Федеральное государственное научно-исследовательское учреждение
«Институт законодательства и сравнительного правоведения
при Правительстве Российской Федерации»

На правах рукописи

Бундин Михаил Вячеславович

ПЕРСОНАЛЬНЫЕ ДАННЫЕ В СИСТЕМЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Специальность: 12.00.13 – информационное право

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук, профессор
Терещенко Людмила Константинова

Москва – 2017

СОДЕРЖАНИЕ

Введение…… 3

Глава 1. Понятие и содержание персональных данных …… 14

1.1. Юридическая природа персональных данных ……. 14

1.2. Понятие и признаки персональных данных ……. 29

1.3. Содержание и виды персональных данных …….. 58

Глава 2. Персональные данные как информация ограниченного доступа…… 72

2.1. Понятие и система информации ограниченного доступа ……,. 72

2.2. Правовой режим персональных данных как информации ограниченного доступа ……..…… 93

2.3. Конфиденциальность как элемент правового режима персональных данных ……..…… 112

Глава 3. Формирование российского и зарубежного законодательства о персональных данных …… 130

3.1. Современные тенденции развития законодательства о персональных данных в зарубежных странах ……. 130

3.2. Особенности формирования российского подхода к правовому регулированию персональных данных ……..… 175

Заключение…… 192

Библиографический список…….. 195

ВВЕДЕНИЕ

Актуальность темы исследования. Обеспечение интересов личности, ее прав и свобод в процессе формирования в России информационного общества является первостепенной задачей современного государства. Широкое использование современных информационных технологий, в частности: технологий больших данных, облачных вычислений, интернета вещей, искусственного интеллекта и других, привносит не только удобство и комфорт в нашу жизнь, но и формирует новые вызовы и угрозы, такие как реальная угроза неконтролируемого накопления и обработки данных об индивиде, которые затем потенциально могут быть использованы негативным или нежелательным для него образом. Дальнейшее повсеместное распространение современных информационных технологий может привести к тому, что сам факт существования частной жизни окажется под угрозой. С учетом сказанного формирование адекватного правового режима персональных данных является важной гарантией прав личности, позволяющей контролировать обработку информации о себе и, в первую очередь, определять порядок и условия доступа к ней. Таким образом, институт персональных данных становится важным элементом правового статуса личности, направленным на обеспечение ее информационной безопасности.

Правовое регулирование персональных данных и вопросов доступа к ним имеет существенное значение для государства, для коммерческих структур и для экономики в целом. Внедрение современных технологий обработки информации является необходимым фактором социального и экономического развития страны, остановить которое представляется практически невозможным, с другой стороны, эти процессы сопровождаются ростом количества информационных систем и объемов данных, содержащихся в них, в том числе и персональных данных. Фактически развитие цифровой экономики и электронного государства, которые часто называются в числе приоритетных направлений государственной политики

не только в России, но и за рубежом, во многом будет зависеть от того, каким будет правовой режим персональных данных и его основные параметры, и в первую очередь – с точки зрения доступа к ним и условий их обработки. Установление избыточных требований к обеспечению конфиденциальности персональных данных, как информации ограниченного доступа, или ограничивающих доступ к ним, может привести к крайне негативным последствиям для экономики и государства, в особенности в тех сферах, где предоставление товаров и услуг напрямую связано с необходимостью автоматизированной обработки персональных данных (государственные и муниципальные услуги, услуги связи, образование, здравоохранение, транспорт и др.).

Проблемы защиты персональных данных и поиска баланса интересов личности, государства и общества не раз отмечались в действующих программных документах. Например, государственная программа «Информационное общество 2011–2020»[1] прямо называет угрозу «неконтролируемого роста объемов информации о гражданах и отсутствие эффективных механизмов контроля ее использования, прежде всего в государственных информационных системах», в качестве наиболее актуальных угроз современного российского общества. Новая редакция Доктрины информационной безопасности Российской Федерации[2] также отмечает существенный рост преступлений против неприкосновенности частной жизни, личной и семейной тайны при обработке персональных данных с использованием информационных технологий. Действующая Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы[3] при рассмотрении вопросов защиты данных и информации указывает на «необходимость соблюдения баланса между своевременным

[1] Утверждена Распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-р г. Москва «О государственной программе Российской Федерации “Информационное общество (2011–2020 годы)”» // Российская газета. – 2010. – 6 нояб.

[2] Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 // Российская газета. – 2016. – 6 дек.

[3] Утверждена Указом Президента Российской Федерации от 9 мая 2017 г. № 203 // Российская газета. – 2017. – 10 мая.

внедрением современных технологий обработки данных с защитой прав граждан, включая право на личную и семейную тайну».

Актуальность темы исследования подтверждают и материалы судебной практики по спорам о нарушении прав субъектов персональных данных как в Российской Федерации, так и в странах Евросоюза и США, при этом отчетливо прослеживается тенденция на увеличение числа таких споров.

В этой связи представляется крайне важным и значимым комплексное изучение и дальнейшее теоретическое осмысление сущности и правового режима персональных данных, особенностей их правового регулирования как информации ограниченного доступа и определения места персональных данных в существующей системе информации ограниченного доступа, на основе чего сформулированы научно обоснованные предложения по совершенствованию законодательства и правоприменительной практики в указанной области.

Степень научной разработанности темы исследования. Проблемные вопросы формирования и реализации применения законодательства о персональных данных в России и зарубежных странах были рассмотрены в диссертационных исследованиях Н.Г. Белгородцевой, И.А. Вельдера, А.В. Дворецкого, А.В. Кучеренко, Н.И. Петрыкиной, О.Б. Просветовой, Ю.С. Телиной, А.С. Федосина.

Существенное внимание проблемным вопросам защиты права на уважение частной жизни и регулированию оборота информации ограниченного доступа, в том числе и персональных данных, уделено также в трудах таких ученых, как: А.Б. Агапов, А.А. Антопольский, А.Г. Арешев, И.Л. Бачило, Е.К. Волчинская, Р.Б. Головкин, О.А. Городов, А.А. Ефремов, В.П. Иванский, В.Н. Лопатин, В.А. Мазуров, А.В. Морозов, В.Б. Наумов, Т.А. Полякова, М. Савинцева, И.В. Смолькова, А.А. Стрельцов, Л.К. Терещенко, Ю.В. Травкин, А.А. Фатьянов и др.

Тем не менее в научно-правовой литературе до настоящего времени отсутствуют комплексные исследования проблематики соотнесения

правового режима персональных данных с существующими правовыми режимами информации ограниченного доступа, что не позволяет сформировать единые подходы к правовому регулированию вопросов обеспечения конфиденциальности персональных данных.

Объект исследования – общественные отношения, связанные с обработкой персональных данных.

Предметом исследования являются правовые нормы, материалы правоприменительной практики, научные доктрины, отражающие эволюцию представлений, идей и концепций о сущности и содержании персональных данных и их правового режима как информации ограниченного доступа в России и за рубежом, их месте в системе информации ограниченного доступа.

Цель диссертационного исследования заключается в выработке и обосновании теоретических положений, имеющих значение для развития института персональных данных и определения их места в системе информации ограниченного доступа.

В рамках поставленной научной проблемы решаются следующие научные **задачи**, определившие логику диссертационного исследования и его структуру:

– сформулировать на основе изучения российского и зарубежного законодательства и практики актуальное определение понятия «персональные данные»;

– определить юридическую природу персональных данных и их взаимосвязь с правами и свободами личности, и прежде всего – с правом на неприкосновенность частной жизни, личную и семейную тайну;

– провести классификацию персональных данных, в зависимости от режима доступа к ним;

– исследовать существующую систему информации ограниченного доступа в российском законодательстве и праве с целью определить в ней место персональных данных;

– определить особенности, содержание и структуру правового режима персональных данных как информации ограниченного доступа.

Методологическую основу исследования составили как общенаучные, так и специальные юридические методы познания. К числу основных используемых в исследовании общенаучных методов следует отнести общелогические методы: диалектический, системно-структурный, формально-логический. Среди специальных юридических методов автором использовались: формально-юридический, историко-правовой и сравнительно-правовой методы.

Теоретическую основу диссертационного исследования составили научные и научно-методические труды по общей теории государства и права, административного и информационного права. В своей работе автор использовал труды таких ученых-юристов, как: А.Б. Агапов, С.С. Алексеев, А.А. Антопольский, А.Г. Арешев, В.М. Баранов, Ю.М. Батурин, Д.Н. Бахрах, И.Л. Бачило, Л. Брандейс, Г. Бребант, А.Б. Венгеров, И.А. Вельдер, Е.К. Волчинская, Р.Б. Головкин, В.П. Иванский, В.А. Копылов, Л.О. Красавчикова, П.У. Кузнецов, М.А. Лапина, В.Н. Лопатин, В.А. Мазуров, А.В. Малько, М.Н. Марченко, Н.И. Матузов, А.В. Минбалеев, А.В. Морозов, В.Б. Наумов, В.Б. Рушайло, И.В. Смолькова, Э.В. Талапина, Л.К. Терещенко, Ю.А. Тихомиров, Б.Н. Топорнин, Ю.В. Травкин, С. Уоррен, А.А. Фатьянов, М.А. Федотов, Т.Я. Хабриева, Л.С. Явич.

Нормативная база исследования представлена Конституцией Российской Федерации, федеральными конституционными и федеральными законами, в частности: Федеральным законом «Об информации, информационных технологиях и о защите информации» и Федеральным законом «О персональных данных», указами Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации, приказами федеральных органов исполнительной власти (Роскомнадзор, ФСТЭК России) и иными нормативными правовыми актами и документами органов государственной власти Российской Федерации и ее

субъектов, затрагивающих вопросы обработки и обеспечения конфиденциальности персональных данных. Существенное внимание в работе уделяется изучению международных правовых актов, среди которых особое место занимают нормативно-правовые акты Совета Европы и Европейского союза. Помимо вышеуказанных актов правовую основу исследования составили также нормативные правовые акты, регулирующие вопросы защиты персональных данных таких стран, как США, Франция, Германия, Дания, Швеция и др.

Эмпирическую базу исследования составили материалы российской и зарубежной судебной практики, практики Европейского суда по правам человека по рассматриваемой проблематике, аналитические и статистические материалы международных организаций – Совета Европы, Европейского союза, Организации по экономическому сотрудничеству (ОЭСР); материалы правоприменительной практики по реализации законодательства о персональных данных в России и зарубежных странах.

Научная новизна исследования определяется разработкой и решением научной задачи, имеющей теоретическую и практическую значимость, и заключается в расширении научных представлений о правовых режимах персональных данных и их соотношении с существующими правовыми режимами информации ограниченного доступа.

В диссертации впервые разработана целостная научно-правовая концепция применимых правовых режимов персональных данных и их месте в системе информации ограниченного доступа.

Научная новизна диссертационного исследования, свидетельствующая о личном вкладе автора в науку, состоит также в сформулированных теоретических и практических положениях, выносимых на защиту.

На защиту выносятся следующие положения:

1. В целях совершенствования существующего понятийного аппарата предлагается авторское определение понятия «персональные данные»:

персональные данные – сведения о физическом лице или относящиеся прямо или косвенно к определенному или определяемому на основании таких сведений физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, а также другая информация, которая, как правило, представлена в формализованном виде, обеспечивающем возможность их обработки в информационных системах, преимущественно с помощью средств автоматизации, полностью или частично.

2. Для отграничения персональных данных от иных видов информации обосновывается использование в качестве основного признака персональных данных наличие взаимосвязи между субъектом и содержанием соответствующей информации о нем. Такая связь может быть очевидной через прямое указание на субъекта данных с использованием идентифицирующей информации, либо она может быть потенциально установлена. В качестве дополнительного признака персональных данных следует рассматривать их формализованный характер, т.е. обусловленный целями и задачами обработки в информационной системе набор сведений, и их связь с информационной системой.

3. В целях упорядочения существующих представлений о месте правового режима персональных данных среди иных режимов информации обоснован вывод об отсутствии единого правого режима персональных данных, поскольку они могут находиться как в режиме общедоступной информации, так и в режиме информации ограниченного доступа. Применительно к персональным данным в режиме информации ограниченного доступа следует выделить особо «правовой режим конфиденциальности персональных данных», который имеет собственное содержание и распространяется на случаи обработки персональных данных на условиях соблюдения конфиденциальности (за исключением государственной тайны). Режим конфиденциальности персональных данных,

в свою очередь, включает в себя режим особых категорий персональных данных и режим биометрических персональных данных, каждый из которых также имеет свои особые параметры.

4. Обосновывается вывод, что конфиденциальность персональных данных представляет собой установленное законодательством требование, обращенное исключительно к оператору, обработчику персональных данных, органу по защите персональных данных, работнику оператора, а также иному лицу, т.е. конфидентам, получившим к персональным данным доступ на законном основании. Конфиденциальность, как обязательное требование, возникает с момента получения доступа к персональным данным конфидента, в отсутствие у него законных оснований для обработки их в режиме общедоступной информации.

5. В целях устранения возникающих коллизий, связанных с соотнесением правового режима конфиденциальности персональных данных с иными правовыми режимами конфиденциальной информации, такими как: врачебная тайна, тайна связи, адвокатская, нотариальная, банковская тайны и др., обосновывается необходимость закрепления в Федеральном законе «О персональных данных» коллизионной нормы-правила, которая бы установила приоритет требований режима конфиденциальности персональных данных, которые должны быть выполнены конфидентами, в условиях, когда иными режимными требованиями предусматривается более низкий уровень защищенности информации.

6. Для разрешения возникающих в правоприменительной практике проблем автором предлагается использование и прямое закрепление в законодательстве положения о «презумпции конфиденциальности персональных данных» в качестве одного из принципов, предусмотренных статьей 5 Федерального закона «О персональных данных».

7. Обоснованы целесообразность и возможность дальнейшего развития правомочий субъекта персональных данных в ответ на появление новых угроз правам и свободам личности. Таковым следует считать «право на

забвение», имеющее в то же время собственное содержание, которое заключается в праве субъекта персональных данных требовать от оператора поисковой системы прекратить индексирование информации о себе (т.е. выдачу ссылок на нее по запросу пользователя поисковой системы), размещенной в информационно-коммуникационной сети Интернет, и которая распространяется с нарушением законодательства, является недостоверной или неактуальной.

Теоретическая значимость исследования состоит в том, что автор в своем исследовании формулирует теоретические положения, определяющие сущность и содержание правового режима персональных данных как информации ограниченного доступа, обусловленные их юридической природой и состоянием законодательства в этой сфере, а также положения, характеризующие место персональных данных в системе информации ограниченного доступа. Отдельное внимание автором уделяется совершенствованию понятийного аппарата в рассматриваемой сфере.

Материалы диссертации в части определения перспектив и существующих тенденций развития правового института персональных данных в России и за рубежом могут служить теоретической основой для совершенствования законодательства в данной сфере, а также стать предметом самостоятельных научных исследований в этой области и области смежных юридических наук.

Практическая значимость исследования заключается в разработке и формулировании конкретных предложений по совершенствованию существующего законодательства о персональных данных, в частности положений Федерального закона «О персональных данных». Результаты исследования могут быть использованы для преподавания в рамках программ бакалавриата и специалитета курсов «Информационное право», «Информационные технологии в юридической деятельности», «Основы информационной безопасности», специальных магистерских курсов, связанных с темой диссертации, и других дисциплин профессионального

цикла программ основного и дополнительного образования, где изучаются такие вопросы, как: информационная безопасность личности, защита частной жизни, защита персональных данных, конфиденциальность информации, правовые режимы информации ограниченного доступа и др.

Степень достоверности и апробация результатов исследования. Основные теоретические и практические выводы, сформулированные в результате проведенного исследования, были:

– обсуждены на заседаниях отдела административного законодательства и процесса, секции публичного права, круглых столах Института законодательства и сравнительного правоведения при Правительстве РФ (22 мая 2017 г., 17 марта 2017 г., 15 октября 2015 г.);

– отражены в публикациях автора по теме исследования, имеющих как научную, так и учебную направленность (из них 3 статьи – в изданиях, включенных в перечень рекомендованных ВАК Минобрнауки РФ, и 5 публикаций, включенных в международную базу научного цитирования Scopus).

Основные выводы и результаты исследования были представлены автором на различных конференциях: Международная конференция по теории и практике электронного правительства (ICEGOV) (7–9 марта 2017 г., г. Нью Дели, Индия; 1–3 марта 2016 г., г. Монтевидео, Уругвай; 27–30 октября 2014 г., г. Гимарайнш, Португалия); Международная конференция по цифровому правительству (Dg.o) (8–10 июня 2016 г., г. Шанхай, КНР; 27–30 мая 2015 г., г. Финикс, США); Международная конференция «Цифровые трансформации и глобальное общество» (DTGS) (21–23 июня 2017 г., Санкт-Петербург; 22–24 июня 2016 г., Санкт-Петербург); Международная конференция «Киберпространство» (27–28 ноября 2015 г., Университет Масарика, г. Брно, Чехия); Международная школа-практикум молодых ученых-юристов Института законодательства и сравнительного правоведения при Правительстве РФ (23–24 мая 2013 г., Москва; 26–28 мая 2010 г., Москва).

Кроме того, отдельные выводы исследования были изложены в научных докладах и обсуждены в ходе неоднократного участия автора в Международной летней школе по киберправу (ISSC) (6–10 июля 2015 г.; 30 июня – 4 июля 2014 г.; 1–5 июля 2013 г.; 2–6 июля 2012 г., Москва, Национальный исследовательский университет «Высшая школа экономики»).

Апробация и внедрение результатов реализовывались через научно-педагогическую деятельность автора на кафедре административного и финансового права юридического факультета Федерального автономного образовательного учреждения высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского» в рамках проведения практических занятий по дисциплинам: «Информационное право», «Информационные технологии в юридической деятельности», «Основы информационной безопасности», где были использованы выводы и результаты, изложенные в публикациях автора.

Структура диссертации в соответствии с поставленными целями и задачами исследования включает в себя: введение, три главы из восьми параграфов, заключение, библиографию.

ГЛАВА 1. ПОНЯТИЕ И СОДЕРЖАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1. Юридическая природа персональных данных

Возникновение персональных данных как категории в информационном праве и праве в целом тесно связано с идеей защиты частной жизни, которая в условиях развития информационного общества все чаще подвергается различного вида угрозам. Именно желание обеспечить должный уровень защиты личности от информационных угроз привело к идее контроля над оборотом информации об индивидах – персональных данных, выделив их в особый вид информации, требующей защиты.

В этой связи говорить о юридической природе персональных данных, не рассматривая их в ракурсе соотношения с категорией права на неприкосновенность/уважение частной жизни, по мнению автора, невозможно.

В настоящее время право на защиту информации о частной жизни, равно как и необходимость уважения частной, личной сферы жизни индивида, равно как и право индивида на защиту информации о нем (персональных данных) считаются неотъемлемыми правами любого человека, что было не всегда.

Упоминание частной сферы жизни индивида как таковой есть еще у Аристотеля[1], но в своеобразной трактовке – как возможность доступного лишь философам отрешения от богов и общества. Предполагалось, что остальные граждане живут для государства, а обеспеченная трудом рабов частная жизнь является лишь средством исполнения гражданином обязанностей. В средние века в условиях феодализма в обществе всеобщей зависимости и жесткого традиционализма частная жизнь определялась во многом сословным положением. В целом, человек в то время не разделял или, по крайней мере, не проводил четкого различия, когда он выступает в качестве «публичного лица» или же как «частное лицо». В частности,

[1] Аристотель. Политика / Соч.: в 4 т. /Аристотель. – М.: Мысль, 1994. – Т. 4. – С. 398–400.

государственные и городские служащие часто обязаны были носить свои мантии как повседневную одежду, которая говорила об их статусе и роли в обществе. Что касается более высокопоставленных особ, то в их случае они выполняли свои «публичные» обязанности постоянно, с утра и до вечера[1].

Идея противопоставления публичной и частной жизни индивида, а равно идея необходимости уважения последней, связана с теорией естественного права, где основной посылкой является неотъемлемое право на владение самим собой (своим телом), физической свободой и своим имуществом.

Впервые о необходимости уважения частной жизни индивида было заявлено в 1890 году, когда американские адвокаты Самуэль Уоррен и Луи Брандейс опубликовали в журнале Harvard Law Review статью The Right to Privacy[2], в которой они обосновали необходимость судебной защиты частной жизни от вторжения, подобно тому, как защищается доброе имя от клеветы и навета. Вскоре после публикации отдельные штаты постепенно стали принимать гражданско-правовые нормы о защите частной жизни как нематериального блага. Другие страны также достаточно быстро восприняли эту идею, хотя невозможно предположить, что в них не обсуждались или не рассматривались аналогичные проблемы до появления названной статьи. Одним из первых законодательных актов на Европейском континенте стал Гражданский кодекс Германии 1900 года[3], который оказал существенное влияние на появление схожих положений о защите частной жизни в законодательстве европейских стран.

