в интернете. Реализация данного института будет невозможной без стимулирования и пропаганды государством в обществе саморегулирования сетевых отношений.

Проблема экстерриториальности и глобальности сети Интернет, обусловленная ее распространенностью в мире и территориальной компетенцией отдельных государств, должна решаться путем международного сотрудничества в данной области через унификацию законодательства о правовом регулировании и функционировании сети Интернет различными странами.

Разработка единых правил (модельных кодексов) приведет к упорядочиванию и унификации взаимоотношений между субъектами сетевых отношений. Поскольку в настоящее время подобная унификация невозможна, вопросами регулирования сети Интернет займутся законодательные органы власти, что приведет к сближению национальных правовых систем» [21].

«Современное состояние законодательной базы в российском сегменте сети Интернет и необходимость ее изменения и развития обозначают три

основных направления развития внутрироссийского законодательства в области регулирования отношений, возникающих в сети Интернет:

- разработка принципиально новых законодательных и иных нормативных актов, учитывающих специфику функционирования и развития сети (например, Федерального закона базисного характера «О правовом регулировании сети Интернет в Российской Федерации»);

- частичная трансформация функционирующей в Российской Федерации нормативно-правовой базы для ее приспособления к действующим правоотношениям;

- создание (или разъяснение) механизмов прямого использования применительно к Интернету части действующих законодательных актов без изменения их содержания» [21].

Также следует выделить следующую проблематику российского законодательного регулирования правомерного использования персональных данных.

1. Двойное регулирование с нормами GDPR. Помимо приведенных законов на российских операторов данных распространяет свое действие Регламент GDPR – как на компании, не учреждённые в Евросоюзе, но обрабатывающие персональные данные находящихся в Евросоюзе субъектов данных. То есть, говорить о гармонизации российского законодательства и Регламента GDPR нельзя, так как в практическом плане для российских компаний это означает «двойное обременение». Более того, многие нормы российского законодательства, входят в расхождение с нормами Регламента. Так, соблюдение российскими компаниями требований Пакета Яровой может привести к нарушению ими законодательных норм, действующих в другом иностранном государстве, в частности – регламентированных GDPR требований о конфиденциальности.

2. Говоря о законодательных противоречиях, стоит посмотреть на проблему и с другой стороны: иностранные компании-операторы данных,

вынужденные выполнять императивные требования Пакета Яровой, также начали значительно сокращать свое присутствие на российском рынке услуг.

В этой связи стоит отдельно отметить Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» от 21 июля 2014 г. N 242-ФЗ. В соответствии с этим законом Россия начала выстраивание беспрецедентного механизма локализации персональных данных, не имеющего аналогов в зарубежных странах. Так, главная копия персональных данных российских граждан, собранных в России, должна быть расположена именно в России. Согласно исследованию ECIPE13 потери российской экономики от ухода европейских компаний всего за год составили 0,27% ВВП, что эквивалентно 5,7 млрд долларов.

По оценкам РСПП, к 2019 г. операторы должны были потратить на реализацию пакета около 17 трлн рублей. Безусловно, эта сумма нереальна для операторов, и строгость законодательных норм в данный момент компенсируется тем, что правоприменительные органы почти не наказывают за фактические нарушения.

3. Как отмечено в Программе «Цифровая экономика», в России, в отличие от большинства государств, не существует правил оценки центров хранения и обработки данных. В связи с этим отсутствует и объективная возможность для оценки уровня оказываемых услуг, в том числе по объему возможных для хранения данных.

Исходя из анализа последних редакций соответствующих законов, можно сделать вывод о том, что российский законодатель пошел по пути локализации данных пользователей, значительно ограничив трансграничную передачу данных. Безусловно, такой подход тоже имеет право на существование, но опыт США и даже Китая, известного своей закрытой цифровой средой, показывают общемировую тенденцию на гармонизацию правовых норм с Регламентом GDPR. Регламент действительно является

наиболее продуманным законом. GDPR имеет юридические решения, которые можно заимствовать для совершенствования отечественного регулирования в данной сфере. Гармонизация права привела бы к повышению уровня защиты прав и законных интересов субъектов персональных данных, устранения правовых споров и повышению предпринимательской активности.

Можно сделать вывод о различии как правового регулирования, так и морального подхода к персональным данным как к объекту регулирования. В Европейском союзе они рассматриваются через призму прав – права на неприкосновенность частной жизни, права на информацию и др. Кроме того, американскую модель можно охарактеризовать большой степенью саморегулирования, в отличие от централизованной европейской. Россия в данный момент склоняется в пользу выстраивания собственной модели работы с данными, обеспечивая полный централизованный внутренний контроль за их использованием.

Так же можно выделить еще одну очень актуальную проблему в российском законодательстве о защите персональных данных. Она заключается в следующем. Несмотря на то, что в России имеется специальный закон, регулирующий обработку персональных данных из Интернета (метаданных), указанные поправки были внесены в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее Закон № 149-ФЗ).