Мировое звучание идея уважения частной жизни получила с принятием Всеобщей декларации прав человека[4] и Международного пакта о

---

[1] Beigner, B. La protection de la vie privee / B. Beigner // Libertes et Droits fondamentaux. – Paris: Dalloz, 2003. – P. 160.

[2] Warren, S.D. Right To Privacy / S.D. Warren, L.D. Brandeis // Harvard Law Review. – 1890. – 10 December. – No. 5. – Vol. IV. – (http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm). – Дата обращения: 2.04.2017.

[3] Beigner, B. La protection de la vie privee / B. Beigner // Libertes et Droits fondamentaux, Dalloz. – Paris, 2003. – P. 160.

[4] Всеобщая декларация прав человека. Принята Резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года. – (http://www.un.org/ru/documents/decl_conv/declarations/declhr). – Дата обращения: 2.04.2017.

гражданских и политических правах[1]. После этого практически во всех международных документах, содержащих положение об основных правах человека, уже традиционно указывается и право на уважение (неприкосновенность) частной жизни.

Однако всеобщее признание никак не приводит к решению многочисленных практических и юридических трудностей, которые не так-то просто разрешить. Самым главным вопросом по-прежнему остается вопрос о юридическом содержании права на неприкосновенность частной жизни, а также само понятие частной жизни.

Одни ученые приходят к выводу о том, что право на уважение/неприкосновенность частной жизни напрямую взаимосвязано со свободой выражения своего мнения, свободой мысли, совести и религии, свободой ассоциаций и собраний, правом на свободу, правом на справедливое разбирательство, правом создавать семью. Во многом эти авторы, таким образом, объединяют при рассмотрении положения статей 8 и 12 Европейской конвенции о защите прав человека и его основных свобод право на уважение частной и семейной жизни, жилища и корреспонденции и право на вступление в брак и создание семьи[2].

Другие авторы относят к содержанию права на уважение/неприкосновенность частной жизни право располагать собой, право на тайну частной жизни и тайну корреспонденции, право на защиту личности и право на уважение к личному статусу[3].

Значительная часть зарубежных авторов рассматривает право на частную жизнь как определенную неотъемлемую составляющую права/прав на личность (droit/droits de la personalité. – *Фр.*), к которым в равной степени относятся: право на жизнь, личную неприкосновенность, на уважение своего

---

[1] Международный пакт о гражданских и политических правах. Принят Резолюцией 2200 А (XXI) Генеральной Ассамблеи ООН от 16 декабря 1966 года. – (http://www.un.org/ru/documents/decl_conv/conventions/pactpol). – Дата обращения: 2.04.2017.

[2] Гомьен, Д. Европейская конвенция о правах человека и Европейская социальная хартия: право и практика / Д. Гомьен, Д. Харрис, Л. Зваак. – М.: Изд-во МНИМП, 1998. – С. 290.

[3] Люшер, Ф. Конституционная защита прав и свобод личности / Ф. Люшер. – М.: ИГ Прогресс, 1993. – С. 91.

имени, чести, достоинства, частной жизни[1]. В таком контексте право на частную жизнь тесно связывают с правом на собственное изображение и голос, а также все то, что индивидуализирует человека и отличает его от других. Есть и другие, по-своему интересные точки зрения, к примеру, Н.Н. Лебедева в своем исследовании сводит право на неприкосновенность частной жизни к защите персональных данных[2].

Однако, обобщая в целом все существующие точки зрения, сложно не согласиться с мнением В.Н. Лопатина по поводу того, что «право на неприкосновенность частной жизни – это сложный по составу правовой институт, включающий в себя множество отдельных правомочий индивида»[3]. Причем перечень этих правомочий, которые указываются в многочисленных национальных и международных актах, нельзя считать исчерпывающим в связи с динамичным развитием отношений в этой сфере. В частности, Р.Б. Головкин, рассматривая право на неприкосновенность частной жизни как «естественное неотчуждаемое право человека на уединение и обособленное общение со своими близкими людьми, свободное от какого-либо произвольного вмешательства, обеспеченное государством и ограниченное морально-правовыми нормами»[4], приводит следующий перечень правомочий: «право на свободу семейных отношений; право на охрану тайны межличностных отношений частного свойства; право на блокирование информации (корреспонденции, телефонных переговоров, почтовых и телеграфных сообщений, Интернета, СМИ); право общения с другими индивидами: право на защиту от вредной информации; право на свободу совести и тайну исповеди»[5]. Другие авторы, например, А. Климчик[1],

---

[1] Beigner, B. La protection de la vie privee / B. Beigner // Libertes et Droits fondamentaux. – Paris: Dalloz, 2003. – P. 161–163.

[2] Лебедева, Н.Н. Биометрия и право на неприкосновенность частной жизни / Н.Н. Лебедева // Обеспечение прав граждан и интересы государства в современном обществе: Мат-лы науч.-практич. конф. (17–18 дек. 2004). – Муром, 2004. – С. 148

[3] Бачило, И.Л. Информационное право / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов. – СПб.: Юридический центр Пресс, 2005. – С. 220

[4] Головкин, Р.Б. Правовое и моральное регулирование частной жизни в современной России: дис. ... д-ра юрид. наук: 12.00.01 / Р.Б. Головкин. – Н. Новгород, 2005. – С. 117.

[5] Там же.

в основном относят к содержанию права на неприкосновенность частной жизни внутреннюю информационную свободу личности, т.е. право на охрану информации о себе и о своей частной жизни, а также право на личную и семейную тайну.

Представители англосаксонской правовой науки при определении права на частную жизнь в основном используют схожее понятие «прайвеси», или приватность (privacy. – *Англ.*), которое традиционно, начиная с уже упомянутой статьи Л. Брандейса[2], трактуется обычно, как право быть «оставленным в покое» (to be left alone. – *Англ.*).

В то же время, можно встретить и другие точки зрения, к примеру, Алан Уэстин определил «прайвеси» как желание человека свободно выбирать, при каких обстоятельствах и до какой степени он готов открыть себя, свои привычки и свое поведение людям[3]. Эдуард Блоуштайн указал на то, что «прайвеси» тесно связано с личностью человека и означает право на неприкосновенность личности, индивидуальную свободу, независимость человека, достоинство и целостность[4].

Другой известный исследователь, Р. Гэвисон, считает, что «прайвеси» состоит из трех элементов: секретности, анонимности и уединения. Это состояние, которое может быть утрачено как по желанию самого человека, так и в результате вмешательства извне[5].

В современной зарубежной литературе все чаще принято называть в качестве составляющих права на уважение частной жизни (right to privacy. – *Англ.*) – право на спокойствие частной жизни (to be left alone. – *Англ.*), право на частную бытовую жизнь, право на тайну частной жизни[6].

---

[1] Климчик, А. Свобода информации и право на частную жизнь в международном праве: дис. ... канд. юрид. наук: 12.00.10 / А. Климчик. – М., 2003. – С. 62.
[2] Warren, S.D. Right To Privacy / S.D. Warren, L.D. Brandeis // Harvard Law Review. –1890. – 10 December. – No. 5. – Vol. IV. – (http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm/). – Дата обращения: 2.04.2017.
[3] Westin, A.F. Privacy and Freedom / A.F. Westin. – New York: Atheneum, 1967. – P. 7.
[4] Bloustein, E. Privacy as an Aspect of Human Dignity / E. Bloustein // New York University Law Review. – 1964. No 39. – P. 971.
[5] Gavison, R. Privacy and the Limits of Law / R. Gavison // Yale Law Journal. – 1980. – No 89. – P. 421, 428.
[6] Beigner, B. La protection de la vie privee / B. Beigner // Libertes et Droits fondamentaux. – Paris: Dalloz, 2003. – P. 174

В целом на основе анализа законодательства и международных актов можно примерно назвать следующий перечень правомочий, которые так и или иначе могут быть отнесены к праву на неприкосновенность` частной жизни:

- право на свободу располагать собой;
- право на тайну частной жизни;
- право на тайну корреспонденции;
- право на свободу мысли;
- право на свободу совести;
- право на свободу вероисповедания;
- право на свободу выражения своего мнения;
- право на пользование родным языком;
- право на защиту личности, чести, достоинства и деловой репутации, национальной принадлежности; право на защиту жилища;
- право на тайну голосования.

Возвращаясь к самому понятию «частной жизни», сразу отметим, что и в этом вопросе с трудом можно найти четкие пределы указанной категории. Наиболее авторитетным источником в качестве возможного ориентира признается практика Европейского суда по правам человека (далее по тексту – Европейский суд), которая к тому же не так давно стала обязательна для следования российскими судами. Примечательно, что Европейский суд достаточно широко подходит к трактовке рассматриваемого понятия, называя ««частную жизнь» емкой категорией, которой невозможно дать исчерпывающего определения»[1]. «Очевидно, что эта категория шире, чем право на личную жизнь, и она касается таких сфер, внутри которых каждый человек волен развивать это понятие и наполнять его определенным

[1] Решение Европейского суда по правам человека по делу «Костелло-Робертс против Соединенного Королевства» (Costello-Roberts v. UK) от 25 марта 1993 г., № 13134/87. – (http://hudoc.echr.coe.int/eng#%7B%22fulltext%22:%5B%22№13134/87%22%5D,%22itemid%22:%5B%22002-9660%22%5D%7D). – Дата обращения: 02.04.2017.

смыслом»[1]. В 1992 г. Суд заявил, что «было бы непозволительно ограничить понятие [личной/частной жизни] «внутренним кругом», в котором может жить отдельный человек своей личной жизнью, которую он выбирает, и исключить оттуда целиком внешний мир, не входящий в этот круг. Уважение к личной/частной жизни должно также включать определенный набор прав для установления и развития взаимоотношений с другими аспектами жизни человека»[2]. Таким образом, понятие частной жизни очевидно включает в себя право на развитие взаимоотношений с другими лицами и внешним миром. В некоторых случаях Судом было признано, что деятельность профессионального и делового характера также может охватываться понятием личная (частная) жизнь, как это фактически было признано в деле *Нимиц*[3]. С недавних пор Суд отнес к числу таких отношений и экологическую безопасность личности, о чем он недвусмысленно высказался сразу в ряде судебных решений, из которых особое внимание привлекает дело *Лопез Остра*[4], в котором была установлена связь между ухудшением экологической обстановки и качеством жизни, в том числе и частной.

В российской науке, по мнению Р.Б. Головкина[5], доминирует институционально-позитивный подход, суть которого состоит в названии сфер жизни индивида, которые относятся к его «частной жизни» (например: интимные отношения, семейные отношения, досуг, общение, быт), что не совсем применимо к такой сложной и многогранной категории. В.М. Баранов[6] считает, что определение всей палитры отношений частной жизни вряд ли возможно и называет лишь основные ее признаки, как то:

---

[1] Там же.

[2] Решение Европейского суда по правам человека по делу «Нимиц против Германии» (Niemietz v. Germany) от 16 декабря 1992 г., № 13710/88. – (http://hudoc.echr.coe.int/eng#%7B%22fulltext%22:%5B%22№13710/88%22%5D,%22itemid%22:%5B%22001-661%22%5D%7D). – Дата обращения 02.04.2017.

[3] Там же.

[4] Решение Европейского суда по правам человека по делу «Лопез Остра против Испании» (Lopez Ostra v. Spain) от 9 декабря 1994 г., №16798/90. – (http://hudoc.echr.coe.int/eng#%7B%22fulltext%22:%5B%22№16798/90%22%5D,%22itemid%22:%5B%22002-10606%22%5D%7D). – Дата обращения 25.04.2013.

[5] Головкин, Р.Б. Правовое и моральное регулирование частной жизни в современной России: дис. ... д-ра юрид. наук: 12.00.01 / Р.Б. Головкин. – Н. Новгород, 2005. – С. 117.

[6] Баранов, В.М. Категория «частная жизнь» / Право граждан на информацию и защита неприкосновенности частной жизни / В.М. Баранов. – Н. Новгород, 1999. – С. 34–37.

особая сфера жизнедеятельности людей, степень открытости которой устанавливает сам индивид, зависящая от социально-психологических характеристик индивида, комплексное образование и т.д. Бернар Бенье[1] также признает тот факт, что в последнее время существует расширение содержания категории частная жизнь, которая перестает ограничиваться рамками скрытой или неизвестной другим сферы деятельности индивида, что стоит теперь разграничивать понятия «личная жизнь» и, по-видимому, более широкое – «частная жизнь», включающее, по его мнению, «частную общественную жизнь».

Рассматриваемые сложности в определении категории «частная жизнь» и «право на уважение частной жизни» не мешают подавляющему большинству авторов признавать, что частная и личная жизнь, как уже было отмечено, в условиях стремительно развивающихся информационных технологий все более находится под угрозой.

Особую озабоченность в подавляющем большинстве стран вызвали новые возможности для автоматизированной обработки данных об индивидах, вплоть до фактического принятия решений в рамках автоматизированных систем обработки данных без участия лица, и при этом имеющие серьезные юридические последствия для него. В качестве примера такой практики можно в полной мере считать очень распространенную теперь и в России практику привлечения к административной ответственности за различные рода нарушения Правил дорожного движения на основе данных автоматической фото- и видеофиксации[2]. В целях предотвращения многочисленных угроз правам и свободам человека, вызванных «манипулированием» данных о физических лицах, появились специальные нормы о защите последних путем ограничения их распространения и обработки. Впоследствии это стало как раз причиной появления новой правовой категории – «персональных данных» как особой

[1] Beigner, B. La protection de la vie privee / B. Beigner // Libertes et Droits fondamentaux. – Paris: Dalloz, 2003. – P. 172–173.
[2] Баршев, В. Лихачи попали в камеру / В. Баршев // Российская газета. – 2017. – 31 янв.

разновидности информации о физическом лице, с особым правовым режимом, необходимость которого была обусловлена серьезной потенциальной опасностью причинения вреда правам и свободам индивида при нарушении правил ее обработки.

В Европейских странах и США указанная категория была введена в обиход уже более 30 лет назад, первоначально как один из важных элементов защиты права на неприкосновенность/уважение частной жизни. На текущий момент законодательство о персональных данных принято более чем в 43 странах мира, которое во многих положениях схоже между собой[1]. Во всех этих случаях необходимость защиты персональных данных рассматривают как необходимый в современном обществе развитых информационных технологий элемент защиты прав и свобод личности. В то же время это, в свою очередь, породило вопрос о соотнесении указанных категорий.

В.Н. Лопатин прямо указывает на персональные данные как на институт охраны права на частную жизнь[2]. У других авторов, как правило, редко можно найти вопрос о соотнесении института защиты персональных данных и права на неприкосновенность частной жизни, хотя они, без сомнения, рассматривают эти понятия как связанные между собой.

На основании анализа международного и зарубежного опыта можно прийти к абсолютно аналогичному выводу. Возьмем, в частности, положения Рекомендаций Совета ОЭСР, касающихся основных положений о защите неприкосновенности частной жизни и международных обменов персональными данными[3], а равно и преамбулы Конвенции Совета Европы о защите личности в связи с автоматизированной обработкой данных[4] от 28

---

[1] Савинцева, М. Правовая защита персональной информации граждан в России / М. Савинцева // Законодательство и практика масс-медиа. – М., 2006. – № 9 (сент.). – С. 12–13.

[2] Бачило, И.Л. Информационное право / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов. – СПб.: Юридический центр Пресс, 2005. – С. 243.

[3] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. – (http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm). – Дата обращения: 02.04.2017.

[4] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в Страсбурге 28.01.1981) // Сайт компании «КонсультантПлюс». – (http://www.consultant.ru/document/cons_doc_LAW_121499/). – Дата обращения: 02.04.2017.

января 1981 года. В обоих случаях указывается в качестве цели гармонизации национального законодательства – укрепление гарантий прав личности, и прежде всего – права на неприкосновенность частной (личной) жизни индивида в условиях автоматизированной обработки данных о нем. Преамбула Директивы Европейского парламента и Совета ЕС 95/46/ЕС о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных[1] в п. 10 явно говорит о том, что предметом национального законодательства о персональных данных является защита фундаментальных прав и свобод, и прежде всего – права на частную жизнь. Европейский суд в своей практике, касающейся статьи 8 Конвенции о защите прав человека и его основных свобод, также признал, что защита персональных данных от разглашения является одним из важнейших элементов осуществления права личности на уважение личной и семейной жизни[2].

Российское законодательство первоначально не связывало напрямую защиту персональных данных и право на уважение/неприкосновенность частной жизни. К примеру, утративший силу Федеральный закон «Об информации, информатизации и защите информации»[3] в ст. 11, во многом ориентируясь на положения статьи 24 Конституции РФ, говоря о персональных данных, лишь указывал на недопустимость сбора сведений о частной жизни лица, а равно информации, нарушающей личную, семейную тайну, тайну переписки, телефонных и телеграфных сообщений физического лица, прямо не указывая, что целью защиты персональной информации является защита права на неприкосновенность частной жизни и других прав и свобод.

---

[1] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Дата обращения: 02.04.2017.

[2] Килкэли, У. Европейская конвенция о защите прав человека и его основных свобод. Статья 8: Право на уважение частной и семейной жизни, жилища и корреспонденции. Прецеденты и комментарии / У. Килкэли, Е.А. Чефранова. – М., 2001. – С. 56.

[3] О персональных данных: федер.закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017).

Окончательная точка в этом вопросе была поставлена в принятом позднее специальном Федеральном законе «О персональных данных», где в ст. 2 в качестве основной цели защиты персональных данных указывается обеспечение прав и свобод человека и гражданина, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Следовательно, будет логично сделать вывод о наличии прямой связи между защитой персональных данных и правом на неприкосновенность частной жизни, а также включенных в него правомочий (право на тайну частной жизни, личную, семейную тайну, тайну исповеди, тайну голосования и т.д.).

В то же время, ориентируясь на законодательное определение «персональных данных», где последние включают в себя всю *информацию о физическом лице или относящиеся к определенному или определяемому на основании таких сведений физическому лицу*[1], можно вполне обоснованно прийти к выводу о том, что круг сведений, информации, которая может быть представлена в виде персональных данных, не ограничивается частной или личной, семейной сферой жизни индивида. В частности, персональные данные могут вполне включать в себя сведения об общественной жизни индивида, о его служебной и профессиональной деятельности и многое другое, что не всегда может охватываться понятием частная жизнь или, по крайней мере, вызывать сомнение такого отнесения к указанной категории. Из анализа существующих положений законодательства следует, что потенциально персональные данные включают в себя, наряду со сведениями о частной жизни лица (тайной частной жизни), целый круг сведений, которые охватываются многими другими правовыми категориями, которые существовали и появились, и укоренились в правовой материи существенно ранее категории «персональные данные».

[1] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017).

В частности, по тексту Федерального закона «О персональных данных»[1], как минимум, можно прийти к выводу, что в отдельных положениях идет речь о персональных данных, составляющих одновременно сведения, охраняемые на условиях других режимов: государственной тайны (ст. 1, ч. 2, п. 4); личной, семейной тайны; тайны частной жизни (ст. 2); врачебной тайны (ст. 10, ч.2, п. 3–4); тайны следствия; тайны правосудия и оперативно-розыскной деятельности (ст. 10, ч. 2, п. 6–7 и ст. 11, ч. 2).

Во всех этих случаях очевидным общим моментом является то, что эта информация – об индивиде, и в отношении ее введен правовой режим тайны.

По общему правилу, режим тайны в соответствии с законодательством означает охрану от распространения информации в отношении третьих лиц, ввиду того что подобное распространение способно нанести вред правам и законным интересам, в данном случае – тайне частной жизни конкретного физического лица или его близких родственников. Такое положение дел вполне можно соотнести с режимом конфиденциальности, который устанавливается ст. 7 закона «О персональных данных»[2].

Следовательно, говоря о соотнесении персональных данных и права на неприкосновенность частной жизни, вполне обоснованно можно сделать вывод, что они являются связанными между собой понятиями, но в то же время не тождественными.

В последнее время этому вопросу посвящено достаточное внимание в целом ряде публикаций и диссертационных исследованиях. И.А. Вельдер заявляет о персональных данных как о «комплексном и самостоятельном образовании» – новом правовом институте[3]. Аналогичного мнения придерживается и А.С. Кучеренко, которая не только обосновывает его самостоятельность, но и подчеркивает его мобильность и динамичное

[1] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017).
[2] Там же.
[3] Вельдер, И.А. Система правовой защиты персональных данных в Европейском союзе: дис. ... канд. юрид. наук: 12.00.10 / И.А. Вельдер. – Казань, 2006. – С. 10.