Анализ правовых источников приводит к выводу, что на сегодняшний день отсутствует специальное регулирование для метаданных. Они регулируются через старое понятие персональных данных либо через расширенный для них термин.

По нашему мнению, данный подход вызывает ряд трудностей для регулирования правомерного использования метаданных. Во-первых, объектом работы с метаданными являются огромные массивы информации, которые лишь частично могут быть отнесены к категории персональных

данных. Даже самые широкие определения, одно из которых, к примеру, дается в GDPR, указывает на то, что персональные данные должны прямо или косвенно указывать на субъект обработки данных. Однако немалый массив метаданных представляет собой статистические данные, являющиеся обезличенными и никак не указывающие на субъекта. Другими примерами могут служить мировые климатические данные, данные GPS-трекеров общественного транспорта, а также - датчиков контейнеров морских судов и так далее.

Во-вторых, законодательство о персональных данных всегда строго в отношении согласия субъекта данных: их можно обрабатывать лишь при его наличии. В некоторых случаях оно может быть выражено не столь явно, в некоторых – требуется совершение определенных действий для получения согласия, то есть оно должно быть ярко выраженным. Кроме того, по п. 3 ст. 7 GDPR отозвать согласие должно быть столь же легко, как и дать его. Однако развитие цифровых технологий демонстрирует продолжительную тенденцию к умалению возможности физического контроля владельца над информацией. Многие авторы даже считают право на неприкосновенность частной жизни устаревшим. В любом случае конфликт между преимуществами, которые обеспечивают современные IT-технологии, и правом на неприкосновенность частной жизни, становится все острее. Даже если не придерживаться такой радикальной точки зрения, тот факт, что в настоящее время субъект не может полноценно подвергать контролю оборот информации о нем в сети Интернет и, следовательно, иметь реальной возможности удалить/изменить информацию, очевиден. Даже если субъект данных действительно изучит соответствующие положения политики конфиденциальности, они все равно могут изменяться, причем часто – большинство компаний включают оговорку о возможности одностороннего изменения политики. При этом даже нововведения GDPR и стремительное развитие «права на забвение» не обеспечивают пользователю Интернета должного уровня информированности и защиты своих прав.

В-третьих, использование персональных данных в большинстве случаев предполагает их целевое использование. Например, п. 7 ст. 5 ФЗ о Персональных данных гласит: «Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных». Однако учитывая тот факт, что метаданные все в большей степени рассматриваются в качестве цифрового актива, законодательное закрепление их целевого, определенного сроком использования препятствуют развитию бизнеса. Так, большинство мессенджеров негласно (т. к. официальная продажа является нарушением действующего законодательства) продают данные другим компаниям. По сути, продажа обезличенных данных – их самый существенный источник прибыли, но он остается в тени. Факт, что данные пользователей – источник доходов поисковых сервисов, мессенджеров и социальных сетей, продолжает игнорироваться законодателем, в том числе и российским. Так, предоставления персональных данных на обработку в качестве встречного предоставления по договору (ст. 423 ГК РФ) недостаточно для его квалификации как возмездного.

Говоря о целевом использовании, в профессиональной среде указывается, что проблема пересечения ФЗ о Персональных данных и метаданных – это свободное использование личной информации, не ограниченной самими же пользователями при выбросе «своей персональной информации» в общедоступные ресурсы. В существующем законодательстве нет предпосылок для использования персональных данных в коммерческих целях.

В-четвертых, сам факт применения законодательства о персональных данных к метаданным вызывает логические затруднения как для простых пользователей, так и для компаний. Даже продвинутые пользователи, которые осведомлены о том, что представляют из себя Большие данные, позиционируют их именно как деперсонализированный набор данных. И

поэтому, например, обращение к «Регламенту о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных» для того, чтобы узнать о своих правах – далеко не самое очевидное для субъекта решение.

Тем не менее, определенные подвижки в сторону того, чтобы отделить метаданные от персональных, все же есть, в том числе в России. В октябре 2018 г. был представлен законопроект № 571124-7 «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации"». Согласно ему «большие пользовательские данные – совокупность не содержащей персональных данных информации о физических лицах и (или) их поведении, не позволяющая без использования дополнительной информации и (или) дополнительной обработки определить конкретное физическое лицо, собираемой из различных источников, в том числе сети Интернет, количество которых превышает тысячу сетевых адресов». Характеристики, содержащиеся в данном определении, весьма спорны, но их обсуждение не столь целесообразно, так как законопроект был отменен. В контексте исследования параграфа данной главы важнее тот факт, что законодатель пошел по пути отделения Больших данных от персональных данных. Следующий шаг – это создание отдельного федерального закона, а не точечная доработка уже существующих.

Вероятно, законодателю следует сконцентрировать свое внимание не на том, как именно пользователь делится с обработчиками данных информацией о себе, а на том, как эти данные впоследствии используются. На данный момент от 40% до 60% людей готовы делиться обезличенными данными. Но гораздо больше пользователей Интернета будут готовы к этому в случае, если они будут уверены в безопасности их применения. Но сейчас превалирует другая тенденция: в 2017 г. было зафиксировано 1579 утечек данных, для сравнения в 2007 г. их было лишь 65617. Отсюда следует, что целесообразнее было бы не продолжать расширение толкования персональных данных и других сопутствующих понятий, а разработать

самостоятельные законодательные акты, применимые к Большим данным, где будет тщательно закреплен порядок хранения и распространения данных: компании будут готовы выполнять жесткие предписания в обмен на послабления в порядке сбора и обработки данных.

Таким образом, на базе анализа актов, был сделан вывод о необходимости разработки особого регулирования использования метаданных. Даже несмотря на высокий правовой уровень и проработанность таких актов, как GDPR, - метаданные ввиду их особой природы и ценности нуждаются в собственном закреплении. А точечное модифицирование существующего законодательного регулирования в сфере защиты персональных данных не сделает его более эффективным.

Можно сделать вывод, что проблемы, которые существуют в процессе защиты персональных данных требуют тщательного регулирования, чтобы избежать в дальнейшем последствий, связанных с использованием конфиденциальной информации заинтересованными в этом третьими лицами.

3.2. Пути решения проблем в сфере конституционно-правовой защиты персональных данных

Организации, специализирующиеся на обработке и хранении персональных данных, используют автоматизированные базы данных. Это компьютерные базы данных, связь с которыми происходит по техническим каналам.

Вот почему вопросы защиты персональных данных, информационных процессов, а также действия государственных норм регулирования отношений между сотрудником и работодателем остаются актуальными. Решение данной задачи не бывает сегментарным.

Требуется комплекс мероприятий, направленных на защиту (техническую и правовую) персональных данных сотрудников и клиентов организации.

Несмотря на проблемы, данная задача решаема. Возможны два варианта защиты обрабатываемых и передаваемых персональных данных, учитывающих требования законодательства и имеющийся у компании бюджет.

Сократить расходы на защиту конфиденциальных баз данных позволит грамотная подготовка и организация всей информационной системы. В корпорации целесообразно разделить базы данных на территориальные, что позволит сократить объем обрабатываемых в каждой базе персональных данных. В результате этого снизится их класс безопасности. А применение зашифрованных идентификаторов обезличит передаваемые персональные данные [60].

Сокращает расходы методика терминального доступа, используемая в программах обработки персональных данных. При использовании данной технологии информация обрабатывается на сервере, а через рабочие станции выводятся и отображаются данные.

Применение данной технологии позволяет понизить класс безопасности рабочих станций до третьего и снизить затраты на защиту и аттестацию системы обработки данных. Используя данную методику, компания экономит на приобретении сложной вычислительной техники и управлении информационными базами данных, благодаря децентрализации информационной базы и уменьшению требований к техническим характеристикам пользовательских компьютеров.

Внедрение новых программ обработки персональных данных с использованием программ со встроенной лицензионной защитой, прошедших аттестацию по требованиям безопасной передачи данных и проверку на наличие недекларированных возможностей, снижает расходы на приобретение в будущем дополнительного ПО и оплату обучения

сотрудников компании. Также при согласовании с ФСТЭК допускается применение программ, не прошедших проверку на недекларированные возможности.

Дополнительно обозначают сотрудников, отвечающих за безопасность персональных данных. В корпорациях более экономным будет создание собственного отдела информационной безопасности, получение необходимых аттестатов и лицензий, самостоятельная защита баз данных.

Далее уточняют, какие персональные данные требуются компании. Чем выше степень обработки данных сотрудников и клиентов, тем сложнее процесс их защиты.

Более усиленный вариант защиты предусмотрен для данных, касающихся здоровья и личной жизни сотрудников или клиентов, – политических и религиозных взглядов, национальности, родственных отношений, а вот данные, необходимые для идентификации лица, в такой охране не нуждаются [64].

Персонал компании, обеспечивающий безопасность персональным данным сотрудников и клиентов, отбирает данные, которые не требуются для работы компании, исключая их из объема собираемой и обрабатываемой информации.

В завершение сотрудники службы безопасности баз данных подготавливают в форме таблицы списки работников, получивших доступ к сбору, обработке и хранению конфиденциальных данных о служащих и клиентах. Предупреждает утечку закрытых данных при увольнении работник, проверяя, что данные о нем заблокированы или удалены.

А для небольших компаний экономически выгодное решение – подписание соглашения с организацией, которая подготовит и внедрит программу безопасности баз данных с последующим аутсорсингом (передачей компании-заказчику) функционирующей системы по защите персональных данных сотрудников и клиентов.