развитие[1]. Н.Г. Белгородцева в своей работе также разделяет идею «самостоятельности» персональных данных, но путем выделения правового института «защиты персональных данных»[2], который носит межотраслевой комплексный характер. Небольшое расхождение в терминологии никак не умаляет в таком случае общую идею выделения правовых норм, регулирующих порядок оборота персональных данных, в самостоятельный правовой институт.

С указанными предложениями трудно не согласиться, учитывая сказанное выше, а также количество законодательных актов в этой сфере, принимаемых в последнее время.

Примерно схожие рассуждения о самостоятельности как института персональных данных в сравнении с правом на неприкосновенность частной жизни можно встретить и у целого ряда зарубежных авторов[3], что еще раз подтверждает общий вектор развития права в этом направлении, который ориентирует нас на самостоятельность правового института персональных данных.

Еще один существенный вопрос, который достаточно остро поднят в работе И.А. Вельдера, требует отдельного внимания – это формирование права на защиту персональных данных, в числе фундаментальных прав личности[4]. Безусловно, идея «прав человека» является динамично развивающимся образованием и постепенно эволюционирует, прирастая новыми значениям, смыслами, а иначе говоря, новыми правами и свободами, которые с развитием общества начинают восприниматься неотъемлемыми и фундаментальными. Аналогично зарождению права на защиту частной жизни из идеи личной свободы, можно со всей обоснованностью

---

[1] Вельдер, И.А. Система правовой защиты персональных данных в Европейском союзе: дис. ... канд. юрид. Наук: 12.00.10 / И.А. Вельдер. – Казань, 2006. – С. 10.

[2] Белгородцева, Н.Г. Теоретико-правовые аспекты защиты персональных данных: автореф. дис. ... канд. юрид. наук / Белгородцева Н.Г. – М., 2012. – С. 10–11.

[3] Beigner, B. Le droit de la personnalité / B. Beigner // Collection “Que sais-je?” – P.U.F., 1992. – n°2703; Hustinx, P.J. Right to privacy and data protection: mission impossible? / P.J. Hustinx // European Data Protection Day. – 2010. – 28 January. – (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa384). – Дата обращения: 02.04.2017.

[4] Вельдер, И.А. Система правовой защиты персональных данных в Европейском союзе: дис. ... канд. юрид. наук: 12.00.10 / И.А. Вельдер. – Казань, 2006. – С. 33.

предполагать о появлении нового права – права на защиту персональных данных, как во многом необходимого элемента информационной культуры современного общества, без которого невозможно было бы обеспечить необходимый уровень защиты личности. Схожую идею можно найти и в исследовании Н.Г. Белгородцевой, которая также склонна рассматривать «защиту персональных данных» и «право на защиту персональных данных» как одну из разновидностей юридических гарантий конституционных прав человека[1], а также у А.С. Федосина[2].

В то же время, упоминание И.А. Вельдером «права на конфиденциальность персональных данных»[3] видится не совсем логичным.

Во-первых, конфиденциальность является скорее требованием, обращенным к операторам персональных данных, и является безусловным, если только иное не предусмотрено законом или самим субъектом, и в некоторых случаях вообще не зависит от воли последнего.

Во-вторых, «конфиденциальность» стоит рассматривать как один из элементов защиты персональных данных как информации особого рода, но далеко не единственный.

Таким образом, «право на конфиденциальность данных» скорее стоит рассматривать не более чем элементом или правомочием «права на защиту персональных данных».

С другой стороны, отметим в продолжение темы, что режим конфиденциальности персональных данных все же способствует установлению режима конфиденциальности информации, составляющей тайну частной жизни, личную и семейную тайну индивида, и гарантирует посредством этого неприкосновенность частной жизни, ограничивая доступ к такой информации со стороны третьих лиц, а также предоставляя индивиду

---

[1] Белгородцева, Н.Г. Теоретико-правовые аспекты защиты персональных данных: автореф. дис. ... канд. юрид. наук / Н.Г. Белгородцева. – М., 2012. – С. 10–11.

[2] Федосин, А.С. Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации: автореф. дис. ... канд. юрид. наук: 12.00.14 / А.С. Федосин. – Саранск, 2009. – С. 7.

[3] Вельдер, И.А. Система правовой защиты персональных данных в Европейском союзе: дис. ... канд. юрид. наук: 12.00.10 / И.А. Вельдер. – Казань, 2006. – С. 61.

возможность контролировать распространение такой информации на основании ст. 14 закона «О персональных данных». Последнее крайне важно, учитывая, что законодательно ни понятие «частной жизни», ни понятие «тайны частной жизни» не определены, если вообще возможно дать их точное определение, о чем уже ранее говорилось, а также принимая во внимание развитие информационных технологий и активное формирование электронных баз данных о физических лицах не только государством, но и частными компаниями – клиентские базы данных, базы данных подписчиков, слушателей, зрителей, базы данных абонентов, пользователей социальных сетей и т.п.

1.2. Понятие и признаки персональных данных

Появление термина «персональные данные» явилось следствием демократических преобразований в Российском государстве и восприятия идеи защиты прав личности как первостепенной задачи государства на пути к информационному обществу. Следует признать, что российское законодательство и практика долгое время не содержали каких-либо конкретных положений о защите персональных данных, ограничиваясь лишь декларативными положениями, и то в очень незначительном объеме, что породило массу рассуждений о сущности категории персональных данных и целесообразности ее появления в российском праве.

Автору видится вполне логичным для реализации целей и задач диссертационного исследования подробно рассмотреть в целом содержание правовой категории «персональные данные». Это позволит в дальнейшем сформулировать и наиболее четко выделить предмет исследования, сформулировать сущность российского подхода к правовому регулированию рассматриваемого явления и дать его оценку. Для этого следует соотнести категории: «информация», «данные» и «персональные данные» и, в первую очередь, выделить отличительные признаки последней.

Начать следует с понятия «информация», которое, по-прежнему, представляет значительные трудности и раскрытие его является одной из важнейших проблем не только юридической, но и всей науки в целом. Сам термин происходит от латинского informatio – ознакомление, изложение, разъяснение. И первоначально ассоциировался с такими понятиями, как послание, сообщение. В современной науке существуют десятки определений информации, однако большинство современных ученых в конечном итоге вынуждены признать, что исчерпывающего понятия сформулировать невозможно, поскольку оно во многом будет зависеть от сферы научных знаний и прикладного характера исследования[1]. Наиболее

[1] Лапина, М.А. Информационное право / М.А. Лапина, Г.А. Ревин, В.И. Лапин. – М.: Юнити-Дана, 2004. – С. 8.

полно сущность информации исследуется в философии и информатике, где известно огромное количество подходов.

Каждая концепция, по мнению О.И. Семенкова[1], отражает определенный аспект информации и поэтому их следует рассматривать в единстве. Р.Ф. Абдеев[2] предлагает свести все предлагаемые разными авторами концепции к двум основным подходам, концепциям информации – атрибутивной и функциональной. Сущность первого подхода состоит в понимании информации как свойства всех материальных объектов, т.е. как атрибут материи. Так, в частности, считают А.С. Пресман, В.Н. Саблин, В.А. Минаев[3] и некоторые другие[4]. В.Н. Лопатин указывает: «…То обстоятельство, что информация реализуется через объекты материи и ее свойства, позволяет нам утверждать, что всякая информация материальна»[5]. Функциональная концепция информации связывает информацию с функционированием самоорганизующихся систем. Н.Ю. Климонтович, предлагает считать информацией лишь то, «…что понимается и само воспроизводит информацию…», т.е. «информация – это язык»[6]. С точки зрения семантической теории информации, основоположником которой является Ю.А. Шрейдер[7], существуют две категории информации – внутренняя и внешняя. Внутренняя информация – информация как характеристика организованности любой системы; то, что еще Аристотель называл «энтелехией», а в современной науке принято именовать «структурной информацией»[8]. Структурная информация присуща всем

---

[1] Семенков, О.И. Информация / О.И. Семенков // Новейший философский словарь. – Минск, 1998. – С. 274–276.

[2] Абдеев, Р.Ф. Философия информационной цивилизации / Р.Ф. Абдеев. – М., 1994. – С. 162.

[3] Теоретические основы информатики и информационной безопасности / Под ред. В.А. Минаева, В.Н. Саблина. – М.: Радио и связь, 2000. – С. 127.

[4] Пресман, А.С. Организация биосферы и ее космические связи / А.С. Пресман. – М., 1997. – С. 26.

[5] Лопатин, В.Н. Информационная безопасность России: человек, общество, государство. Фонд поддержки науки и образования в области правоохранительной деятельности «Университет» / В.Н. Лопатин. – СПб.: Ун-т МВД России, 2000. – С. 23.

[6] Климонтович, Н.Ю. Без формул о синергетике / Н.Ю. Климонтович. – Минск, Вышэйшая школа, 1986. – С. 132.

[7] Шрейдер, Ю.А. Об одной модели семантической теории информации / Ю.А. Шрейдер // Проблемы кибернетики. – Вып. 13. – М., 1965. См. также: Философский словарь / Под ред. И.Т. Фролова – 5-е изд. – М., 1986. – С. 172.

[8] Философский словарь / Под ред. И.Т. Фролова. – 5-е изд. – М.: Политиздат, 1986. – С.172.

объектам живой и неживой природы и обладает относительной объектной самостоятельностью. Внешняя информация – информация как средство организации любой системы, то, что Аристотель назвал «кинесисом», а в современной науке именуется «относительной информацией», «оперативной информацией»[1], тесно связанной с отражением. Норберт Винер, «отец» кибернетики, как его иногда называют, указывал, что «информация – это информация, а не энергия и не материя», формулируя понятие информации через «обозначение содержания… такого сообщения, которое получено от внешнего мира в процессе нашего приспособления к нему и приспособления наших чувств»[2]. А.А. Стрельцов рассматривает информацию именно как «результат отражения движения объектов материального мира в системах живой природы»[3], отвергая тем самым концепцию информации в качестве атрибута материи. По его мнению, информация как отражение движения объектов материального мира, запечатленное в организме или коллективе организмов, используется последними для адаптации к изменениям окружающей действительности и проявляется в форме сведений и сообщений. При этом сведения и есть результат отражения организмами материального мира, в том числе и сообщений, а сообщения в таком случае – набор знаков, при помощи которых сведения передаются другим организмам и могут быть восприняты ими, т.е. при помощи которых организмы обмениваются сведениями[4].

ЮНЕСКО определило «информацию как универсальную субстанцию, пронизывающую все сферы человеческой деятельности, служащую проводником знаний и сведений, инструментом общения, взаимопонимания и сотрудничества, утверждения стереотипов мышления и поведения»[5].

---

[1] Семенков, О.И. Информация / О.И. Семенков // Новейший философский словарь. – Минск. 1998. – С. 276.
[2] Винер, Н. Мое отношение к кибернетике, ее прошлое и будущее / Н. Винер. – М.: Советское радио, 1969. – С. 23.
[3] Стрельцов, А.А. Обеспечение информационной безопасности России / А.А. Стрельцов. – М.: Изд-во МЦНМО, 2002. – С. 22.
[4] Там же. – С. 24–26.
[5] Лапина, М.А. Информационное право / М.А. Лапина, Г.А. Ревин, В.И. Лапин. – М.: Юнити-Дана, 2004. – С. 9.

В целом, определение понятия информации через категории «сведения», «сообщение» встречается наиболее часто в различного рода справочной литературе. Так, к примеру, С.И. Ожегов дал такое простое определение:

1) «сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством;
2) сообщения, осведомляющие о положении дел, о состоянии чего-нибудь»[1].

Современный словарь иностранных слов трактует понятие информации как одно из наиболее общих понятий современной науки схожим образом:

1) «сообщение о чем-либо;
2) сведения, являющиеся объектом хранения, переработки и передачи;
3) в математике, кибернетике – количественная мера устранения неопределенности (энтропии), мера организации системы»[2].

Пожалуй, можно назвать еще множество источников, научных работ, в которых с позиции различных сфер научного знания рассматривается понятие информации, но практически чуть ли не в большинстве из них она определяется именно через категории «сведения» и «сообщение». Понятие «сведения» в русском языке определяется как «знание, представление о чем-либо», которые можно рассматривать в качестве результата отражения в сознании человека материального мира. Понятие «сообщение» во многом связывают с актом коммуникации, т.е. передачи сведений, знаний от одного субъекта/системы – другой.

Н. Винер, отмечая подобные закономерности, назвал их двумя измерениями информации, определяющими ее природу, и выделил информацию-*сообщение* (сигнал, команду) и информацию-*содержание*, как результат восприятия сообщения[3].

---

[1] Ожегов, С.И. Словарь русского языка / С.И. Ожегов, Н.Ю. Шведова. – 22-е изд., стереотипное. – М.: Русский язык, 1990. – С. 253.
[2] Современный словарь иностранных слов / Сост. Н.М. Ланда. – М.: Русский язык, 1993. – С. 245.
[3] Винер, Н. Кибернетика и общество / Н. Винер. – М.: Изд-во иностр. лит-ры, 1958. – С. 32.

П.У. Кузнецов также отметил два составляющих элемента понимания информации, применительно к человеческому организму: переданного *сообщения* (команды, сигнала) и полученного *образного обозначения* (концепта), составляющих вместе единое гомогенное целое. На основании чего им был сделан вывод о двух дескриптах информации: сообщение (сигнал, команда) – *формального* свойства и образного обозначения (концепта) – *содержательного* свойства[1], т.е. о *дуалистической* природе информации.

В конечном итоге можно прийти к выводу о том, что для объектов живой природы:

«Информация – есть результат отражения движения объектов материального мира, запечатленный в организме и используемый им для адаптации к изменениям окружающего мира. В коллективе однотипных организмов информация обращается в виде сведений и сообщений»[2].

Применительно к человеческому сообществу можно считать, что информацией будет как раз результат отражения изменений материального мира в организме человека, коллектива человеческих индивидов, который существует в виде сведений и передается в виде сообщений другим индивидам/коллективам индивидов.

Насколько такое определение функционально и подходит для использования в правовой науке, однозначно сказать сложно, поскольку проблема определения информации в праве столь же актуальна, как и в других сферах научного знания. Тем не менее, многими авторами признается, что в праве, как и в других гуманитарных науках, используются именно подобные определения через категории «значение», «сообщение», «сведения». Отсутствие единого понятия, в том числе и в праве, отмечено специалистами еще в середине 1980-х годов. В настоящий момент при

---

[1] Кузнецов, П.У. Теоретические основания информационного права: автореф. дис. ... д-ра юрид. наук: 12.00.14 / П.У. Кузнецов. – Екатеринбург, 2005. – С. 18.

[2] Стрельцов, А.А. Обеспечение информационной безопасности России / А.А. Стрельцов. – М.: Изд-во МЦНМО, 2002. – С. 39.

определении информации очень часто используются такие термины и понятия, как: «информация», «документ», «массив документов», «официальная информация», «массовая информация», «данные», «банки данных», «информационный ресурс», «компьютерная информация», «файл», «сайт», «страница», «электронная подпись», «правовая информация» и т.д. Такое обилие терминов, по мнению И.Л. Бачило[1], может служить основанием для теории системы объектов информации, однако вплоть до настоящего момента такая система еще только начинает складываться.

По оценке Л.К. Терещенко, в большинстве исследований в области правовой науки, посвященных вопросам подробного исследования правовой дефиниции информации, как правило, результат не выходит за рамки уже существующих правовых дефиниций[2].

В основном эти определения также исходят из материальной или идеальной природы информации.

К первой группе можно отнести определение А.А. Антопольского, который определяет информацию как «результат сознательной деятельности человека, зафиксированный в любой пригодной для восприятия форме»[3]. Недостатком указанного определения является слишком широкий круг объектов, которые могут быть одновременно и результатами сознательной деятельности людей и иметь воспринимаемую индивидом форму. Далее в своей работе А.А. Антопольский уточняет, что под информацией понимает «записанные или сообщенные сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления»[4], что фактически по содержанию в значительной степени близко к легальному определению информации. Другим примером может служить определение информации в работе А.В. Минбалеева – «идеальный продукт отражения

---

[1] Бачило, И.Л. Информация и информационные отношения в праве / И.Л. Бачило // НТИ. – 1999. – № 8. – Сер. 1.
[2] Терещенко, Л.К. Правовой режим информации / Л.К. Терещенко. – М.: Юриспруденция. 2007. – С. 11.
[3] Антопольский, А.А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: автореф. дис. … канд. юрид. наук / А.А. Антопольский. – М., 2004. – С. 6.
[4] Там же. – С. 12.

мира (окружающей действительности) во всей совокупности его составляющих (явления, объекты, процессы, связи и т.п.), существующий в какой-либо способной для объективного восприятия форме»[1].

Если обратиться непосредственно к законодательному определению, то основополагающий закон «Об информации, информационных технологиях и о защите информации» определил информацию как «сведения (сообщения, данные) независимо от формы их представления»[2]. Если провести аналогию с предшествующим законом, в котором говорилось, что «информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления»[3], – то налицо можно отметить некоторые положительные тенденции в определении информации не только как сведения, но и через сообщение и данные. Однако законодатель относит, судя по всему, сообщения и данные к категории сведений, исходя из самой структуры определения, и, к сожалению, не дает непосредственно определения ни одной из этих категорий, и уж тем более не дает представления об их соотношении, что является серьезным основанием для критики.

С учетом специфики правовой сферы А.А. Антопольский[4] предложил понимать под информацией «продукт отражения в сознании субъектов реальных явлений, предметов и процессов, существующих в объективной форме и обладающих свойствами воспроизводимости и копируемости». В таком случае, по его мнению, информацию следует определить как «*записанные или сообщенные сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления*». Такое определение в действительности не слишком отличается по смыслу от

---

[1] Минбалеев, А.В. Система информации: теоретико-правовой анализ: автореф. дис. … канд. юрид. наук / А.В. Минбалеев. – Челябинск., 2006. – С. 8.

[2] Об информации, информационных технологиях и о защите информации: федер. закон от 29.07.2006 № 149-ФЗ (ред. от 19.12.2016). – Ст. 2.

[3] Об информации, информатизации и защите информации: федер. закон от 20.02.1995 № 24-ФЗ. – Ст. 2. (Утратил силу.)

[4] Антопольский, А.А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: автореф. дис. … канд. юрид. наук / А.А. Антопольский. – М., 2004. – С. 12

легального, но в тоже время, по мнению автора, является достаточно удачным, поскольку в равной степени отражает содержательное свойство информации (сведение, знание, образ, концепт) и соотносит его с формальным (сообщением, сигналом), при этом приковывая внимание к последнему. Это логично еще и в связи с тем, что содержательная составляющая (знание, образ-концепт) скорее относится к ментальной деятельности, сущности индивида и вряд ли может быть в таком случае объектом правового регулирования, тогда как формально выраженное сообщение – может. При этом категория «сведения» видится вполне употребимой при обозначении информации, поскольку отражает конечный продукт предполагаемого воздействия на сознание индивида, т.е. на возникающий в сознании индивида концепт. Очевидно, используемую категорию «сведения» в отношении информации, циркулирующей в обществе, следует рассматривать как указание на образ-концепт, передаваемый от одного субъекта или группы субъектов другой, посредством сообщений (сигналов, команд), в рамках определенной системы, обеспечивающей или стремящейся обеспечить с максимальной эффективностью тождественность концепта-образа у субъекта-источника и субъекта-реципиента или их групп. Такой универсальной системой команд, сигналов следует признать язык как универсальное средство передачи образов-концептов (сведений) от одного индивида или группы индивидов другим.

Возвращаясь к понятию «данные», следует упомянуть, что оно прочно ассоциируется со сферой информатики и понимается там, прежде всего, как «информация, представленная в формализованном виде, что обеспечивает возможность её хранения, автоматической обработки и передачи с помощью технических средств (например, ЭВМ)»[1]. Словарь Т.Ф. Ефремовой дает приблизительно схожее определение и рассматривает данные как «сведения, факт, характеризующие кого-либо, что-либо, необходимые для каких-либо

[1] Энциклопедический словарь, 2009. – (http://dic.academic.ru/contents.nsf/es/). – Дата обращения: 02.04.2017.

выводов, решений»[1]. Толковый словарь русского языка содержит аналогичное определение: «данные – сведения, необходимые для какого-нибудь выводов, решения»[2]. Электронный словарь бизнес-терминов также содержит близкое по содержанию предыдущим понятие данных как «сведения, информация, сведения о людях, фирмах, представленные в формализованном виде, удобном для пересылки, интерпретации и обработки»[3].

По мнению автора, следует отметить в этих определениях два существенных момента – два основных значения термина «данные» в языке.

1. «Данные – информация (сведения, сообщения), необходимые для производства с ней определенных действий, т.е. ее обработки. В этом случае термин не имеет какого-либо специального значения и употребляется как синоним слова информация в целом.
2. Данные, как специальный термин в информатике, обозначающий информацию (сведения, сообщения) в определенном упорядоченном и формализованном виде, подготовленную для обработки с помощью средств автоматизации, технических средств (ЭВМ)»[4].