Данное соглашение позволит снизить затраты на обучение и выплату зарплаты штатным работникам, а также минимизирует риски утечки конфиденциальной информации.

Перед заключением данного соглашения составляется список требований к внедряемой системе защиты информации. При этом учитывают, что все системы защиты конфиденциальных данных имеют специальное назначение. Они призваны предупредить утечку защищаемых данных и обеспечить их сохранность и доступность. Требования к системам защиты баз данных варьируются в зависимости от выявленной модели угроз.

Индивидуальная разработка программ информационной безопасности потребует от разработчика высокой квалификации и повышенной ответственности за функционирование и значимость представленной модели. В то же время такие системы защиты персональных данных нацелены исключительно на выявленную модель угроз и уступают по функциональности типовым системам информационной безопасности.

Данное направление постоянно развивается, поскольку государственное регулирование в сфере технических требований к обеспечению информационной безопасности также меняется. До появления сети Интернет основную угрозу представляли модели зарубежных технических разведок, поэтому система защиты от них была четко прописана в нормативных актах. На основании существующих норм строится и защита личной информации сотрудников компании с учетом специфики ее работы.

Отметим, что согласно упомянутой статье 13.11. КоАП РФ за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) предусмотрена ответственность в виде предупреждения или наложения административного штрафа:

- на должностных лиц - от 500 до 1000 рублей;
- на юридических лиц - от 5000 до 10 000 рублей.

«Представляется, что столь незначительное наказание не имеет должного эффекта для предотвращения нарушений в области защиты персональных данных. Так, решением суда должностному лицу, нарушившему требования законодательства при передаче третьему лицу сведений об адресе работников, а также не принявшему меры по уничтожению документов, содержащих персональные данные, после истечения сроков хранения, назначено административное наказание в виде предупреждения. А в случае, отсутствия у работодателя мер защиты персональных данных, суд налагает административный штраф в размере 500 рублей.

К тому же, в соответствии с частью 1 статьи 4.5 КоАП РФ постановление по делу об административном правонарушении не может быть вынесено по истечении трех месяцев со дня совершения административного правонарушения, в связи с чем виновных не всегда получается привлечь к ответственности» [44].

«Так, в 2015 году в Государственную Думу РФ был направлен законопроект, существенно ужесточающий меры наказания за нарушение норм в области защиты персональных данных. Например, невыполнение оператором обязанности по опубликованию политики в отношении обработки персональных данных и сведениям о реализуемых требованиях к защите персональных данных в соответствии с предложенным законопроектом влечет предупреждение или наложение административного штрафа на должностных лиц - от 3000 до 6000 рублей, на юридических лиц - от 15000 до 30000 рублей; обработка персональных данных без согласия субъекта наказанием в виде штрафа на должностных лиц - от 5000 до 15000 рублей; на юридических лиц - от 30000 до 50000 рублей; а за незаконную обработку специальной категории персональных данных – штрафом на должностных лиц - от 10000 до 25000 рублей; на юридических лиц - от 150000 до 300000 рублей» [44].

По нашему мнению, подобные меры будут способствовать соблюдению законодательства о защите персональных данных, однако, приведение внутренних процессов в соответствии с законодательством связано с большими затратами, поэтому вступление в силу рассматриваемого законопроекта может привести к дополнительной нагрузке на работодателей и как следствие – уменьшению рабочих мест.

«Статьей 13.12. КоАП РФ предусматривается административная ответственность за нарушение правил защиты информации.

Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации, влечет наложение административного штрафа:

- на должностных лиц - от 2500 до 3000 рублей;

- на юридических лиц - от 20000 до 25000 рублей с конфискацией несертифицированных средств защиты информации или без таковой.

За нарушение требований защиты информации, установленных федеральными законами или иными нормативными правовыми актами РФ, налагается административного штраф:

- на должностных лиц - от 1000 до 2000 рублей;

- на юридических лиц - от 10 000 до 15 000 рублей.

Если работодатель игнорирует требование статьи 18.1 Закона № 152-ФЗ в части назначения ответственного за организацию обработки персональных данных и издания локальных актов по вопросам обработки персональных данных, ему грозит наложение административного штрафа в размере от 30000 до 50000 рублей.

Статья 12 Гражданского кодекса РФ (далее – ГК РФ) перечисляет способы защиты нарушенных прав. Применительно к области обработки персональных данных можно отнести возмещение убытков и компенсацию морального вреда» [44].

«Так, в статье 15 ГК РФ устанавливается, что лицо, чье право нарушено, может требовать возмещения причинённых убытков, то есть расходов, которые понесло пострадавшее лицо, и неполученных этим лицом доходов, а согласно части 2 статьи 1099 ГК РФ моральный вред подлежит компенсации в случаях, предусмотренных законом.

Статья 152.2. ГК РФ устанавливает запрет на сбор, хранение, распространение и использование любой информации о частной жизни гражданина без его согласия.