Во-вторых, и это, пожалуй, самое главное, что данные являются информацией формализованной, представленной в каком-то определенном виде, который бы обеспечивал возможность их дальнейшей обработки или, по крайней мере, способствовал этому и сделал сведения удобными для последующей обработки. Степень формализации в определениях не подчеркнута, в связи с чем можно обосновано рассматривать их в самом широком смысле. Упорядочение информации может затронуть в частности:

---

[1] Ефремова, Т.Ф. Новый словарь русского языка. Толково-словообразовательный / Т.Ф. Ефремова. – М.: Русский язык, 2000. – (http://www.efremova.info). – Дата обращения: 02.04.2017.
[2] Ожегов, С.И. Словарь русского языка / С.И. Ожегов, Н.Ю. Шведова. – (http://slovar.plib.ru/dictionary/d19/). – Дата обращения: 02.04.2017.
[3] Словарь бизнес-терминов. – Академик.ру, 2001. – (http://dic.academic.ru/dic.nsf/business/3172). – Дата обращения: 02.04.2017.
[4] Бундин, М.В. Персональные данные как термин российского законодательства / М.В. Бундин // Правовые вопросы связи. – 2009. – № 1. – С. 4.

1) носитель, на котором содержатся сведения (электронный, бумажный, иного рода);

2) знаковую систему (язык, язык программирования и т.п.);

3) внутреннее содержание (логическая структура, категории сведений, необходимые реквизиты).

Принятие такого положения дел позволяет говорить о некоторой возможности соотнесении понятий «информация» – «данные». Очевидно, что эти понятия нужно рассматривать как общее и частное, и «данные» в этой связи являются одной из форм представления информации, и что их отличительным признаком следует назвать формализованность, т.е. их определенную упорядоченность. Формализованность данных проявляется в способе и средствах представления сообщений, сведений, чтобы обеспечить их возможность обработки определенным способом или облегчить ее.

Законодательного определения термина «данные» мы не найдем, но существуют другие определения, которые могут натолкнуть на мысль о том, как же законодатель трактует это понятие. В российском законодательстве активно использовались и используются термины «база данных», «банк данных», «информационный ресурс(ы)». В частности, ныне утративший силу Федеральный закон «О правовой охране программ для электронных вычислительных машин и баз данных» содержал такое определение базы данных – «это объективная форма представления и организации совокупности данных (например: статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ»[1]. Гражданский кодекс в ст. 1260 ч. 2 под «базой данных» понимает «представленную в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с

[1] О правовой охране программ для электронных вычислительных машин и баз данных: закон РФ от 23.09.1992 № 3523-1 // «Российская газета». – 1992. – 23 сент. (Утратил силу.)

помощью электронной вычислительной машины (ЭВМ)». Словосочетание «банк данных» чаще встречается в законодательстве применительно к какой-то конкретной совокупности сведений, например Федеральный закон «О государственном банке данных о детях, оставшихся без попечения родителей»[1], где под государственным банком данных о детях, оставшихся без попечения родителей, в ст. 1 подразумевают совокупность информационных ресурсов и информационных технологий, с помощью которых осуществляется их сбор, обработка, накопление, хранение, поиск и предоставление гражданам. Такая же точка зрения – объединять под понятием «банк данных» совокупность базы данных и информационных технологий для их обработки – отражена в Постановлении Правительства «О государственном учете и регистрации баз и банков данных»[2], где в п. 2 прямо указывается, что «под базой данных понимается совокупность организованных взаимосвязанных данных на машиночитаемых носителях», а «банк данных» – это, соответственно, «совокупность баз данных, а также программные, языковые и другие средства, предназначенные для централизованного накопления данных и их использования с помощью электронных вычислительных машин»[3]. Категория «информационные ресурсы» используется столь же широко в законодательстве, однако непосредственно трактовка этого термина была дана в Федеральном законе «Об информации, информатизации и защите информации», где под ними подразумевались «отдельные документы или массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)»[4], который теперь утратил силу, а принятый ему на смену закон такое понятие не использует в принципе.

---

[1] О государственном банке данных о детях, оставшихся без попечения родителей: федер. закон от 16.04.2001 № 44-ФЗ (ред. от 30.12.2008) // «Российская газета». – 2001. – 16 апр.

[2] Временное положение «О государственном учете и регистрации баз и банков данных». Утверждено Постановлением Правительства Российской Федерации от 28 февраля 1996 г. № 226 (в ред. Постановления Правительства от 02.03.2006). (Утратило силу.)

[3] Там же.

[4] Об информации, информатизации и защите информации: федер. закон от 20.02.1995 № 24-ФЗ // Собрание законодательства Российской Федерации. – 1995. – № 8. – Ст. 609.

Таким образом, можно сделать вывод о том, что и в законодательстве под «данными» подразумевается, в первую очередь, информация (сообщения, сведения), определенным образом организованные и представленные на машинных носителях, т.е. предназначенные для автоматизированной обработки с использованием информационных технологий и находящиеся в базах или банках данных, а говоря современным языком, в информационных системах. Иными словами, законодатель не проводит четкого различия между данными и информацией, однако, безусловно, рассматривает данные как разновидность информации. В некоторых законодательных актах, например, в Федеральном законе «О связи»[1], ничего не говорится о том, что данные представляют собой информацию на электронном носителе или что они обрабатываются полностью, или хотя бы частично, с помощью средств автоматизации. В то же время анализ текста статьи 53 данного закона позволяет говорить о том, что под базами данных здесь понимаются автоматизированные (электронные) базы данных об абонентах операторов связи и что они представлены в формализованном/упорядоченном виде, о чем свидетельствует ч. 1 и ч. 2 этой статьи, где говорится о перечне сведений, заносимых в базу данных, а также о возможности передачи сведений из базы данных на магнитных носителях и с помощью средств телекоммуникации. Другой пример – данные, заносимые в государственный банк данных о детях, оставшихся без попечения родителей. Сам Федеральный закон[2] говорит в ст. 4 о формализации – стандартизации документированной информации о детях, оставшихся без попечения родителей и гражданах, желающих их принять, которая затем заносится в базу/банк данных, и стандартизации (унификации) процессов обработки, хранения, восстановления, дублирования, предоставления указанной информации. Сам процесс сбора заносимых в вышеуказанный банк данных сведений осуществляется в

[1] О связи: федер. закон от 07.07.2003 № 126-ФЗ (ред. от 06.07.2016).

[2] О государственном банке данных о детях, оставшихся без попечения родителей: федер. закон от 16.04.2001 № 44-ФЗ // Российская газета. – 2001. – 20 апр.

соответствии с порядком, предусмотренным, соответствующим приказом Министерства образования РФ[1], в котором прямо указывается, какая информация в него заносится и каким образом. Происходит это частично путем заполнения анкеты ребенком или соответственно гражданином, желающим усыновить ребенка, что позволяет говорить о том, что запрашиваются и включаются в базу данных определенные категории сведений: Ф.И.О., пол, дата и место рождения, гражданство, состояние здоровья и т.д. Вся документированная информация хранится в личном деле ребенка или гражданина и заносится в автоматизированные базы данных.

Такой порядок работы со сведениями, заносимыми в базы и банки данных, является далеко не исключением, а скорее правилом, поскольку, когда речь идет о формировании баз и банков данных, процесс включения сведений (данных) в них является формализованным, упорядоченным, с точки зрения их представления и категорий сведений, которые в них включаются. Практически в любом случае, когда речь идет о сборе сведений для ведения реестров, регистров, баз данных, всегда предусматриваются категории информации, которые подлежат включению в них, а также порядок ее сбора, что опять говорит о формализованном характере сведений, включаемых в категорию «данные».

В правовой науке соотнесению категорий «информация» и «данные» посвящено не так уж много работ, и в основном эти понятия рассматриваются как синонимичные, без выделения каких-либо особенных признаков данных как разновидности информации. Все же отдельные идеи об этом можно встретить у В.П. Иванского, который подчеркивает, что под «данными» следует понимать преимущественно информацию, полученную в результате обработки ЭВМ или подготовленную в специальной форме для такой обработки[2].

---

[1] Приказ Министерства образования РФ от 28.2002 № 2482.

[2] Иванский, В.П. Правовая защита информации о частной жизни граждан. Опыт современного правого регулирования: монография / В.П. Иванский. – М.: Изд-во РУДН, 1999. – С. 8

Следовательно, на основе анализа положений законодательства и справочной литературы следует прийти к выводу о том, что:

Данные – это информация (сведения, сообщения), упорядоченная с точки зрения формы представления и внутреннего содержания, что обеспечивало или упрощало бы ее обработку полностью или частично с помощью средств автоматизации в информационных системах.

Следовательно, при соотнесении двух категорий – «информация» и «данные» можно прийти к выводу о том, что «данные» будут являться одной из форм информации, главным отличительным признаком которой будет ее упорядоченный характер, который бы упрощал обработку, работу с ней, и которая подлежит обработке в информационных системах, преимущественно с помощью средств автоматизации.

Теперь становится возможным соотнести, наконец, категории «информация», «данные» и «персональные данные» и определить отличительные признаки последних, и дать их определение.

Впервые термин «персональные данные» в российском законодательстве появляется одновременно с аналогичным понятием «информация о гражданах», в Федеральном законе «Об информации, информатизации и защите информации»[1], в ст. 2 которого говорилось: «…*информация о гражданах (персональные данные) – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность*». По тексту данного закона подразумевалось, что более подробно вопрос о персональных данных будет решен путем принятия специального законодательства[2], которое затянулось почти на 10 лет. С принятием специального законодательства – Федерального закона «О персональных данных»[3] – трактовка понятия персональных данных несколько изменилась: «персональные данные – любая

[1] Об информации, информатизации и защите информации: федер. закон от 20.02.1995 № 24-ФЗ. – Ст. 11. – Ч. 1. (Утратил силу).
[2] Там же.
[3] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017). – Ст. 2.

информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация»[1]. Следует отметить в новой трактовке ряд существенных позитивных элементов, отсутствовавших в ранее действующем законодательстве:

– отказ от понятия «информация о гражданах» и упоминания в дальнейшем по тексту определения только граждан и переход к категории «физического лица», включая в категорию субъектов персональных данных не только граждан, но и других лиц, иностранцев, лиц без гражданства и т.д.;

– отказ от «идентификации» в качестве одного из основных признаков персональных данных, заменив его «информацией об определенном или определяемом на основании этой информации физическом лице»[2].

«Идентификация» в качестве необходимого критерия или признака персональных данных выделяется также у А.А. Фатьянова[3]. Однако использование данного критерия может привести к ряду затруднений, учитывая, что сам процесс идентификации в качестве критерия отграничения персональных данных от иных категорий сведений приведет неизбежно к возникновению множества споров о возможности или невозможности однозначно установить лицо на основании совокупности тех или иных сведений о нем, а следовательно, к проблемам в правоприменительной практике. О.Б. Просветова в этом отношении придерживается мнения о нецелесообразности сужения значения персональных данных лишь к сведениям, служащим для идентификации личности, что, по ее мнению, «не соответствует статье 24 Конституции, которая охватывает все сведения о

[1] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017). – Ст. 3.
[2] Там же.
[3] Фатьянов, А.А. Тайна и право (основные системы ограничения на доступ к информации в российском праве) / А.А. Фатьянов. – М.: Проспект, 1999. – С. 188.

частной жизни лица»[1]. Г. Бребант справедливо отмечает, что «в настоящее время, с развитием технологий обработки полученной информации, потенциально расширяется возможность идентификации лица по какому-либо фрагменту информации. В этой связи, с его точки зрения, справедливо расширение значения персональных данных до указания на информацию, так или иначе связанную с субъектом, приводя в качестве примера фрагменты звуко-, видеозаписей, почерка, текста с особенностями морфологии и стиля»[2].

В других законодательных актах также содержатся аналогичные определения персональных данных, как через категорию информации, так и через категорию сведения, в частности в Трудовом кодексе в ст. 85 говорится, что: «персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника», а в Федеральном законе «О Государственной автоматизированной системе Российской Федерации «Выборы» в ст. 2 п. 7, что «персональные данные – сведения, которые содержатся в ГАС «Выборы», позволяют идентифицировать личность гражданина и перечень которых устанавливается федеральными законами». Федеральное законодательство о государственной службе также активно использует понятия «персональные данные государственного служащего»[3] и «персональные данные государственного гражданского служащего»[4], не раскрывая их значения в самом тексте законов. Однако специальное Положение о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела содержит определение:

«…персональные данные государственного гражданского служащего

---

[1] Просветова, О.Б. Защита персональных данных: дис. … канд. юрид. наук: 05.13.19 / О.Б. Просветова. – Воронеж, 2005. – С. 26

[2] Braibant, G. Données personnelles et société de l’information / G. Braibant. – Paris, 2000. – P. 76–77.

[3] О системе государственной службы Российской Федерации: федер. закон от 27.05.2003 № 58-ФЗ (ред. от 23.05.2016). – Ст. 14.

[4] О государственной гражданской службе Российской Федерации: федер. закон от 27.07.2004 № 79-ФЗ (ред. от 19.12.2016). – Ст. 42.

как сведения о фактах, событиях и обстоятельствах жизни гражданского служащего, позволяющие идентифицировать его личность и содержащиеся в личном деле гражданского служащего либо подлежащие включению в его личное дело»[1].

В зарубежной и международной практике «персональные данные» в равной степени трактуются через категорию информации или схожие категории, учитывая при этом особенности или «погрешности», которые неизбежно возникают при переводе терминологии с одного языка на другой.

На международном уровне, к примеру, можно назвать Рекомендации Совета ОСЭР, касающиеся основных положений о защите неприкосновенности частной жизни и международных обменов персональными данными[2], в которых предлагается относить к персональным данным «любую информацию, относящуюся к индивидууму («субъекту данных»), чья личность либо известна, либо может быть установлена». Очень схожее по своей сути определение содержится и в Конвенции Совета Европы о защите личности в связи с автоматизированной обработкой данных[3], в которой под персональными данными понимают «информацию, касающуюся конкретного или могущего быть идентифицированным лица (“субъекта данных”)».

В одном из наиболее известных источников – Директиве Европейского парламента и Совета ЕС 95/46/ЕС[4] содержится более развернутое определение, впрочем, логически мало отличающееся от предыдущих:

«…“персональные данные” – любая информация, связанная с идентифицированным или идентифицируемым физическим лицом

---

[1] Утверждено Указом Президента Российской Федерации от 30.05.2005 № 609. – П. 2

[2] Приложение к Рекомендации Совета ОСЭР, касающееся основных положений о защите неприкосновенности частной жизни и международных обменов персональными данными // Защита персональных данных: Опыт правового регулирования. – М.: Галерия, 2001. – (http://www.gdf.ru/library/item/5/60). – Дата обращения: 02.04.2017.

[3] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в Страсбурге 28.01.1981) // Сайт компании «КонсультантПлюс». – (http://www.consultant.ru/document/cons_doc_LAW_121499/). – Дата обращения: 02.04.2017.

[4] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Дата обращения: 02.04.2017.

(“субъектом данных”); идентифицируемым лицом является лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификационный номер или на один, или несколько факторов, специфичных для его физической, психологической, ментальной, экономической, культурной или социальной идентичности».

Последний источник на международном уровне, который стоит отдельного упоминания в таком случае, является Модельный закон «О персональных данных» для стран СНГ, где предлагается следующая трактовка:

«Персональные данные – информация (зафиксированная на материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним. К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном, социальном положении, образовании, профессии, служебном и финансовом положении, состоянии здоровья и прочие»[1].

Современное зарубежное законодательство во многом повторяет вышеуказанные определения, что и не удивительно, поскольку перечисленные трактовки термина «персональные данные» содержатся в международных актах, которые имплементированы в законодательстве многих государств.

В частности, в большинстве стран Европейского союза термин «персональные данные» аналогично положениям Директив Европейского парламента и Совета ЕС 95/46/ЕС определяются через категорию «идентифицируемость субъекта данных».

Примером может служить Австрийский закон 2000 года, где в ст. 4 сек. 1 дается следующее определение персональных данных:

«…информация, относящаяся к субъекту данных, который

[1] Модельный закон «О персональных данных» принят на 14-м пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ (Постановление № 14–19 от 16 октября 1999 года) // Информационный бюллетень. Межпарламентская ассамблея государств-участников Содружества Независимых Государств. – 2000. – № 23. – С. 315–326.

идентифицирован или может быть идентифицирован»[1]. Практически идентичное положение содержится в ст. 1 Датского закона о защите данных[2]. Аналогичные определения содержатся также в законодательстве Швеции[3] и многих других европейских стран.

Более развернутое определение можно найти в законодательстве Франции[4]: «…персональные данные – это любая информация, относящаяся к физическому лицу, идентифицированному или которое может быть идентифицировано, прямо или косвенно, путем ссылки на идентификационный номер или один, или несколько элементов, которые ему (субъекту) присущи».

Доктринальные определения персональных данных в российской правовой науке не столь уж многочисленны и во многом очень схожи. К примеру, О.Б. Просветова дает ему такую трактовку: «персональные данные – это сведения о фактах, событиях, и обстоятельствах жизни физического лица, его семьи, а также позволяющие отождествить их с конкретным индивидом и отражающие особенности последнего по отношению к другим людям (обществу)»[5].

В.Н. Лопатиным также дает в чем-то похожее определение:

«…персональные данные – информация (зафиксированная на любом носителе) о конкретном человеке, которая отождествляется или может быть отождествлена с ним»[6].

По своему интересным выглядит, по сути говоря, комментарий к

---

[1] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000) (Австрийский закон о защите данных. – *Нем.*). – (http://www.argedaten.at/recht/dsg2000.htm). – Дата обращения: 02.04.2017.

[2] Wet bescherming persoonsgegevens, 2000. (Закон о защите персональных данных Нидерландов. – *Нидер.*). – (https://compri.eu/assets/documentatie/8/origineel/wbp.pdf.) – Ст. 1

[3] Personuppgiftslagen (PuL), 1998. (Шведский закон о защите данных). – (http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204http://www.datainspektionen.se/in-english/legislation/the-personal-data-act/). – Дата обращения: 02.04.2017.

[4] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Закон № 78-17 от 6 января 1978 года «Об информатике, картотеках и свободах». – *Фр.*). – (http://www.cnil.fr/en-savoir-plus/textes-fondateurs/loi78-17/). – Дата обращения: 02.04.2017.

[5] Просветова, О.Б. Защита персональных данных: дис. … канд. юрид. наук / О.Б. Просветова. – М., 2005. – С. 27–28.

[6] Бачило, И.Л. Информационное право / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов. – СПб.: Юридический центр Пресс, 2005. – С. 244.

легальному определению, коллектива авторов (А.Г. Арешев, И.Л. Бачило, Л.А. Сергиенко), которые ориентируются на легальное определение, рассматривая его как общее, в то же время уточняя содержание и значимость рассматриваемой категории следующим образом:

« персональные данные – это такие сведения, которые формируются по личному желанию индивида и на основе закона в процессе контакта индивида со структурами публичной власти, общественными и частными структурами, с другими индивидами в процессе его жизненного цикла, используются в социальной среде в его интересах и в интересах государства на основе международных норм и национального законодательства»[1].

Можно найти и другие определения, но в основном все очень близки к определению, данному законодателем с некоторыми вариациями. Некоторые современные исследования А.В. Кучеренко[2] и А.И. Вельдера[3] не содержат собственного определения персональных данных, видимо, авторы считают его достаточно устоявшимся в науке и практике, сосредотачивая внимание на иных вопросах правового регулирования их оборота.

Во всех перечисленных определениях, с точки зрения автора, присутствует одна и та же логическая неточность, которой достаточно легко было бы избежать. Сразу стоит оговорить, что это не касается определений в международных и зарубежных актах, поскольку в них могут присутствовать ошибки при переводе и семантические неточности, практически всегда возникающие при переводе с одного языка на другой. Неточность состоит в том, что ни в одном из вышеперечисленных случаев термин «персональные данные» не определяется как «данные», а используются при этом более общие категории без соответствующего уточнения: «сведения», «информация», тогда как по логике вещей нужно было бы сделать обратное.

---

[1] Арешев, А.Г. Персональные данные в структуре информационных ресурсов. Основы правового регулирования / А.Г. Арешев, И.Л. Бачило, Л.А. Сергиенко. – М., 2006. – С. 23.

[2] Кучеренко, А.В. Правовое регулирование персональных данных в Российской Федерации: автореф. дис. ... канд. юрид. наук / А.В. Кучеренко. – Челябинск, 2010. – С. 22.

[3] Вельдер, И.А. Система правовой защиты персональных данных в Европейском союзе: автореф. дис. ... канд. юрид. наук / И.А. Вельдер. – Казань, 2006. – С. 27.