Такими действиями пострадавшему может быть причинен моральный вред, за возмещением которого он вправе обратиться в суд. В соответствии с частью второй статьи 24 Закона № 152-ФЗ, возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

При определении размеров денежной компенсации за причинённый моральный вред учитываются степень физических и нравственных страданий гражданина, которому причинен вред, а также степень вины нарушителя. Норма о необходимости компенсировать моральный вред работника существует также в Трудовом кодексе (статья 237 ТК РФ). Она указывает на необходимость согласования сторонами спора размера денежной формы такой компенсации» [44].

Пленум Верховного Суда Российской Федерации уточняет, что при рассмотрении споров, возникших в связи с распространением информации о частной жизни без согласия ее владельца, последний вправе требовать возмещения морального вреда.

«При рассмотрении дела о разглашении персональных данных работника путем публикации дополнительного соглашения к трудовому договору в сети Интернет истец утверждал о наступлении негативных последствий - условия трудового договора стали предметом обсуждения неограниченного числа пользователей. Суд обязал взыскать с ответчика компенсацию морального вреда в размере 25 000 рублей» [44].

Материальная ответственность за нарушение норм защиты персональных данных возникает на основании статьи 238 ТК РФ. Так, работник, разгласивший персональные данные своих коллег, обязан возместить затраты работодателя на возмещение ущерба, понесенного работником третьим лицам.

Таким образом, работодатель вправе потребовать с виновного работника компенсации затрат на возмещение морального вреда пострадавшим, в том числе обратиться в суд в течение одного года со дня обнаружения причиненного ущерба. (часть 2 статья 392 ТК РФ)

Пленум ВС РФ устанавливает правило, в соответствии с которым работник несет материальную ответственность лишь в пределах сумм, выплаченных работодателем третьим лицам в счет возмещения ущерба, при условии наличия причинно-следственной связи между виновными действиями (бездействием) работника и причинением ущерба третьим лицам.

Из вышесказанного можно сделать вывод, что «наложение материальной ответственности на работника возможно только в случае выполнения следующих условий:

- разглашение произошло из-за виновного противоправного поведения работника (статья 233 ТК РФ);

- существует причинно-следственная связь между виновными действиями (бездействием) работника и причинением ущерба третьим лицам;

- неразглашение охраняемой законом тайны предусмотрено трудовым договором или приложением к нему, а такая тайна может стать известна работнику при выполнении им трудовых обязанностей;

- полная материальная ответственность за ущерб, причиненный разглашением сведений, составляющих охраняемую законом тайну, прямо предусмотрена федеральным законом» [18].

Решение проблем, возникающих в сфере обеспечения информационной безопасности, возможно при взаимодействии сотрудников, собирающих и

обрабатывающих персональные данные, разработчиков компьютерных программ и систем защиты информации и государственных структур.

Несмотря на то что стимулирование поддержания доминирования компании в сборе, обработке и использовании данных не являются конкурентным для рынка, принося выгоду как для потребителей, так и для компаний и государства инновации, многие антимонопольные органы подчеркивают, что экономика, выстраиваемая персональными данными, может также приводить к рыночной власти и долгосрочным конкурентным преимуществам одних компаний над другими.

Возможный выход из этой ситуации, который можно предложить – это введение дополнительных пороговых значений для нотификации, например стоимости сделки. Это позволило бы уменьшить количество «предупреждающих поглощений», то есть ситуаций, когда большая корпорация покупает небольшие компании, обладающие меньшими ресурсами, но большим потенциалом (в том числе в виде нового способа применения данных). Еще один вариант – это дополнительная проверка, достаточно ли платформы дифференцированы для доступа разных групп потребителей.

Монополизации рынка также может способствовать тому, что структура издержек использования, а также обработки информации весьма необычна: имеются в виду высокие начальные невозвратные издержки при стремящихся к нулю предельных издержках. Поэтому компания, однажды занявшая первенство в обработке и использовании данных, может сохранять лидерство долгие годы, даже предоставляя более слабый рыночный продукт.

На сегодняшний день крупные агрегаторы информации повсеместно пытаются монополизировать имеющиеся у них данные, получаемые от пользователей. Поскольку выработанных законодательных норм в этой сфере еще не существует, сейчас линия противостояния подобных монополистов с иными участниками рынка, заинтересованными в сборе и использовании в своем бизнесе такой информации, проходит в основном через судебные

органы. Суды в условиях отсутствия законодательного регулирования метаданных вынуждены подменять собой другие ветви власти, что неправильно.

Таким образом, решая поставленные проблемы, можно сделать вывод, что законодательство о персональных данных и антимонопольное законодательство не отвечают современным требованиям в сфере регулирования применения метаданных. Наиболее логичным решением данной ситуации является разработка профильного закона для метаданных, а также доработка существующего антимонопольного законодательства. При этом важно, чтобы закон учитывал, что не столько сбор данных, сколько возможность оперативно извлекать полезную информацию из их большого объема и разнообразия обеспечивает конкурентное преимущество компаний.