По крайней мере, определение персональных данных через категорию «информация», без нужного уточнения, выглядит в некоторой степени нелогично без указания признаков этой информации именно как данных.

Поэтому наиболее правильным подходом в таком случае было бы определить «персональные данные» через категорию «данные» или «информация», в последнем случае указывая на ее отличительные признаки как данных – формализованный характер, в целях их дальнейшей обработки и использования в информационных системах с помощью преимущественно средств автоматизации. Единственным отличительным признаком собственно «персональных данных» на основании предшествующих рассуждений будет то, что эти данные будут об определенном физическом лице, т.е. связаны с ним, вне зависимости от возможности идентификации последнего на их основании.

Интересно, что при анализе Директивы Европейского парламента и Совета ЕС 95/46/ЕС[1] можно сделать вывод, что определенным образом она делает уточнения именно такого характера, не случайно вводя в оборот понятия «файл персональных данных», указывая на определенную структурированность информации, которая позволяет ее включение и нахождение в базах данных/банках данных, информационных системах, а также облегчает возможность поиска по какому-либо ее фрагменту.

Таким образом, предлагаемое автором определение должно выглядеть следующим образом:

Персональные данные – сведения о физическом лице или относящиеся прямо или косвенно к определенному или определяемому на основании таких сведений физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия,

[1] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Ст. 2 и п. 15 Преамбулы. – Дата обращения: 02.04.2017.

доходы, а также другая информация, которая представлена в формализованном виде, обеспечивающем возможность их обработки в информационных системах, преимущественно с помощью средств автоматизации, полностью или частично.

Отметим в указанном определении ключевой признак «персональных данных» – с*вязь лица (субъекта данных) и информации.* Такая связь может быть *прямой* – путем указания на само лицо либо ряд индивидуальных/уникальных черт, характеристик лица, его изображение, голос и т.д., персональные идентификаторы, – а также *косвенной,* когда анализ имеющейся совокупности информации о субъекте неизбежно указывает на него, даже в случае отсутствия прямого указания на это лицо.

Утрата или отсутствие такой связи не позволяет характеризовать информацию как персональные данные. Этим примером является «обезличивание» персональных данных, т.е. разрыв связи между субъектом и некоторой совокупностью информации путем удаления из нее сведений об индивидуальных/уникальных чертах, характеристиках лица, его персональных идентификаторов. Однако вопрос об «обезличенности» данных может вызвать, в свою очередь, и массу других проблем, поскольку применяемые на практике технологии обезличивания данных не гарантируют в полной мере «невозможности» их соотнесения с конкретным лицом[1]. Наиболее часто встречающиеся технологии подчас заключаются лишь в удалении из информационной системы фамилии, имени, отчества, даты рождения, места жительства, персональных идентификаторов и т.п. информации. Зачастую это позволяет операторам снизить расходы на обслуживание систем персональных данных путем разделения информации на собственно базу данных, т.е. информацию и систему персональных идентификаторов/указателей, хранящихся раздельно, для соотнесения в

[1] Волокитина, Е.С. Метод и алгоритмы гарантированного обезличивания и реидентификации субъекта персональных данных в автоматизированных информационных системах: автореф. дис. ... канд. техн. наук: 05.13.19 / Е.С. Волокитина. – СПб., 2013. – С. 24; Шередин, Р.В. Методы и системы защиты информации, информационная безопасность: автореф. дис. ... канд. техн. наук: 05.13.19 / Р.В. Шередин. – М., 2011. – С. 18.

случае необходимости информации с конкретным лицом. В последнем случае оператору приходится прикладывать меньше усилий для защиты «обезличенной информации», защищая в первую очередь информационную систему персональных идентификаторов. В то же время «слабость» такой защиты заключается в потенциальной возможности идентификации субъекта данных на основании совокупности сведений, хранящихся в системе обезличенных персональных данных, а также из других аналогичных или открытых информационных систем, учитывая современные технологические возможности по поиску и обработке информации. Как видно из сказанного, термин «обезличивание» требует определенного, более подробного изучения, в том числе и законодательной трактовки, возможно, с разделением на различные уровни или технологии «обезличивания», гарантирующие в той или иной степени «невозможность» идентификации субъекта с данными.

Другим, своего рода дополнительным критерием отнесения информации к персональным данным является ее содержание – т.е. формализованный характер и связь с информационной системой, когда информация представляет собой обусловленный целями и задачами обработки в информационной системе набор сведений. В действительности обработка персональных данных производится в информационных системах персональных данных и, как правило, такая связь может быть установлена даже в случае ее извлечения из информационной системы, в особенности если в системе обрабатывается уникальный набор данных.

В дополнение к вопросу о терминологии отметим, что в литературе и нормативных источниках вплоть до настоящего времени используется множество синонимичных понятий, так, в частности, можно встретить: «персональные данные», «информация о гражданах», «персональная информация», «информация персонального характера», «личные данные». При кажущейся синонимичности этих понятий следует все-таки провести определенную грань между ними и выделить определенные ситуации и случаи их употребления.

Наиболее часто используемым и часто встречающимся в нормативных актах термином из всех перечисленных выше является термин «персональные данные», несмотря на то, что в подавляющем большинстве законодательных и нормативных актов, где он используется, его трактовка отсутствует, по-видимому, отсылая к терминологии специального законодательства. К таким законодательным актам можно отнести: Кодекс об административных правонарушениях[1] – ст. 13.11, Налоговый кодекс[2] – ст. 84; Воздушный кодекс[3] – ст. 85.1; Федеральный закон «Об актах гражданского состояния»[4] – ст. 12 ч. 1; Федеральный закон «Об основных гарантиях избирательных прав и прав на участие в референдуме граждан Российской Федерации»[5] – ст. 2, п. 52.1; Федеральный закон «О государственной охране»[6] – ст.22; Федеральный закон «О присяжных заседателях судов общей юрисдикции в Российской Федерации»[7] – ст. 5 ч. 3; Федеральный закон «О воинском учете и воинской обязанности»[8] – ст. 8; Федеральный закон «О негосударственных пенсионных фондах»[9] – ст. 15; Федеральный закон «Об обязательном страховании гражданской ответственности владельцев транспортных средств»[10] – ст. 30; Федеральный закон «О государственной регистрации юридических лиц и индивидуальных предпринимателей»[11] – ст. 6 ч. 6; Федеральный закон «Об инвестировании средств для финансирования накопительной части трудовой пенсии в Российской

[1] Кодекс Российской Федерации об административных правонарушениях: от 30.12.2001 № 195-ФЗ (ред. от 03.04.2017).
[2] Налоговый кодекс Российской Федерации (часть первая): от 31.07.1998 № 146-ФЗ (ред. от 28.12.2016).
[3] Воздушный кодекс Российской Федерации: от 19.03.1997 № 60-ФЗ (ред. от 06.07.2016).
[4] Об актах гражданского состояния: федер. закон от 15.11.1997 № 143-ФЗ (ред. от 03.07.2016).
[5] Об основных гарантиях избирательных прав и прав на участие в референдуме граждан Российской Федерации: федер. закон от 12.06.2002 № 67-ФЗ (ред. от 28.12.2016).
[6] О государственной охране: федер. закон от 27.05.1996 № 57-ФЗ (ред. от 03.07.2016).
[7] О присяжных заседателях федеральных судов общей юрисдикции в Российской Федерации: федер. закон от 20.08.2004 № 113-ФЗ (ред. от 03.07.2016).
[8] О воинской обязанности и военной службе: федер. закон от 28.03.1998 № 53-ФЗ (ред. от 03.04.2017).
[9] О негосударственных пенсионных фондах: федер. закон от 07.05.1998 № 75-ФЗ (ред. от 03.07.2016).
[10] Об обязательном страховании гражданской ответственности владельцев транспортных средств: федер. закон от 25.04.2002 № 40-ФЗ (ред. от 03.07.2016).
[11] О государственной регистрации юридических лиц и индивидуальных предпринимателей: федер. закон от 08.08.2001 № 129-ФЗ (ред. от 28.12.2016).

Федерации»[1] – ст. 37; Федеральный закон «О рынке ценных бумаг»[2] – ст. 44 и т.д. Во многих из этих случаев, если не в самом тексте закона, то в тексте подзаконных нормативных актов, дополняющих его положения, содержится примерное указание на то, что же относится к персональным данным, как то: Ф.И.О., дата и место рождения, пол, возраст, а также зачастую специальные сведения, необходимые для реализации целей обработки данных (ИНН, номер пенсионного страхования) и т.п.

В качестве синонима «персональных данных» в законодательстве и нормативных актах часто используется термин «информация о гражданах», обычно их употребление происходит параллельно в тексте, как, например, в Кодексе об административных правонарушениях[3] – ст. 13.11, но можно назвать ряд нормативных актов, где употребление термина «информация о гражданах» происходит без упоминания «персональных данных». К примеру, в ст. 2 Федерального закона «О почтовой связи»[4] или положения Концепции создания системы изготовления, оформления и контроля паспортно-визовых документов нового поколения[5]. Впрочем, это скорее не правило, а исключение, к тому же специальным образом термин «информация о гражданах» в таких случаях не трактуется, что вполне объясняется согласованностью с определением прежнего базового закона «Об информации, информатизации и защите информации»[6].

Некоторое замешательство в большей степени вызывает использование в тексте нормативных актов и в научной литературе терминов: «персональная информация», «информация персонального характера», «информация о личной жизни лица/информация личного характера». Если в

---

[1] Об инвестировании средств для финансирования накопительной пенсии в Российской Федерации: федер. закон от 24.07.2002 № 111-ФЗ (ред. от 28.12.2016).
[2] О рынке ценных бумаг: федер. закон от 22.04.1996 № 39-ФЗ (ред. от 03.07.2016).
[3] Кодекс Российской Федерации об административных правонарушениях: от 30.12.2001 № 195-ФЗ (ред. от 03.04.2017).
[4] О почтовой связи: федер. закон от 17.07.1999 № 176-ФЗ (ред. от 06.07.2016).
[5] Распоряжение Правительства РФ от 15.03.2005 № 277-р «О Концепции создания государственной системы изготовления, оформления и контроля паспортно-визовых документов нового поколения».
[6] Об информации, информатизации и защите информации: федер. закон от 20.02.1995 № 24-ФЗ (ред. от 10.01.2003). (Утратил силу.)

научной сфере они используются часто в качестве синонимов «персональных данных», как правило, для логической разгрузки текста, поскольку различия в таких случаях и придания им специального значения, отличного от «персональных данных», не производится, то в нормативных актах такое употребление выглядит скорее нелогичным, поскольку вполне обоснованно может вызвать вопрос о терминологии, юридическом содержании, толковании и в конечном итоге породить практические трудности. В частности, в Федеральном законе «О социальном обслуживании граждан пожилого возраста и инвалидов»[1] еще не так давно использовался в ст. 7 термин «информация личного характера», а в Федеральном законе «О внешней разведке»[2] в ст. 9 – термин «информация, затрагивающая личную жизнь, честь и достоинство граждан», при этом специальным образом они опять-таки не трактуются. Термин «персональная информация» используется в гл. IV абз. 4 Концепции создания системы персонального учета населения РФ[3], а также в ряде других нормативных актов и научных трудах, как синоним «персональных данных». Законодательство города Москвы тоже использует термин «информация персонального характера»[4], ссылаясь при этом на текст статей 23 и 24 Конституции РФ. Кроме этого, термин «информация персонального характера» был использован в названии законопроекта «Об информации персонального характера»[5], вносимого группой депутатов Государственной Думы, хотя в самом тексте трактовался и использовался лишь термин «персональные данные».

Пожалуй, это лишь небольшой экскурс в столь разнообразную терминологию законодательства, поскольку существуют еще

---

[1] О социальном обслуживании граждан пожилого возраста и инвалидов: федер. закон от 02.08.1995 № 122-ФЗ (ред. от 25.11.2013). (Утратил силу.)

[2] О внешней разведке: федер. закон от 10.01.1996 № 5-ФЗ (ред. от 06.07.2016).

[3] Распоряжение Правительства РФ от 09.06.2005 № 748-р «Об одобрении Концепции создания системы персонального учета населения Российской Федерации».

[4] Об информационных ресурсах и информатизации города Москвы: закон г. Москвы от 24.10.2001 № 52. – Ст. 6 (ред. от 07.05.2014); Об Архивном фонде Москвы и архивах: закон г. Москвы от 28.11.2001 № 67. – Ст. 16 (ред. от 07.05.2014).

[5] Проект Федерального закона № 17844-3 «Об информации персонального характера» (ред., внесенная в ГД ФС РФ, текст по состоянию на 20.10.2000).

законодательные акты, где понятие персональных данных не используется, хотя, несомненно, речь идет о крайне схожих категориях. Федеральный закон «О связи» использует термин «сведения об абонентах-гражданах»[1], в Федеральном законе «Об индивидуальном персонифицированном учете в системе обязательного пенсионного страхования» в ст. 8 употребляется термин «сведения о застрахованных лицах»[2], в Федеральном законе «О правовом положении иностранных граждан в РФ» в ст. 26 – «информация об иностранном гражданине»[3], в Федеральном законе «О всероссийской переписи населения» – «сведения о населении»[4], а также множество других, где, так или иначе, рассматривается вопрос о порядке обработки информации о физических лицах.

Такое видимое разнообразие терминов является скорее дезориентирующим и требует гармонизации и/или унификации терминологии на основе законодательства о персональных данных.

При этом автор считает вполне логичным использование наряду с термином «персональные данные», термина «персональная информация», соотносящиеся как общее и частное. В таком случае «персональными данными» следует считать только ту информацию, которая обрабатывается полностью или частично с помощью средств автоматизации или аналогичным, схожим образом, представленную в формализованном виде, например: в автоматизированных системах, базах данных, библиотеках, архивах, тогда как персональная информация будет наряду с уже сказанным включать в себя весь массив информации об индивиде, независимо от формы их представления и дальнейшего использования и обработки. В целом термин «персональная информация», с учетом вышесказанного, можно было трактовать так:

---

[1] О связи: федер. закон от 07.07.2003 № 126-ФЗ. – Ст. 53 (ред. от 06.07.2016).
[2] Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования: федер. закон от 01.04.1996 № 27-ФЗ. – Ст. 4 (ред. от 28.12.2016).
[3] О правовом положении иностранных граждан в Российской Федерации: федер. закон от 25.07.2002 № 115-ФЗ. – Ст. 26, ч. 2 (ред. от 07.03.2017).
[4] О Всероссийской переписи населения: федер. закон от 25.01.2002 № 8-ФЗ. – Ст. 6 (ред. от 28.03.2017).

Персональная информация – любая информация (сведения, сообщения) о физическом лице, включая информацию о его частной, личной жизни, персональные данные, а также иную информацию (сведения, сообщения) о фактах, событиях и обстоятельствах жизни лица.

Соответственно появление в СМИ или иным образом размещение полностью или частично фрагмента данных, относящихся к физическому лицу, из какой-либо базы данных будет ничем иным как распространением персональных данных, или персональной информацией одновременно. В то же время появление в прессе рассказа или сообщения, содержащего сведения об обстоятельствах жизни физического лица, которые были получены у него лично или от его знакомых, родственников, не подвергаясь обработке с помощью средств автоматизации и не будучи занесенной предварительно в базу/банк данных, будет ничем иным как сообщением персональной информации и никак не персональными данными, к чему в противном случае можно прийти на основании анализа определения, предложенного в законодательстве. Можно привести еще множество таких примеров, где в действительности речь идет именно о персональной информации, которую иногда, видимо неосознанно, называют схожим и синонимичным понятием, но при этом имеющим свою специфику – «персональные данные». Утверждение, что «не всякая информация о личности есть персональные данные», можно найти и у О.Б. Просветовой.[1]

Опасность такого расширительного толкования может привести к смешению существующих правовых институтов и норм, разграничение которых и так вопрос более чем непростой, в частности, как минимум, – права на уважение частной жизни. Поскольку появление сообщений о частной и личной жизни индивида, которые не были извлечены из базы/банка данных или архива, а такое более чем возможно (к примеру, прямое цитирование рассказа очевидца и т.п.), будет затрагивать напрямую

[1] Просветова, О.Б. Защита персональных данных: дис. … канд. юрид. наук: 05.13.19 / О.Б. Просветова. – Воронеж, 2005. – С. 29.

право на уважение частной, личной жизни – самостоятельный хоть и родственный правовой институт, который имеет самостоятельное законодательное регулирование, а не вопрос защиты «персональных данных».

1.3. Содержание и виды персональных данных

Вопрос о юридическом содержании персональных данных и о том, какую информацию следует отнести к ним, также далеко не простой. Учитывая сказанное ранее, можно лишь выделить общий признак информации, которая включается в эту категорию, а именно – информация (сведения, сообщения) о физическом лице, которая отождествляется с ним или может быть отождествлена с ним, о нецелесообразности использования критерия «идентификации» было уже сказано выше. Как видно, это крайне широкая трактовка, в рамках которой можно было бы выделить и перечислить все возможные виды сведений. Но такие попытки были – О.Б. Просветова в своем диссертационном исследовании, высказываясь за необходимость установления исчерпывающего перечня конфиденциальных сведений о гражданах (персональных данных), с сожалением отмечала, в частности, отказ от исчерпывающего перечня при создании Модельного закона о персональных данных, также при создании проекта Федерального закона «О персональной информации»[1]. Ею был предложен достаточно исчерпывающий перечень сведений, относимых к конфиденциальной информации о гражданах[2], включающий 34 позиции, из которых, все-таки в последней позиции, были названы «иные данные»: фамилия, имя, отчество, дата и место рождения, пол, гражданство, национальность, отношение к воинской обязанности, адрес места жительства/пребывания, семейное положение, информация о членах семьи, сведения о доходах, номера электронной почты, телефонов, место работы, должность, данные паспорта, дипломов об окончании учебных заведений, дактилоскопическая информация, медицинская информация, информация о политических взглядах, религиозных и иных убеждениях, о содержании личных разговоров, государственный номер транспортного средства, водительский стаж, личные коды, персональные идентификаторы и др.

---

[1] Просветова, О.Б. Защита персональных данных: дис. … канд. юрид. наук: 05.13.19 / О.Б. Просветова. – Воронеж, 2005. – С. 28–30.
[2] Там же. – С. 33–34.

В.Н. Лопатин приводит следующий примерный перечень персональных данных[1], который примерно совпадает с перечнем уже упомянутого Модельного закона о персональных данных:

– «биографические и опознавательные данные (в том числе об обстоятельствах рождения, усыновления и развода);

– личные характеристики (в том числе о личных привычках и наклонностях);

– сведения о семейном положении (в том числе о семейных отношениях);

– сведения об имущественном, финансовом положении (кроме случаев, прямо установленных в законе);

– сведения о состоянии здоровья»[2].

М. Савинцева[3] скорее высказывается за существование открытого перечня сведений, относимых к персональным данным, отмечая при этом отсутствие необходимости в этом, ссылаясь на примерный перечень, данный федеральным законом – «фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия, доходы, другая информация»[4], который, по-видимому, необходим лишь для раскрытия содержания понятия.

В.П. Иванский в своей классификации, базирующейся на анализе зарубежного законодательства о защите данных, основывает ее на критерии *«чувствительности»* и выделяет три категории персональных данных:

– *««обычные»* персональные данные – их сбор, обработка, использование и передача возможны без специального разрешения в режиме, предписанном национальными законами;

---

[1] Бачило, И.Л. Информационное право / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов. – СПб.: Юридический центр Пресс, 2005. – С. 245.

[2] Модельный закон «О персональных данных» принят на 14-м пленарном заседании Межпарламентской ассамблеи государств-участников СНГ (Постановление № 14-19 от 16 октября 1999 г.) // Межпарламентская Ассамблея государств-участников Содружества Независимых Государств: Информационный бюллетень. – 2000. – № 23. – С. 315–326. – Ст. 2.

[3] Савинцева, М. Правовая защита персональной информации граждан в России / М. Савинцева. // Законодательство и практика масс-медиа. – М., 2006.– № 9 (сент.) – С. 7.

[4] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017). – Ст. 2.

– *«чувствительные»* персональные данные – их сбор, обработка, использование и передача требуют особых мер защиты и безопасности, специально установленных законом;
– *«особо чувствительные»* персональные данные – их сбор, обработка, использование и передача либо вообще запрещены законом, либо разрешены только в исключительных случаях с использованием специальных мер защиты и безопасности»[1].

М. Бибент[2], как и многие другие европейские ученые, использует другой подход к определению содержания персональных данных, которые он именует скорее как идентифицирующие данные (données nominatives), где особо выделяются медицинские данные; чувствительные данные (о членстве в религиозных, общественных организациях, политических партиях и т.д.); данные о правонарушениях и оперативные данные.