Заключение

В настоящее время использование персональных данных открывает компаниям новые возможности по воздействию и контролю над конкурентной ситуацией на рынке, ставит под угрозу тайну личной жизни и равенство людей. Стремительное развитие цифровой экономики в сочетании с низким уровнем расходов на внедрение инновационных продуктов влечет постоянное отставание государственного регулирования от экономических реалий. При этом объем данных, обрабатываемых в мировом масштабе, растет колоссальными темпами.

Освоение персональных данных, в зависимости от субъективной точки зрения, можно отнести как к одному из величайших достижений человечества, так и к одной из самых больших проблем. Безусловно, начало использования персональных данных дало возможность компаниям предлагать новые решения, построенные на основе индивидуальных предпочтений потребителя, а ему – получать новый персонализированный продукт, наиболее подходящим образом удовлетворяющий желаниям.

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

Проведя анализ правового режима персональных данных, мы приходим к выводу, что вышеуказанные нормы создают необходимое социальное состояние и высокую степень благоприятности для удовлетворения интересов субъектов персональных данных и защиты таких данных.

В настоящей работе на основании действующего законодательства в области защиты персональных данных как в национальном праве, так и на международном уровне, научных трудов ведущих российских школ

трудового права, правоприменительной и судебной практики было проведено исследование особенностей регулирования защиты персональных данных работников.

В частности, были изучены основные положения законодательства по исследуемой теме, рассмотрены особенности обработки персональных данных при приеме на работу, в процессе трудовой деятельности, после увольнения работников, проанализированы меры уголовной, административной, гражданско-правовой, материальной и дисциплинарной ответственности за нарушение установленных требований обработки персональных данных работников с учетом позиций судов РФ при рассмотрении соответствующих дел.

Таким образом, разобрав основные вопросы правового регулирования защиты персональных данных работников, приняв во внимание научные доводы и факты, действующее законодательство, судебную и правоприменительную практику, выявив пробелы, коллизии, практические проблемы, и составив рекомендации по их устранению, считаем цель настоящего исследования достигнутой.

В связи с принятием Закона № 152-ФЗ и последующими изменениями ТК РФ регулирование отношений, связанных с обработкой персональных данных работников, значительно приблизилось к уровню международных стандартов в этой области, однако, остались проблемные места, в частности, обозначенные в настоящей работе, которые законодателю еще предстоит исправить.

Подводя итог вышесказанному, необходимо отметить следующее. Проблемы правового обеспечения безопасности обработки персональных данных, на которые обращено внимание в работе, не являются полными и всеобъемлющими.

По мнению автора, проведенное исследование позволяет сделать вывод о том, что законодатель заложил основы регулирования персональных

данных и начал создавать рычаги для безопасности их обработки в сети Интернет.

В процессе разработки направлений совершенствования правового регулирования защиты персональных данных в Российской Федерации нужно исходить из того, что отсутствие теоретических исследований в данной области приводит к тому, что развитие законодательства идет по пути заполнения существующих пробелов и устранения имеющихся недостатков, но не по пути опережающего и направляющего воздействия на новые, формирующиеся в демократическом обществе, отношения.

Список используемой литературы

1. Конституция РФ (принята всенародным голосованием 12.12.1993) (в ред. от 21.07.2014) // Собрание законодательства РФ, 04.08.2014, № 31, ст. 4398.

2. Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948) // Российская газета, № 67, 05.04.1995.

3. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (в ред. от 01.04.2019) // Российская газета, № 256, 31.12.2001.

4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (в ред. от 31.12.2017) // Российская газета, № 165, 29.07.2006.

5. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) // Собрание законодательства РФ, 03.02.2014, № 5, ст. 419.

6. Regulation (EU) 2016/679 of the European Parliament and of the Council of April 2016 «On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing // Official Journal. L 119. 4/05/2016. P. 0001 - 0088.

7. Directive 95/46/EC (General Data Protection Regulation). URL: http://ec.europa.eu/justice/data- protection/reform/files/regulation_oj_en.pdf.

8 Директива № 95/46/4 ЕС Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» (Принята в г. Люксембурге 24.10.1995) (Документ опубликован не был) // СПС «КонсультантПлюс».

9. Александрова Н.В., Иванов Н.В. Совершенствование законодательных основ права собственности на недвижимое имущество // Актуальные проблемы юридической науки и правоприменительной практики: сборник материалов VI международной научно-практической

конференции, посвященной 25-летию юридического факультета. Чебоксары, 2016. С. 75-80.

10. Александрова Н.В., Федоров И.З. Реализация прав граждан на справедливое судебное разбирательство в гражданском процессе // Вестник Российского университета кооперации. 2015. № 4 (22). С. 82-85.