В основном подобные примерные перечни скорее называют категории сведений, исходя из сфер жизни индивида, которые описываются ими, но это далеко не единственный вариант классификации или категоризации персональных данных. К примеру, можно встретить классификацию, исходя из принципа разграничения доступа к ним, на основании которой можно выделить:

– *«открытые* персональные данные, которые гражданин раскрывает добровольно или обязан раскрывать по требованию государства без гарантий их защиты, как то: приобретение товара в магазине или сведения об открытой (публичной) деятельности лица;
– персональные данные *ограниченного доступа*, которые государство обязывает граждан раскрывать, принимая на себя обязательства по их охране, а также сведения, переданные третьим лицам на условиях сохранения их конфиденциальности;

[1] Иванский, В.П. Правовая защита информации о частной жизни граждан. Опыт современного правого регулирования: монография / В.П. Иванский. – М.: Изд-во РУДН, 1999. – С. 12.
[2] Bibent, M. Le Droit du Traitement de l'Information / M. Bibent. – Paris: ADBS, Nathan, 2000. – P. 46–48.

– персональные данные *ограниченного доступа, представляющие собой охраняемую законом тайну*, для тех граждан, которым они были доверены по роду службы (профессии) – профессиональная тайна (служебная, налоговая, адвокатская, банковская, тайна следствия и т.д.);
– *личные (персональные) тайны* – данные, которые лицо или группа лиц (семья и т.п.) считает своей тайной и по поводу которой он (они) берет(ут) на себя добровольные обязательства по предотвращению их разглашения путем недопущения доступа к ним со стороны третьих лиц»[1].

Личные тайны при этом можно также подразделить на общепринятые и частноопределяемые тайны[2]. К общепринятым, в таком случае, следует отнести, к примеру, данные об интимных сторонах жизни индивида или его семьи, разглашение которых способно нанести моральный вред с точки зрения морали и нравственности. Частноопределяемыми тайнами могут быть данные, которые лицо по собственному желанию не хочет и не желает раскрывать и по защите которых государство не несет никаких обязательств.

В.Я. Ищейнов[3] предлагает разделить персональные данные:

- на физические;
- физиологические;
- соотносительные данные.

К числу физических и физиологических данных, по его мнению, следует отнести: пол, возраст, цифровой образ лица, отпечатки пальцев, ладоней и т.д. Соотносительные данные включают в себя: место и время рождения, расовое, этническое происхождение, политические взгляды др. В таком случае вполне можно согласиться с мнением А.В. Кучеренко

[1] Каптерев, А. Концепция персональной информации / А. Каптерев. – 2004. – (http://prompolit.ru/151796). Дата обращения: 02.04.2017.
[2] Там же.
[3] Ищейнов, В.Я. Персональные данные в законодательных и нормативных документах Российской Федерации и информационных системах / В.Я. Ищейнов // Делопроизводство. – 2006. – № 3. – С. 90.

о целесообразности использования такой классификации скорее в целях делопроизводства, нежели правового регулирования[1].

Н.И. Петрыкина[2] предложила делить персональные данные по степени их "оборотоспособности", выделив при этом следующие категории:

- свободно обращаемые (Ф.И.О., адрес, номер телефона, электронная почта и пр.);
- ограниченно обращаемые (регистрационные номера, дата рождения, образование, семейное положение, наличие детей, состояние здоровья и др.);
- запрещенные к обороту (специальные персональные данные).

Такая классификация, по-своему логична, но в некоторой степени не согласуется с основной идеей зашиты персональных данных, которая предполагает в первую очередь волеизъявление субъекта — т. е. право выбора конкретного правового режима своих данных.

Вероятно, можно предложить и другие классификации «персональных данных», скажем в зависимости от целей их обработки (коммерческие, управленческие, поддержание безопасности и охрана порядка), способов обработки (с использованием или без использования средств автоматизации), от вида оператора (частный, публичный) возможны и другие, однако все они, пожалуй, имеют меньшую «ценность» и используются реже, чем уже названные.

Интерес вызывает также выделение и существование особых видов персональных данных, которые специально указываются как в зарубежной и международной практике, так и в российском законодательстве и доктрине. Речь идет, в частности, о таких категориях, как «общедоступные персональные данные», «идентифицирующие данные», «чувствительные данные (информация)».

---

[1] Кучеренко, А.В. Правовое регулирование персональных данных в Российской Федерации: дис. … канд. юрид. наук / А.В. Кучеренко. – Челябинск, 2010. – С. 82.

[2] Петрыкина, Н.И. Некоторые вопросы регулирования оборота персональных данных в РФ / Н.И. Петрыкина // Московский журнал международного права. – 2007. – № 2. – С. 78–79.

Среди названных стоит отдельно остановиться на категории «чувствительной информации/данных» (sensitive information или données sensibles) – эта категория персональных данных выделяется практически в подавляющем количестве случаев, хотя в целом одним из первых источников, который дает их перечень, является Директива Евросоюза № 95/46/ЕС[1] (далее – Директива). В ст. 8 содержится перечень особых категорий персональных данных – раскрывающих расовое или этническое происхождение, политические взгляды, вероисповедание или философское воззрение, членство в профессиональном союзе, а также обработку данных, касающихся здоровья или интимной жизни. Именно эти данные принято именовать «чувствительными»[2]. Особое отношение к ним объясняется в п. 33 преамбулы Директивы[3], где недвусмысленно говорится о повышенной потенциальной опасности нанести вред фундаментальным правам и свободам при обработки этих категорий персональных данных, имея в виду право на неприкосновенность частной жизни. Особый характер выражается в том числе и в особом предполагаемом характере обработки этих данных. Рассматриваемая ст. 8 Директивы содержит, что немаловажно, общий запрет на обработку указанных данных, допуская лишь в качестве исключения ряд строго определенных случаев, когда их обработка возможна:

– наличие ясно выраженного согласия лица, исполнение законного обязательства контролера в соответствии с трудовым законодательством;

– обработка необходима в медицинских, диагностических целях;

– обработка необходима для обеспечения жизненно важных интересов лица, других субъектов;

– обработка осуществляется фондом или ассоциацией в отношении данных о своих членах при условии соблюдения надлежащих гарантий;

---

[1] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Дата обращения: 02.04.2017.

[2] Braibant, G. Données personnelles et société de l’information / G. Braibant. – Paris, 2000. – P. 76–77.

[3] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Дата обращения: 02.04.2017.

– обработка осуществляется в целях защиты публичного интереса.

Интересно, что в этой же статье содержится упоминание о данных, касающихся правонарушений, уголовного наказания или мер безопасности, обработка которых должна осуществляться только под контролем официального органа и персональных идентификаторов. Тем самым можно говорить об отнесении этих данных к категории особых, при этом их обработка должна регулироваться особым образом, самостоятельно государствами-участниками.

Российский закон о персональных данных также выделил фактически аналогичную категорию персональных данных, назвав их в статье 10 «специальными категориями персональных данных»[1], положения которой мало чем отличаются концептуально от положений Директивы, как в части установления общего запрета на их обработку, так и в части определения исключений, выделив в самостоятельную группу «биометрические данные».

В целом выделение «особой категории персональных данных (чувствительных данных)» более чем целесообразно и служит не чем иным, как существенной гарантией защиты фундаментальных прав личности и, в первую очередь, права на неприкосновенность частной жизни, угроза нарушения которого повышается в случае обработки таких данных.

Существенный интерес вызывает вопрос об обособлении категории «идентификационные данные», которые в зарубежных источниках иногда еще называют “information nominative”[2]. С одной стороны, если вернуться к вопросу о понятии персональных данных у тех авторов, которые в качестве основного критерия выделения такой категории вообще указывали «идентификацию», то вполне возможно было бы установить знак равенства между ними. В то же время, как уже упоминалось, такой критерий выделения не является столь уж удачным и ставит сложный, практически риторический вопрос о возможности или невозможности идентификации той или иной

[1] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017).
[2] Braibant, G. Données personnelles et société de l’information / G. Braibant. – Paris, 2000. – P. 76–77.

личности на основании некой совокупности сведений, хотя, безусловно, в большинстве случаев она возможна. Но есть и еще один, тоже достаточно существенный аргумент в пользу выделения категории идентификационных данных – это выделение специальных категорий информации, персональных идентификаторов, которые создаются и используются исключительно для целей идентификации личности с соответствующим файлом досье в определенной базе данных. К таким данным, в частности, следует отнести:

– паспортные данные, данные удостоверений личности (личные данные);

– персональные идентификаторы (ИНН, номер пенсионного и социального страхования, номер полиса обязательного медицинского страхования);

– биометрические данные, традиционно используемые для идентификации личности: отпечатки пальцев, особенности радужной оболочки глаза и т.д.

Все перечисленные категории сведений используются, как правило, исключительно для идентификации личности, которая возможна без каких-либо серьезных криминалистических исследований, за исключением биометрических данных, при условии, что они не считываются электронными устройствами. Сюда же можно отнести сведения о едином гражданском номере – ЕГН, существование которого или его аналогов вызывало и вызывает многочисленные споры, а в некоторых государствах он уже существует. В России тоже были попытки введения ЕГН на уровне законодательных положений, в частности при разработке проекта закона «О персональных данных», текст которого к первому чтению в статье 24 содержал положения о «едином государственном регистре населения», куда бы заносились «идентификаторы персональных данных» (уникальные и постоянные номера, присваиваемые физическим лицам органами государственной власти и местного самоуправления) всех физических лиц,

постоянно или временно проживающих или пребывающих на территории Российской Федерации.

Вопрос об идентифицирующих данных интересен еще и потому, что последнее время появляются предложения не только о выделении такой категории, но и о придании им статуса общедоступных сведений, что отчасти не лишено некоторого смысла. Речь в первую очередь идет о паспортных и аналогичных им данных о лице, которые используются повсеместно для его идентификации как такового, и, безусловно, такой возможностью должны обладать не только органы государства или государственные структуры, но и другие субъекты, организации. Речь идет в том числе и о паспортной базе данных, и о базе данных по потерянным паспортам, которые доступны только органам государственной власти, что лишает возможности других субъектов идентифицировать лицо и сравнить представленные им сведения с общей базой данных. Дефицит идентифицирующей информации привел во многом к существованию «серых» баз данных УФМС, ГИБДД, БТИ. Проблема отчасти усугубляется и тем, что сам индивид очень часто и повсеместно сообщает свои паспортные данные, данные удостоверения личности другим субъектам по самому различному поводу. Несмотря на рациональное зерно в таких рассуждениях и проблеме закрытости идентифицирующей информации о лице для других субъектов, что во многом необходимо для снижения рыночного риска, неопределенности и повышения доверия между субъектами общественных отношений, вопрос о переводе идентификационных данных в разряд общедоступной информации требует более тщательного дальнейшего изучения, какие категории идентификационных данных целесообразно перевести в разряд общедоступных.

Своеобразная категория персональных данных была введена Федеральным законом о персональных данных – это «общедоступные

персональные данные»[1] в его прежней редакции до 25 июля 2011 г. В ст. 3 они были определены как «персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных либо на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности». Исходя из определения, можно четко выделить два основания перевода персональных данных в категорию общедоступных: согласие субъекта персональных данных, предписание федерального закона. Однако вопрос не такой уж простой на самом деле. Касательно раскрытия персональных данных по требованию закона здесь все достаточно понятно, и речь идет о персональных данных политических и общественных деятелей, которые становятся общедоступными в силу предписаний закона в соответствии с избирательным и налоговым законодательством и иными актами, как то – сведения о доходах и биографические данные, сообщаемые кандидатами или лицами, занимающими государственные должности. Сложности возникают там, где речь идет о соотнесении категорий общедоступной информации, которая в соответствии с законом определяется как «информация, доступ к которой не ограничен, или общеизвестные сведения»[2]. В этой связи встает вопрос, является ли распространение персональных данных через средства массовой информации тем, что делает их общеизвестными сведениями? Безусловно, да, но вот общедоступными, видимо, с точки зрения законодателя, нет. Возникает логически странная ситуация, когда сведения стали общеизвестными, но не общедоступными и запрещенными к обработке без согласия субъекта, тогда как единожды ставшая общеизвестной и общедоступной, информация не может быть переведена снова в разряд конфиденциальной, поскольку последняя по своей природе не может быть общеизвестной. В своем исследовании А.В. Кучеренко также подчеркивает, что «общедоступные персональные данные» и «общедоступные источники

[1] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017).
[2] Об информации, информационных технологиях и о защите информации: федер. закон от 29.07.2006 № 149-ФЗ (ред. от 19.12.2016). – Ст. 7.

персональных данных» не одно и то же[1]. Появление рассматриваемой категории в российском законе было своеобразной новеллой, поскольку, если говорить о европейской практике, то там используется лишь указание на общедоступные источники персональных данных[2], но вот об общедоступных персональных данных нигде больше не упоминается. Видимо, осознание этих негативных моментов в конечном итоге и привело к отказу от использования в законодательстве категории «общедоступные персональные данные». В действительности гораздо проще оперировать понятиями «общедоступная информация» и «персональные данные», учитывая, что последние могут быть также и общедоступной информацией, что в свою очередь не исключает необходимости их обработки, использования без ущерба правам и интересам физического лица, субъекта персональных данных.

Еще одной категорией персональных данных, которая вызывает некоторые споры среди ученых, является категория «оценочные персональные данные». Так, в частности, Ю.В. Травкин высказался в пользу того, что «к персональным данным относятся также мнения о данном человеке, объективные или субъективные, если они зафиксированы и соотнесены с данным человеком»[3].

Бесспорно, что поскольку персональные данные могут быть любой информацией о лице, предположительно они могут включать субъективное мнение о человеке со стороны других лиц. На основании таких предположений И.А. Вельдер предложил выделение особой категории – «персональные данные оценочного характера»[4] (аналогичная категория

---

[1] Кучеренко, А.В. Правовое регулирование персональных данных в Российской Федерации: автореф. дис. ... канд. юрид. наук / А.В. Кучеренко. – Челябинск, 2010. – С. 86.

[2] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Дата обращения: 02.04.2017.

[3] Травкин, Ю.В. Персональные данные / Ю.В. Травкин. – М.: Амалданик, 2007. – С. 33.

[4] Вельдер, И.А. Система правовой защиты персональных данных в Европейском союзе: дис. ... канд. юрид. наук: 12.00.10 / И.А. Вельдер – Казань, 2006. – С. 47.

использовалась также в ст. 85 Трудового кодекса РФ)[1], которые в действительности не могут объективно характеризовать субъекта и не совсем соотносятся с положениями законодательства о персональных данных, требующего в большинстве случаев «точности», «актуальности»[2], которые часто отождествляют с понятием «достоверность». На том же основании А.В. Кучеренко возражает в принципе от использования указанных терминов и характеристики их в качестве персональных данных как таковых, предлагая взамен термин «персональная информация» по аналогии с законодательством Чехии и Японии[3]. Несмотря на то, что указанные предложения не лишены определенной доли логики, все же появление категории «оценочные персональные данные» скорее было бы ошибкой. На самом деле термины «актуальность» и «точность», а также «достоверность» не совсем применимы к категории «суждения» или «мнения», которые, безусловно, являются не более чем субъективными предположениями, передают чувства и настроения людей, их внутреннее мироощущение и восприятие действительности. В частности, Европейский суд по правам человека не раз в своих решениях уделял внимание трактовке терминов «факты» в противовес «мнениям» и «оценочным суждениям». Анализ этой практики[4] позволяет говорить о том, что категории «достоверность», «истинность» неприменимы в полной мере в случае, если речь идет о «мнении» или «оценочном суждении», которые подчас сложно подтвердить или опровергнуть. Следовательно, можно предположить, что по отношению к содержанию «оценочных персональных данных» также неприменима категория их «истинности» или «достоверности», за исключением указания на их автора или обстоятельства их появления и т.п. С другой стороны, использование термина «персональная

[1] Трудовой кодекс Российской Федерации от 26.12.2001 № 197-ФЗ // Собрание законодательства Российской Федерации. – 2002. – № 1. – Ст. 3. – Ст. 85. (Статья утратила силу в соответствии с Федеральным законом от 7.05.2013 № 99-ФЗ // Собрание законодательства Российской Федерации. – 2013. – № 19. – Ст. 2326.)

[2] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ // Российская газета. – 2006. – 27 июля. – Ст. 5

[3] Кучеренко, А.В. Правовое регулирование персональных данных в Российской Федерации: – дис. … канд. юрид. наук / А.В. Кучеренко. – Челябинск, 2010. – С. 59.

[4] Маковей, М. Европейская конвенция о защите прав человека и основных свобод. Ст. 10: Право на свободу выражения своего мнения. Прецеденты и комментарии / М. Маковей, Е.А. Чефранова. – М., 2001. – С. 12.

информация» по отношению к ним также не выглядит убедительным, ввиду того что такая информация также может накапливаться в информационных системах наряду с достоверными фактами и обстоятельствами, более того, говорить об отсутствии интереса субъекта по защите этой информации как «не персональных данных» тоже не приходится – такое деление вызвало бы массу проблем в правоприменительной практике, поскольку по своей сути эта информация обладает всеми признаками персональных данных.

Следуя логике того же Европейского суда по правам человека, «оценочные персональные данные» являются такими же «персональными данными», как и другие, и к ним также применяются требования по их «актуальности» и «точности».

Относительно формы представления персональных данных также следует сделать некоторые весьма существенные комментарии, которые, по мнению автора, будут не лишними. Естественно, что чаще всего называются такие наиболее очевидные случаи представления персональных данных, как то: данные о подписчиках, клиентские базы данных. Поскольку речь о данных идет, прежде всего, применительно к информации, которая предназначена для автоматизированной обработки и представлена чаще всего в виде совокупности знаков или кодов, то вот о причислении к персональным данным видео-, фотоизображений, звукового ряда как-то иногда забывают, хотя это такие же формы представления информации, как и другие. К примеру, зарубежные авторы идут даже несколько дальше, не только рассматривая подобные формы представления информации, сведений как формы персональных данных, но также поднимая и другие немаловажные, связанные с этим проблемы, в частности, проблему регистрации или сообщения о наличии систем видеонаблюдения или прослушивания в учреждениях и организациях, которые также являются средствами сбора персональной информации, которая затем проходит

автоматизированную обработку или с использованием автоматизированных средств[1].

На основании анализа положений сферы действия специального законодательства о защите данных, в частности ст. 1 уже упомянутой Директивы 95/46/ЕС[2] и ст. 1 Федерального закона «О персональных данных»[3], можно говорить также и об еще одной особой группе персональных данных – персональные данные, на которые распространяется специальный правовой режим их защиты. Это становится очевидным, поскольку в указанных положениях прямо говорится о тех персональных данных, на которые не распространяется действие указанных документов, равно как и особый режим конфиденциальности, предусмотренный ими. Следовательно, основным отличием этой группы персональных данных как раз и будет их охрана – установление особого порядка доступа к ним, выраженного в самостоятельном, специальном правовом режиме. Именно этот вид персональных данных представляет наибольший интерес в контексте данной работы и требует дальнейшего изучения, равно и их правовой режим. Именно этот вид персональных данных представляет наибольший интерес в контексте настоящего диссертационного исследования.

[1] Commission nationale de l'information et des libertés, Voix, Image et Protection des Données Personnelles. – Paris, 2005. – P. 17–20.
[2] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Дата обращения: 02.04.2017.
[3] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017).

ГЛАВА 2. ПЕРСОНАЛЬНЫЕ ДАННЫЕ КАК ИНФОРМАЦИЯ ОГРАНИЧЕННОГО ДОСТУПА

2.1. Понятие и система информации ограниченного доступа

Конституция Российской Федерации, согласно международным стандартам в области прав и свобод личности, в статье 29 прямо закрепляет «право свободно искать, получать, передавать, производить и распространять информацию любым законным способом»[1]. При этом в статье 55 ограничения этого права возможны «только федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства»[2].

Федеральный закон «Об информации, информационных технологиях и о защите информации»[3] в статье 3 части 1 указывает в числе основных принципов регулирования информационной сферы – принцип «свободы поиска, получения, передачи, производства и распространения информации любым законным способом» и «установление ограничений доступа к информации только федеральными законами». Суть этого принципа подробно раскрывается в статье 5, согласно которой информацию следует подразделять по категории доступа на информацию общедоступную и информацию, доступ к которой ограничен в соответствии с федеральными законами (информацию ограниченного доступа). Указанные положения соответствуют в целом логике права и направлены на достижение необходимого баланса интересов между правом на информацию, включая право на доступ к информации, и необходимостью обеспечения защиты прав и законных интересов других лиц посредством установления ограничений в доступе к той или иной информации.

---

[1] Конституция (Основной закон) Российской Федерации от 12.12.1993 // Российская газета. – 1993. – 25 дек.
[2] Там же.
[3] Об информации, информационных технологиях и о защите информации: федер. закон от 29.07.2006 № 149-ФЗ (ред. от 19.12.2016).

Со временем необходимость защиты интересов общества, государства и частных лиц привела к появлению достаточно большого количества правовых конструкций, предусматривающих ограничение доступа к информации. К таким случаям можно отнести: различного рода «тайны», «секреты», «конфиденциальную информацию». При этом разнообразие терминологии в указанной сфере связано как с особенностями заимствования (перевода) терминов и правовых институтов из зарубежного законодательства и практики, так и с некоторыми специфическими особенностями терминологии в различных сферах деятельности или отраслях права.

Скорее всего, преимущественно этим обстоятельством можно объяснить особенности употребления терминологии «секретный» или «секретность» в советском и затем в российском законодательстве и праве в отношении института государственной тайны или появление термина «секрет производства (ноу-хау)», что стало неожиданным, по мнению некоторых авторов[1], в части 4 Гражданского кодекса РФ[2].

Проблема систематизации законодательства в сфере установления ограничений на доступ к информации и в целом права на информацию уже неоднократно обозначалась современными исследователями и практиками. К примеру, по оценкам разных авторов, в действующем российском законодательстве можно обнаружить от 30 до 70[3] разновидностей «тайн» и иных видов информации, доступ к которой ограничивается, находящих отражение в нормативно-правовых актах, подчас никак не связанных между собой[4].

По этим причинам, следует последовательно подойти к рассмотрению этой проблематики, начав с изучения правовой природы данных явлений и

---

[1] Информационное право. Актуальные проблемы теории и практики / Под ред. И.Л. Бачило. – М.: Юрайт, 2009. – С. 455.

[2] Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 03.07.2016, с изм. от 28.03.2017) (с изм. и доп., вступ. в силу с 01.01.2017).

[3] Городов, О.А. Информационное право: учебник. / О.А. Городов. – М.: ТК Велби, изд-во Проспект, 2008. – С. 62.

[4] См., напр.: Лопатин, В.Н. Концептуальные основы развития законодательства в сфере обеспечения информационной безопасности / В.Н. Лопатин // Управление защитой информации. – Минск – М., 1999. – Т. 3 – № 1. – С. 27–35.

уточнения терминологии, и затем перейти к вопросу о систематизации различных видов информации с ограниченным доступом в действующем российском законодательстве и праве.

В целом, саму идею ограничения доступа к информации следует связать с укоренением в законодательстве и практике категории «тайна», как, например, «государственная тайна», которая нашла отражение еще в законодательстве Российской империи о шпионаже[1]. В то же время, сам термин «тайна» в исторической ретроспективе стоит рассматривать как общий для обозначения существования ограничений доступа к той или иной информации. В частности, в работах некоторых авторов еще в дореволюционной России можно встретить упоминания об иных разновидностях тайн, которые сейчас уже широко известны науке и практике, к примеру, промысловая тайна, как разновидность коммерческой тайны[2], или адвокатская тайна[3] и т.д.

В различной справочной литературе и источниках термину «тайна» дается достаточно простое определение – «нечто скрываемое от других, известное не всем, секрет»[4]. В Толковом словаре В. Даля приводится два значения термина «тайна». В широком смысле: «тайна – кто чего не знает, то для него тайна; все сокрытое, неизвестное, неведомое»[5]; и в узком смысле: «тайна – нечто скрытно хранимое, что скрывают от кого-либо с намерением таить»[6]. Безусловно, такую трактовку можно рассматривать как «бытовую», в то же время, отметим, что к праву и рассматриваемому нами явлению ближе второе, более «узкое» понимание «тайны», сформулированное у В. Даля.

Современная наука и законодательство характеризуются неоднозначным подходом к пониманию термина «тайна» и ее места в системе

---

[1] Столяров, Н.В. Организация защиты государственной тайны в России / Н.В. Столяров. – (http://www.sec4all.net/gostaina-russ.html). – Дата обращения: 02.04.2017.
[2] Розенберг, В. Промысловая тайна / В. Розенберг. – СПб.: Типогр. редакции Министерства финансов, 1910. – С. 8.
[3] Цыпкин, А.Л. Адвокатская тайна / А.Л. Цыпкин. – Саратов: СГУ, 1947. – С. 40.
[4] Ожегов, С.И. Словарь русского языка / С.И. Ожегов. – М.: Русский язык, 1984. – С. 683.
[5] Даль, В. Толковый словарь / В. Даль. – М., 1955. – Т. 4. – С. 386.
[6] Там же.

права, что не раз отмечалось многими учеными и становилось предметом обсуждений. Различные трактовки термина «тайна» можно встретить в работах Л.О. Красавчиковой, Л.Е. Владимирова, О.А. Городова, И.В. Смольковой, И.В. Бондаря, А.А. Фатьянова, М.А. Вуса, С.В. Кузьмина и других авторов.

К примеру, один из видных ученых-юристов дореволюционной России Л.Е. Владимиров понимал под тайной «сохранение в негласности обстоятельства, разглашение которого принесло бы больше вреда, чем пользы, понимая последнюю не только в смысле утилитарном, но и в смысле отвлеченном, т.е. ограждение существования и питания нравственных идеалов человеческого совершенствования»[1].

Как это справедливо отмечено у И.В. Смольковой, такое определение скорее несет в себе больше нравственную, чем правовую нагрузку и может рассматриваться как «принцип, отражающий интересы человеческой культуры»[2].

Л.О. Красавчикова в своих трудах приводит следующее определение тайны – «определенная информация о действиях (состоянии и иных обстоятельствах) определенного лица (гражданина, организации, государства), не подлежащая разглашению»[3]. Такое определение, по мнению И.В. Смольковой, не лишено недостатков, так как оно «не включает ряд существенных признаков тайны, связанных с обязанностями хранить тайну и ответственностью за ее разглашение»[4].

Достаточно широко известным считается понятие тайны, данное в работах И.В. Смольковой, которая определяет ее как «особым образом охраняемый законом блок секретной или конфиденциальной информации (сведений), известной или доверенной узкому кругу субъектов в силу

---

[1] Владимиров, Л.Е. Учение об уголовных доказательствах. Части Общая и Особенная / Л.Е. Владимиров. – Спб., 1910. – С. 304.
[2] Смолькова, И.В. Проблемы охраняемой законом тайны в уголовном процессе / И.В. Смолькова. – М.: Луч, 1999. – С. 12–13.
[3] Красавчикова, Л.О. Личная жизнь под охраной закона / Л.О. Красавчикова. – М., 1983. – С. 119
[4] Смолькова, И.В. Указ. соч. – С. 13.

исполнения служебных, профессиональных и иных обязанностей или отдельных поручений, разглашение которых может повлечь юридическую ответственность»[1].

М.В. Мазуров, весьма положительно высказавшийся об определении И.В. Смольковой, дополняет его и дает ему такую трактовку: «тайна – это охраняемые законом конфиденциальные и секретные сведения в области частной жизни граждан, предпринимательской, финансовой, политической, экономической, военной и иных сферах, известные или доверенные определенному кругу лиц в силу их профессиональных, служебных и иных обязанностей, незаконное получение, использование, разглашение которых причиняет вред или создает угрозу причинения вреда правам и законным интересам граждан, общества, государства и влечет за собой ответственность виновных лиц в соответствии с действующим законодательством»[2].

В итоге можно говорить о том, что в современной науке сформировались два «основных» подхода к пониманию феномена тайны. Согласно первому из них тайну следует понимать как сведения, доступ к которым ограничен, т.е. саму информацию или объект правоотношений. (М.А. Вус, А.А. Фатьянов, В.А. Мазуров, И.В. Смолькова). Отметим, что именно указанный подход в целом доминирует в современном законодательстве, несмотря на то, что его позиции несколько ослабевают. В числе примеров можно указать Закон РФ «О государственной тайне», где в статье 2 она понимается как «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ»[3]. В таком определении достаточно явно просматривается указание именно на информацию и/или сведения. Аналогичный подход к понятию тайны можно

[1] Там же. – С. 23.
[2] Мазуров, В.А. Тайна: государственная, коммерческая, банковская, частной жизни: Уголовно-правовая защита: Учебное пособие / В.А. Мазуров / Под научн. рук. д-ра юрид. наук, проф. С.В. Землюкова. – М.: Издательско-торговая корпорация «Дашков и К°», 2003. – С. 27.
[3] О государственной тайне: закон РФ от 21.07.1993 № 5485-1 (ред. от 08.03.2015).

заметить в ч. 1 ст. 102 Налогового кодекса (налоговая тайна)[1]; ст. 1123 Гражданского кодекса (тайна завещания)[2]; ст. 13 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» (врачебная тайна)[3]; ст. 15 Федерального закона «О связи» (тайна связи)[4]; ст. 26 Федерального закона «О банках и банковской деятельности» (банковская тайна)[5] и во многих других случаях.

Второй подход трактует термин «тайна» через указание на определенный правовой режим информации, как это делает О.А. Городов[6]. В таком понимании использование термина «тайна» в законодательстве и практике является скорее определением правового режима информации нежели самой информации. Это можно объяснить тем, что ограничение доступа к информации приводит к ее неизвестности (энтропии) для третьих лиц, по отношению к этой информации. Таким образом, для обладателя это – не тайна, а для третьих лиц – не информация, следовательно, понятие «тайна» не следует сводить к информации. Такой подход был частично использован в информационном законодательстве. В частности, в Федеральном законе «О коммерческой тайне»[7], где в статье 3 термин «тайна (коммерческая тайна)» трактуется как «режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду». Иначе говоря, анализ положений действующего Федерального закона «Об информации, информационных технологиях и о защите информации» также

---

[1] Налоговый кодекс Российской Федерации от 31.07.1998 № 146-ФЗ, часть первая //СЗ РФ. – 1998. – № 31. – Ст. 3824.

[2] Гражданский кодекс Российской Федерации (часть третья) от 26.11.2001 № 146-ФЗ (ред. от 28.03.2017) // СЗ РФ. – 2001. – № 49. – Ст. 4552.

[3] Об основах охраны здоровья граждан в Российской Федерации: федер. закон от 21.11.2011 № 323-ФЗ (ред. от 03.04.2017).

[4] О связи: федер. закон от 07.07.2003 № 126-ФЗ (ред. от 06.07.2016).

[5] О банках и банковской деятельности: федер. закон от 02.12.1990 № 395-1 (ред. от 03.07.2016 г.) (с изм. и доп., вступ. в силу с 01.01.2017).

[6] Городов, О.А. Информационное право: учебник / О.А. Городов – М.: ТК Велби, изд-во Проспект, 2008. – С. 64.

[7] О коммерческой тайне: федер. закон от 29.07.2004 № 98-ФЗ (ред. от 12.03.2014).

свидетельствует о том, что при его разработке использовался в большей степени второй подход, поскольку в нем в качестве указания на информацию ограниченного доступа используется термин «конфиденциальность»[1]. О.А. Городов при анализе этих положений закона однозначно делает вывод о синонимичности понятий «тайна» и «конфиденциальность»[2].

Откровенно говоря, такое понимание термина «тайна» не лишено определенной притягательности, но в то же время здесь следует отметить и некоторые отрицательные моменты такого подхода. Следуя этой логике, мы вполне можем столкнуться с проблемой субъективности восприятия, т.е. известность или неизвестность той или иной информации для субъекта, напротив, обозначение «тайны» как информации (сведений) лучше конкретизирует общественные отношения через их объект.

В дополнение к вышеуказанному можно упомянуть еще об одной трактовке термина «тайна», которое подчас можно встретить в трудах специалистов частного права, таких как С. Нестерова, М.Ю. Тихомиров[3], Н. Ткаченко[4], А. Егорова[5], рассматривающих его применительно к коммерческой тайне как праву субъектов предпринимательской деятельности (предприятий) на засекречивание финансовых, производственных, хозяйственных операций и документации по ним. Такой подход не лишен своей логики, так как в действительности применительно к частноправовым отношениям и случаям, когда определение объекта защиты, т.е. той или иной информации, зависит целиком от желаний и интересов частного лица, такое утверждение было бы вполне справедливым. С другой стороны, рассматривать это определение как основу для понимания термина «тайна» в целом не представляется возможным, ввиду того, что оно неприемлемо

---

[1] Об информации, информационных технологиях и о защите информации: федер. закон от 29.07.2006 № 149-ФЗ (ред. от 19.12.2016). – Ст. 9 ч. 2.
[2] Городов, О.А. Информационное право: учебник / О.А. Городов. – М.: ТК Велби, изд-во Проспект, 2008. – С. 67.
[3] Тихомиров, М.Ю. Юридическая энциклопедия / М.Ю. Тихомиров. – М., 1997. – С. 92.
[4] Нестерова, С. Институт коммерческой тайны в законодательстве России / С. Нестерова, Н. Ткаченко // Экономика и жизнь. – 1994. – №4. – С. 204.
[5] Егоров, А. Правовые основы институтов тайны / А. Егоров // Закон. – 1998. – № 2. – С. 75.

применительно к публично-правовым отношениям, как то государственной или служебной тайны.

В конечном итоге следует, по-видимому, согласиться с мнением А.А. Фатьянова[1] и И.В. Вельдера[2] и говорить о комплексности и многоаспектности понятия «тайна», что, очевидно, и объясняет множественность его трактовок в научно-правовой литературе, законодательстве и практике. Иными словами, определение термина «тайна» часто дается с разных позиций, подчеркивающих особенности его восприятия применительно к конкретным случаям или для характеристики общественных отношений по поводу той или иной информации.

В таких условиях для установления определенной системы координат, учитывая, что основным в системе отношений по поводу той или иной тайны является объект, т.е. собственно информация, автор предлагает использовать для характеристики различных аспектов тайны следующие термины: «тайна» (как указание на сам объект, т.е. информацию), «режим тайны» (как указание на режим конфиденциальности/защиты) и «право на тайну» (как конкретное правомочие лица устанавливать соответствующий режим в отношении той или иной информации). Предлагаемая система взаимосвязанных между собой терминов для характеристики «тайны» лучше отражает сложившуюся ситуацию в современном законодательстве и практике.

Принятие во внимание всего вышесказанного позволяет сформулировать по примеру И.В. Смольковой определенные признаки тайны:

- «тайна есть, прежде всего, сведения, информация;
- сведения должны быть известны или доверены узкому кругу лиц;
- сведения могут быть известны или доверены определенным субъектам в силу их профессиональной или служебной деятельности, осуществления определенных поручений;

---

[1] Фатьянов, А.А. Тайна как социальное и правовое явление. Ее виды / А.А. Фатьянов // Государство и право. – 1998. – № 6. – С. 19–28.

[2] Вельдер, И.А. Система правовой защиты персональных данных в Европейском союзе: автореф. дис. ... канд. юрид. наук / И.А. Вельдер. – Казань, 2006. – С. 11.

- сведения не подлежат разглашению (огласке);
- разглашение сведений (информации) может повлечь наступление негативных последствий (материальный и моральный ущерб ее собственнику, владельцу, пользователю или иному лицу);
- на лицах, которым доверена информация, не подлежащая оглашению, лежит правовая обязанность ее хранить;
- за разглашение этих сведений устанавливается законом юридическая ответственность»[1].

Именно указанные признаки чаще всего называются основными в большинстве определений «тайны» как таковой, а также и в отношении ее разновидностей, что допускает его принятие за основу.

Схожий перечень признаков можно встретить и у И.В. Бондаря[2], однако отметим при этом ряд вполне существенных и справедливых уточнений.

Во-первых, иногда термин «тайна» охватывает не только документированную информацию, т.е. ту, которая отражена в материальной форме, но и ту, что существует в идеальной форме (в сознании индивида в виде образов, а также передаваемая устно), что подходит для характеристики таких видов тайн, как тайна исповеди, личная и семейная тайна и т.п.

Во-вторых, следует особо выделить указание на действительную или потенциальную «ценность» информации, составляющей тайну. Данный признак «тайны» вполне справедливо упоминается целым рядом авторов, поскольку категория «ценность» достаточно точно отражает стоящие за этим охраняемые законом права и интересы субъектов. При этом, как справедливо отмечает И.В. Бондарь[3], «ценность» информации как тайны кроется или достигается в силу неизвестности ее третьим лицам, а фактически, по мнению автора, в возможности контроля за ее оборотом со стороны субъекта тайны, или, следуя современной терминологии в законодательстве, ее

---

[1] Смолькова, И.В. Проблемы охраняемой законом тайны в уголовном процессе / И.В. Смолькова. – М., 1999. – С. 23.
[2] Бондарь, И.В. Тайна по российскому законодательству (проблемы теории и практики): автореф. дис. ... канд. юрид. наук: 12.00.01 / И.В. Бондарь. – Нижний Новгород, 2004. – 27 с.
[3] Там же. С. 14.

обладателем, который по своему усмотрению имеет право ограничивать доступ к ней или предоставлять его, а также предопределять правила использования такой информации при ее передаче на условиях соблюдения конфиденциальности.

В итоге следует подчеркнуть основные объективные признаки «тайны», как это уже было сделано в других работах автора:

- «тайна – это информация в самых различных формах ее проявления, включая образы в сознании индивида, а также устные сведения;
- информация имеет действительную или потенциальную ценность для обладателя, который вправе на основании закона контролировать оборот и, в первую очередь, доступ к ней, и, как следствие, ограничивать его;
- разглашение, свободный доступ к информации приведет к негативным последствиям (материальный ущерб, моральный вред) для обладателя и в некоторых случаях для других лиц;
- обладатель информации принимает меры по защите информации, включая ограничение доступа или контроль над доступом к ней;
- за разглашение, несанкционированный доступ к информации, а также иногда за совершение иных действий (связанных с нарушением порядка использования, оборота) устанавливается юридическая ответственность»[1].

В качестве комментария к названным выше признакам требуется дать пояснение относительно использования в данном случае и в целом в работе термина «обладатель». В своей работе автор использует его в контексте Федерального закона «Об информации, информационных технологиях и о защите информации», а также части 4 Гражданского кодекса РФ, в отличие от работ других авторов, опубликованных до разработки и вступления в силу

[1] Бундин, М.В. Система информации ограниченного доступа и конфиденциальность // Вестник Нижегородского университета им. Н.И. Лобачевского. – Н. Новгород: Изд-во Нижегор. гос. ун-та. – 2015. – № 1. – С. 123.

данных актов, когда в научно-правовой литературе и законодательстве доминировал подход к информации (документированной информации) как объекту права собственности или близкий к нему по смыслу. Это представляет актуальность для оценки определений, результатов и выводов в большинстве научных работ, которые используют активно термины «собственник информации», «владелец информации» или аналогичные им. В таком контексте автор работы разделяет в целом идею о неприменимости к информации категории «право собственности» и скорее к необходимости использовать категорию «исключительных прав», которые могут быть у субъекта в отношении информации, ввиду особого характера или особых свойств последней. Поэтому в настоящей работе понятие «обладатель информации» трактуется в контексте статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» как «лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам».

Таким образом, с учетом обозначенных признаков предлагается использовать следующую трактовку понятия «тайна» – «*это информация в самых различных формах ее проявления (документированная, существующая в виде образов в сознании индивида, в устной форме), имеющая действительную или потенциальную ценность, доступ к которой ограничен на основании федерального законодательства ее обладателем, в связи с чем в отношении нее принимаются меры по ее защите, ограничению доступа, и разглашение, нарушение правил оборота которой влечет юридическую ответственность*»[1].

Другим аспектом, требующим отдельного изучения, является проблема соотношения понятий: «тайна», «информация с ограниченным доступом», «конфиденциальная информация» и «секрет», а также вопрос о

[1] Бундин, М.В. Система информации ограниченного доступа и конфиденциальность // Вестник Нижегородского университета им. Н.И. Лобачевского. – Н. Новгород: Изд-во Нижегор. гос. ун-та. – 2015. – № 1. – С. 124.

классификации и систематизации информации ограниченного доступа.

Существующая в настоящий момент некоторая путаница в этом вопросе обусловлена подчас «бессистемностью» российского законодательства в определении разновидностей информации с ограниченным доступом.

Началось это с появлением в статье 10 Федерального закона «Об информации, информатизации и о защите информации»[1] классификации документированной информации на открытую и ограниченного доступа. Последняя при этом подразделялась на информацию, составляющую государственную тайну, и конфиденциальную информацию. Таким образом, государственная тайна рассматривалась как особый, отдельный вид информации с ограниченным доступом, по отношению к которой применялся термин «секретность» и/или производные от него. Остальные разновидности информации ограниченного доступа рассматривались как конфиденциальная информация, которая определялась как «документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации»[2]. В реальности такая классификация активно использовалась не только по отношению к документированной информации, но и в отношении иных видов информации, доступ был ограничен в соответствии с законом. В подтверждение этого можно упомянуть «Перечень сведений конфиденциального характера», установленный Указом Президента РФ № 188 от 6 марта 1997 г.[3], который часто рассматривается как попытка определенной систематизации видов конфиденциальной информации, существующих на тот период. В конечном итоге система информации с ограниченным доступом в соответствии с требованиями Федерального закона

[1] Об информации, информатизации и защите информации: федер. закон от 20.02.1995 № 24-ФЗ. (Утратил силу.)
[2] Об информации, информатизации и защите информации: федер. закон от 20.02.1995 № 24-ФЗ. – Ст. 10. (Утратил силу.)
[3] Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» (ред. от 23.09.2005.).