11. Алексеева Е.В. Гарантии защиты персональных данных работника в современном российском законодательстве // К познанию права. 2018, № 3. С. 42-48.

12. Богатыренко З.С. Новейшие тенденции защиты персональных данных работника в российском трудовом праве // Трудовое право. 2016. № 10. С. 29-51.

13. Бундин М.В. Неприкосновенность частной жизни и защита персональных данных // Инновации в государстве и праве России. 2017, № 1. С. 277-284.

14. Важорова М.А. Проблемы совершенствования системы обеспечения защиты персональных данных // Актуальные вопросы российского права и проблемы правоприменения в условиях современности. 2015. №1. С. 38-40.

15. Вельдер И.А. Практика защиты персональных данных в странах Европейского Союза: роль национальных административных и судебных органов // Интеллектуальная собственность и ее исследователь. 2015. № 3. С. 171-178.

16. Веселова А.Б. Защита персональных данных работников / Трудовые споры. 2016, № 10. С. 33-46.

17. Ветров Д.М. Защита персональных данных и защита информации на предприятии. Некоторые спорные вопросы применения // Проблемы права. 2016, № 1. С. 114-121.

18. Волчинская Е.К., Дятленко В.В. Законодательство о защите персональных данных: проблемы и решения // Информационное право. 2016, № 1 (4). С. 11-16.

19. Выскребцев Б.С. Проблема реализации права работника на защиту персональных данных // Проблемы современного российского права. 2015. № 6 С. 69-71.

20. Гаврюшина Н.И. Проблемы правовой защиты персональных данных // Актуальные вопросы современного российского права. 2015. № 1. С. 158-161.

21. Ганижев А.Я. Формирование информационного права и его влияние на защиту персональных данных работника // Эффективность правового регулирования общественных отношений в России. 2017. № 2. С. 120-122.

22. Горев А.И. Защита прав субъектов персональных данных в информационном обществе // Международные юридические чтения. 2017, № 2. С. 117-122.

23. Гуляева Е.Е. Международно-правовые проблемы защиты персональных данных // Актуальные проблемы современного международного права. 2018. № 2. С. 110-117.

24. 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. 2015. №1. С. 64-69.

25. Зайцева Л.В. Юридическая ответственность в области защиты персональных данных работников // Вестник НГУ. 2016. № 2. С. 84-87.

26. Идрисов И.Д. Правовое регулирование защиты и обработки персональных данных в электронной коммерции // Актуальные проблемы юридической науки и правоприменительной практики. 2018. № 1. С. 180-184.

27. Кадацкая Т.А. Защита персональных данных как одна из составляющих информационной безопасности граждан / Современный мир: безопасность и права человека. 2016. № 2. С. 135-139.

28. Крушина А.С. Право на защиту персональных данных // Современные проблемы юридической науки. 2014. № 1. С. 289-290.

29. Лушников А.М. Защита персональных данных работника: сравнительно-правовой комментарий гл. 14 ТК РФ // Трудовое право. - 2018. - № 10 (116). - С. 77-82.

30. Майер-Шенбергер В., Кукьер К. Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим. Москва: Манн, Иванов и Фербер, 2014.

31. Малеина М.Н. Право на тайну и неприкосновенность персональных данных // Журнал российского права. - 2017. - № 11. - С. 19-24.

32. Малышева И.В. Механизм правового регулирования: учебное пособие. - Новокузнецк: ФКОУ ВО «Кузбасский институт ФСИН России», 2016. - 52 с.

33. Марченко М.Н., Дерябина Е.М. Право Европейского Союза. Вопросы истории и теории. – М.: Проспект, 2016. - 308 с.

34. Международная и внутригосударственная защита прав человека. Учебное пособие для вузов / Отв. ред. Р.М. Валеев, Р.Г. Вагизов. - Казань: Казанский государственный университет им.В.И. Ульянова-Ленина, 2017. - 674 с.

35. Международная и внутригосударственная защита прав человека: Учебник / под ред. Р.М. Валеева. - М.: Статут, 2014. - 830 с.

36. Назаров Б.Л. Права человека: история, теория и практика: Учебное пособие. - Москва: Русспит, 2015.

37. Наумов В.Б. Персональные данные в соцсетях и социальных медиа: правовые проблемы защиты и использования // Закон. – 2018. – № 5. – С. 119 - 125.

38. Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет. Под редакцией А.С. Дупан (Гутниковой). Москва: Издательский дом Высшей школы экономики, 2016.

39. Ожегов С.И. Словарь русского языка / Под ред. Н.Ю. Шведовой. 22-е изд. стер. М., 2015.

40. Пазюк А., Соколова М. Защита персональных данных: введение в проблематику: учебное пособие. Минск, 2015. – 116 с.

41. Паризер Э. За стеной фильтров. Что Интернет скрывает от вас? М.: Альпина Бизнес Букс, 2016 - 304 с.

42. Параскевов А.В., Левченко А.В., Кухоль Ю.А. Сравнительно-правовой анализ правового регулирования защиты персональных данных в России и за рубежом // Научный журнал КубГАУ. – 2015. - №110 (06).

43. Петров М.И. Комментарий к Федеральному закону «О персональных данных» (постатейный). - М.: ЗАО Юстицинформ, 2017.

44. Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. М.: Статут, 2016.

45. Поливанов Г. Всевидящее око: частная жизнь сотрудников // Консультант. - 2016. - № 21. – С. 34-37.

46. Постникова Е.В. Некоторые аспекты правового регулирования защиты персональных данных в рамках внутреннего рынка Европейского Союза // Право. Журнал Высшей школы экономики. - 2018. - № 1.

47. Право европейского союза в 2 ч. Часть 1 : учебник и практикум для бакалавриата и магистратуры / А. Х. Абашидзе [и др.] ; под ред. А. Х. Абашидзе, А. О. Иншаковой. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 293 с. — (Серия : Бакалавр и магистр. Академический курс). — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/441944 (дата обращения: 07.05.2019).

48. Право Европейского Союза в вопросах и ответах: учеб. пособие / С.Ю. Кашкин [и др.]; отв. ред. С.Ю. Кашкин. - М.: ТК Велби, Изд-во Проспект, 2015. - 304 с.

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». 2018. № 1. С. 248-251.

50. 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. 2015. № 3. С. 213-215.

51. 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. 2018. - 146 с.

52. Просвирнин Ю.Г. Защита персональных данных / Вестник Воронежского государственного университета. 2018. № 2 (5). С. 174-188.

53. Прытков Ю. Правовое регулирование общественных отношений в сфере защиты персональных данных на территории РФ / Актуальные проблемы правовой теории и практики. 2017. № 1. С. 186-191.

54. Терехова Т.А. Место правового регулирования СМИ в европейском информационном праве // Вопросы современной юриспруденции: сб. ст. по матер. XXXVIII междунар. науч.-практ. конф. – Новосибирск: СибАК, 2017. - № 6 (38).

55. Терещенко Л.К., Тиунов О.И. Правовой режим персональных данных // Журнал российского права. – 2016. - № 12.

56. Тотьев К.Ю. Конкурентное право (правовое регулирование конкуренции). Учебник. – М.: Издательство РДЛ, 2017. - 352 с.

57. Цадыкова Э.А. Гарантии охраны и защиты персональных данных человека и гражданина / Конституционное и муниципальное право. 2017. № 14. С. 15-18.

58. Челнокова Г.Б. Проблемы защиты персональных данных в рамках трудовых отношений // Право и государство: теория и практика. 2017. № 9. - С. 65-70.

59. Шахов Н. Отношения по охране частной жизни и информации о частной жизни как объект теоретико-правового исследования. Ростов-на Дону, 2018.

60. Albea, S. D. Commentary: Security, Interests in Deposit Accounts and the Banking Industy’s Use of Setoff / S. D. Albea. — M. : Law Reviw Fall, 2012.

61. Bova, I. Effective protection of the financial and legal institution of banking secrecy as a guarantor of the development of the country's economy // Jurisprudence: problems and prospects: proceedings of the Intern. extramural scientific conf. - Perm: Mercury, 2012.

62. Keen, A. Nothing personal: How social networks, search engines and special services use our personal data / Andrew Keen. - M .: Alpina Digital, 2015 .- - 321 p.

63. Lewalle, J. Introduction to data analysis using continuous wavelet transform / Lewalle J . - LA: Oracle, 2018. - 490 c.

64. Report on Banking Secrecy. Anti-Fraud and Anti-Money Laundering Committee and Fiscal Committee. The European Banking Federation. Brussels. April, 2014 // European Banking Federation. — Режим доступа: http://www.ebf-fbe.eu/wp-content/uploads/2014/03/Bk_secrecy_Report04-2004-02083-01-E.pdf.

65. Data Localization in Russia (2015) // ECIPE (http://ecipe.org/publications/data-localisation-russia-self-imposed-sanction/).

66. Lawyer faactivist slaps global platforms with $8 billion GDPR lawsuits // Global Legal Post URL: http://www.globallegalpost.com/big-stories/lawyer-activist-slaps-global-platforms-with-$8-billion-gdpr-lawsuits-94806240.

67. Refining the EU Merger Control System // European Commission URL: https://ec.europa.eu/commission/commissioners/2014-2019/vestager.

68. US consumers more willing to share data than Europeans // Phocus Wire URL: https://www.phocuswire.com/US-consumers-more-willing-to-share-data-than-Europeans.

69. Volume of data/information created worldwide from 2005 to 2025 (in zetabytes) // Statista URL: https://www.statista.com/statistics/871513/worldwide-data-created.