«Об информации, информатизации и защите информации» 1995 года[1] и уже названном выше перечнем информации конфиденциального характера может быть представлена следующим образом (см. рис. 1).

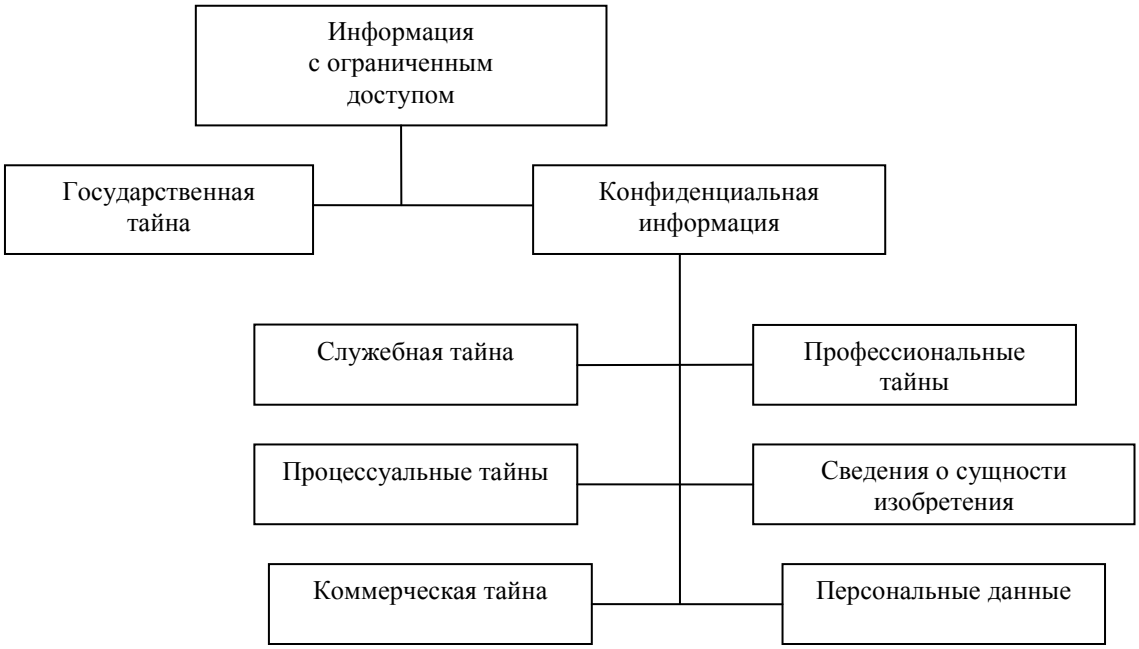

Рис. 1

С появлением в 2006 году Федерального закона «Об информации, информационных технологиях и о защите информации»[2] система информации ограниченного доступа существенно изменилась.

Во-первых, в новом законе была проведена классификация именно «информации» в зависимости от доступа к ней, а не «документированной информации».

Во-вторых, в нем появилось новое определение – «конфиденциальность информации», которая трактуется как «обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее

[1] Об информации, информатизации и защите информации: федер. закон от 20.02.1995 № 24-ФЗ. (Утратил силу.)
[2] Об информации, информационных технологиях и о защите информации: федер. закон от 29.07.2006 № 149-ФЗ (ред. от 19.12.2016).

обладателя»[1], как видим, здесь отсутствует какое бы то ни было упоминание о «конфиденциальной информации».

Таким образом, в основе Федерального закона «Об информации, информационных технологиях и о защите информации» лежит принципиально иная идея систематизации информации с ограниченным доступом[2]. Следовательно, можно говорить о принципиальном отказе законодателя от деления ее на государственную тайну и конфиденциальную информацию и, по-видимому, стоит вести речь о разновидностях ограничения доступа к информации, т.е. о разновидностях информации, доступ к которой ограничен в соответствии с федеральным законом.

В целом «конфиденциальность» согласно указанному выше закону можно рассматривать как признак информации с ограниченным доступом и как определенное указание на ее правовой режим. В то же время закон не приводит исчерпывающего перечня видов информации ограниченного доступа, а лишь называет типичные ее виды, в числе которых: государственная, коммерческая, профессиональная, служебная, личная, семейная и иная тайна. В соответствии с вышеизложенным, систему информации ограниченного доступа согласно требованиям Федерального закона «Об информации, информационных технологиях и о защите информации» можно схематично представить следующим образом (см. рис. 2).

[1] Об информации, информационных технологиях и о защите информации: федер. закон от 29.07.2006 № 149-ФЗ (ред. от 19.12.2016). – Ст. 2.
[2] Об информации, информационных технологиях и о защите информации: федер. закон от 29.07.2006 № 149-ФЗ (ред. от 19.12.2016).

Рис. 2.

Примечательно, что такая концепция систематизации информации ограниченного доступа нашла неоднозначную оценку в научной среде. Основная причина этого кроется в разной трактовке и значении, которые придаются терминам: «конфиденциальность», «секретность», «конфиденциальная информация».

Часть авторов рассматривает эти понятия как равнозначные и выделяет в качестве основного, или базового, термина «конфиденциальную информацию» для обозначения всех видов информации с ограниченным доступом[1]. Однако, как справедливо замечает Л.К. Терещенко, термин «конфиденциальная информация имеет свое определенное значение, вследствие чего не вся информация с ограниченным доступом может быть рассмотрена в качестве таковой»[2]. Само значение термина «конфиденциальный», т.е. дословно «доверительный», в отношении информации скорее применимо к случаям передачи ее обладателем другим лицам, т.е. «конфидентам», на которых одновременно возлагается обязанность обеспечить ее конфиденциальность или, иными словами,

[1] Ефремов, А. Понятие и виды конфиденциальной информации / А. Ефремов. – (http://www.russianlaw.net/law/confidential_data/a90/); Алексенцев, А.И. О составе защищаемой информации / А.И. Алексенцев // Безопасность информационных технологий. – 1999. – № 2. – С. 5–7.

[2] Терещенко, Л.К. Правовой режим информации / Л.К. Терещенко. – М., 2008. – С. 72.

«сохранить ее в тайне». Последнее обусловлено наличием у обладателя охраняемого законом права или интереса, которые могут оказаться под угрозой в результате передачи или распространения информации без его согласия третьим лицам. Фактически «конфиденциальность» – это требование, обращенное исключительно к доверенному лицу – конфиденту, получившему доступ к информации на законном основании, т.е. в силу прямого указания в законе о необходимости передачи ему тех или иных сведений или же по желанию обладателя. При этом последний вправе часто распоряжаться и контролировать оборот этой информации (тайны) и во многих случаях, по своему желанию, может снять ограничения в доступе, сделав ее общедоступной.

Разберем несколько таких примеров подробнее. Некоторые существующие разновидности тайн фактически нельзя рассматривать как «конфиденциальную информацию», к примеру – личная, семейная тайна, тайна частной жизни и иные, так называемые «частноохраняемые» тайны. В этом случае обладатель или субъект тайны самостоятельно берет на себя обязательства по ее охране – т.е. просто не передает или не сообщает ее иным лицам, а следовательно, конфиденты попросту отсутствуют. В случае передачи этих сведений иным лицам – они становятся конфидентами. Отметим, что при этом, как правило, изменяется сам режим тайны или информации. В частности, при передаче информации в государственные органы она охраняется уже как служебная тайна или ее разновидности (тайна записи актов гражданского состояния, налоговая тайна и др.). Если ее передать в коммерческую или некоммерческую организацию – в качестве персональных данных, тайны исповеди, банковской тайны и т.д. Иными словами, конфиденциальной информация станет только в случае передачи или сообщения ее конфиденту, который на основании закона вынужден обеспечивать ее конфиденциальность в интересах обладателя.

Из вышесказанного следует, что требование о «конфиденциальности», предусмотренное законом, относится исключительно к конфиденту, тогда как

обладатель обеспечивает защиту информации (ограничивает доступ к ней), чаще всего, добровольно, действуя в своем интересе, так же, как и соглашается на ее общедоступность.

Следует отметить, что термин «конфиденциальность» используется также по отношению к трудовым отношениям для обозначения требования со стороны работодателя к работнику. Если обладателем информации (тайны) является юридическое лицо или индивидуальный предприниматель, то конфидентами будут его работники или служащие, которые принимают на себя добровольно обязательства по обеспечению конфиденциальности полученной ими информации в целях реализации своих должностных обязанностей.

Аналогичным образом обстоят дела с использованием термина «секретность» по отношению к государственной тайне. Обладателем тайны в таком случае будет государство в лице его органов, а своего рода конфидентами – государственные служащие и юридические лица, которые берут на себя соответствующие обязательства и обладают специальным правом, или «допуском к государственной тайне». Более того, государство и его органы как обладатели вправе самостоятельно принимать и использовать меры по защите государственной тайны, определять параметры ее правового режима, а также ее «рассекречивать».

В связи с этим предложенная действующим Федеральным законом «Об информации, информационных технологиях и о защите информации»[1] концепция систематизации информации ограниченного доступа по целому ряду причин может быть названа удачной лишь отчасти.

Среди основных причин стоит назвать не только уже отмеченное разнообразие видов «тайн», но и логически мало чем оправданную подмену термина «конфиденциальная информация» на «конфиденциальность», что скорее внесло еще большую путаницу в этом вопросе. В настоящий момент в

[1] Об информации, информационных технологиях и о защите информации: федер. закон от 29.07.2006 № 149-ФЗ (ред. от 19.12.2016).

нормативно-правовых актах эти термины используются одновременно. При этом в большинстве случаев простая замена этих терминов в принципе невозможна и требует логического перестроения текста нормативно-правового акта.

С учетом сложившейся ситуации в научной литературе были предложены другие альтернативные классификации информации ограниченного доступа. Е.К. Волчинская[1], в частности, предлагает классифицировать тайны на первичные (естественные) и производные. К первой группе она относит «тайны, непосредственно связанные с жизнедеятельностью субъекта, как то: личная тайна – физическое лицо, коммерческая тайна – юридическое лицо (субъект предпринимательской деятельности), государственная и служебная тайна – орган государственной власти»[2]. Ко второй группе она относит преимущественно профессиональные тайны (врачебная тайна, тайна исповеди, тайна банковских вкладов, налоговая, нотариальная и др.).

Наиболее существенным различием между первичными и производными тайнами, по мнению Е.К. Волчинской, являются права субъекта по установлению и изменению режима ограничения доступа к информации, которые присутствуют у него в случае с первичными тайнами, и фактически только обязанность по соблюдению ее конфиденциальности в случае с производными тайнами.

Объективно данная классификация не лишена смысла и по своей сути является отражением идеи отграничения конфиденциальной информации от иных видов информации ограниченного доступа. Согласно этой классификации следует отнести конфиденциальную информацию к числу «производных тайн», т.е. тех случаев, когда информация доверяется субъектом тайны (т.е. обладателем) другому лицу (конфиденту) при обязательном условии сохранения ее конфиденциальности.

---

[1] Волчинская, Е.К. Коммерческая тайна в системе конфиденциальной информации / Е.К. Волчинская // Информационное право. – М.: Юрист, 2005. – № 3. – С. 17–21.

[2] Там же.

При этом, по мнению Е.К. Волчинской[1], часть тайн, как например служебная тайна, могут объединять в себе одновременно информацию, доверенную органам государственной власти иными лицами на условиях соблюдения ее конфиденциальности, и информацию, полученную государственным органом в процессе своей деятельности, распространение которой может привести к негативным последствиям. Очевидно, что в первом случае ее следует отнести к числу «производных тайн», а во втором – к числу «первичных».

Указанная выше классификация является далеко не единственной и последней в своем роде, что еще больше приводит к мысли о необходимости соотнесения существующих режимов информации ограниченного доступа между собой. При этом требуется также разработка правил своего рода «трансформации» режима информации, общедоступность которой привела бы к нарушению прав и законных интересов определенного круга субъектов, из одного режима ограничения доступа (тайны) в другой аналогичный режим.

Этому можно привести множество примеров, хотя бы уже упомянутый институт служебной тайны, правовой режим которой используется не только для защиты информации, создаваемой органами государственной и муниципальной власти в процессе осуществления своей деятельности, но и для охраны интересов граждан и юридических лиц, которые доверили или передали им сведения на условиях конфиденциальности.

К практически похожим случаям следует отнести институт персональных данных. В целом персональные данные нельзя полностью рассматривать как информацию ограниченного доступа, поскольку закон допускает возможность их существования в режиме общедоступной информации[2]. Таким образом, они могут быть как общедоступной, так и конфиденциальной информацией.

---

[1] Волчинская, Е.К. Коммерческая тайна в системе конфиденциальной информации / Е.К. Волчинская // Информационное право. – М.: Юрист, 2005. – № 3. – С. 17–21.

[2] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017). – Ст. 3.

С другой стороны, анализ существующих законодательных положений, что ранее отмечалось автором[1], позволяет говорить о своего рода «презумпции конфиденциальности» персональных данных, до тех пор, пока оператором не получено однозначного согласия субъекта данных на их общедоступность, или если это специально не установлено федеральным законом.

В конечном итоге появление самой этой категории в российском праве и законодательстве по-прежнему создает массу проблем, которые объясняются частично непониманием того, как режим персональных данных как информации ограниченного доступа соотносится с другими режимами информации. К примеру, часть давно известных институтов тайн в российском законодательстве предполагает охрану информации, полученной от физических лиц, т.е. фактически персональных данных. В отдельных случаях это может быть лишь частью содержания этих тайн (банковская тайна, служебная тайна, налоговая тайна и др.), в других случаях, наоборот, может сложиться впечатление, что они изначально были созданы для защиты персональных данных и обеспечения их конфиденциальности при передаче их государственным органам и органам местного самоуправления или иным субъектам (тайна записи актов гражданского состояния, тайна усыновления, врачебная тайна и др.). В связи с этим возникают вполне справедливые вопросы о соотнесении указанных режимов между собой и очевидные затруднения на практике, связанные с необходимостью выполнения требований законодательства о персональных данных. Отметим, что в ходе Парламентских слушаний[2], посвященных проблемам вступления в силу и реализации Федерального закона «О персональных данных», аналогичный вопрос задавался неоднократно.

---

[1] Бундин, М.В. Система информации ограниченного доступа и конфиденциальность // Вестник Нижегородского университета им. Н.И. Лобачевского / М.В. Бундин. – Н. Новгород: Изд-во Нижегор. гос. ун-та. – 2015. – № 1. – С. 127.

[2] Рекомендации Парламентских слушаний на тему: «Актуальные вопросы развития и применения законодательства о защите прав граждан при обработке персональных данных» (состоялись 20 октября 2009 г.). – (http://komitet2-16.test.km.duma.gov.ru/Novosti_Komiteta/item/24813/). – Дата обращения: 02.04.2017.

Следует признать, что пока действующее законодательство не способно дать на эти вопросы однозначных ответов. Обилие всевозможных «тайн» скорее отрицательно сказывается на защите прав и законных интересов обладателей информации, а также на реализации права на информацию иных лиц. Как это справедливо отмечает Л.К. Терещенко, «в настоящий момент обстоятельное и практичное решение этого вопроса может быть в принятии однозначных законодательных положений, которые давали бы четкий ответ на вопрос об иерархии существующих видов тайн и их режимов, а также о правилах их трансформации»[1].

[1] Терещенко, Л.К. Правовой режим информации: автореф. дис. … д-ра юрид. наук. / Л.К. Терещенко. – М., 2011. – С. 48.

2.2. Правовой режим персональных данных как информации ограниченного доступа

Перед тем как приступить к анализу правового режима персональных данных как информации ограниченного доступа, следует отметить, что сам термин «правовой режим» имеет в теории различное значение, что требует и от автора определенных пояснений на этот счет.

В целом как категория правовой режим достаточно часто используется как в научно-правовой литературе, так и в законодательстве. Категорию режима можно встретить более чем в трехстах законодательных актах федерального уровня.

Категория режима активно используется в земельном законодательстве, в частности в ст. 1 Земельного кодекса[1] неоднократно используется термин «правовой режим земель», который определяется принадлежностью ее к определенной категории по целевому назначению. Налоговый кодекс[2] также в ст. 12, п. 7 использует в некоторых случаях термин «правовой режим» в контексте установления «специальных налоговых режимов». В Трудовом кодексе[3] можно найти массу отсылок к тем или иным правовым режимам: режим труда и отдыха (ст. 46), режим рабочего времени и времени отдыха (ст. 57), режим неполного рабочего дня (смены) и (или) неполной рабочей недели (ст. 74), особый режим работы – ненормированный рабочий день (ст. 101), и др. Правовой режим как категория активно используется Семейным кодексом[4] для характеристики имущественных отношений супругов, устанавливая законный режим имущества супругов (глава 7) как режим их совместной собственности и договорный режим (глава 8). Закон о правовом положении иностранных граждан также использует термин правовой режим в части определения режима пребывания (проживания)

---

[1] Земельный кодекс Российской Федерации от 25.10.2001 № 136-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.01.2017).
[2] Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ (ред. от 28.12.2016).
[3] Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.01.2017).
[4] Семейный кодекс Российской Федерации от 29.12.1995 № 223-ФЗ (ред. от 28.03.2017).

иностранных граждан на территории РФ (ст. 7).

Конституционный суд тоже достаточно часто в своих решениях оперирует понятием правового режима, в качестве примера можно привести Определение Конституционного суда РФ от 21.12.2004 № 441-О «Об отказе в принятии к рассмотрению жалобы гражданки Ивановой Н.А. на нарушение ее конституционных прав положениями статьи 4 Закона Российской Федерации «О приватизации жилищного фонда в Российской Федерации», где суд ссылается на то, что порядок предоставления служебной жилой площади и пользование ею определяется специальным режимом – «режимом служебной жилой площади».

Как видно из примеров, категория правового режима используется как универсальная для описания многочисленных правовых явлений, причем, что примечательно, с помощью ее описывается не только обычная жизнедеятельность или нормальное состояние объекта права, но и вводятся исключения из общих правил в виде его специальных или особых режимов. Исключительность правового режима может быть изначально указана в законе, как, например, в законах о чрезвычайном[1] и военном положении[2], или она может подразумеваться самим смыслом закона, как то – Закон РФ «О закрытом административно-территориальном образовании»[3].

В достаточно большом числе случаев описывается основной – общий правовой режим, или режим обычного состояния, а исключения или отступления от него будут рассматриваться как особые или специальные режимы. В качестве примера этому можно назвать уже упомянутый Семейный кодекс, устанавливающий законный режим имущества супругов в качестве основного, тогда как иные режимы, в частности договорный, следует рассматривать в качестве специального.

Широкое применение и универсальность термина «правовой режим»

---

[1] О чрезвычайном положении: федер. конституционный закон от 30.05.2001 № 3-ФКЗ (ред. от 03.07.2016).
[2] О военном положении: федер. конституционный закон от 30.01.2002 № 1-ФКЗ (ред. от 12.03.2014).
[3] О закрытом административно-территориальном образовании: закон РФ от 14.07.1992 № 3297-1 (ред. от 03.07.2016).

для описания тех или иных правовых явлений никоим образом не способствует его однозначному пониманию в юридической науке.

Отчасти это может быть результатом многозначности самого термина «режим», имеющего в русском языке несколько значений. Толковый словарь дает ему такое определение:

- государственный строй (обычно об антинародном, антидемократическом строе);
- распорядок дел, действий;
- условия деятельности, работы, существования чего-нибудь[1].

В юридической литературе, что отмечается многими авторами, сложилось также неоднозначное понимание термина «режим», «правовой режим», «социальный режим». В основном эти понятия активно изучаются в сфере теории права. В общем и целом, можно, пожалуй, выделить два основных подхода к пониманию термина «правовой режим» в научно-правовой литературе.

Первый подход, предложенный известными учеными в области теории права Н.И. Матузовым и А.В. Малько, состоит в рассмотрении правового режима как «особого порядка правового регулирования, выражающегося в определенном сочетании юридических средств и создающего желаемое социальное состояние и конкретную степень благоприятности или неблагоприятности для удовлетворения интересов субъектов. Таким образом, это система условий и методов осуществления правового регулирования, своего рода – «функциональная характеристика права»»[2].

Аналогичные по своему содержанию идеи также можно встретить и у С.С. Алексеева, рассматривающего правовой режим «как порядок регулирования, который выражен в комплексе правовых средств, характеризующих особое сочетание взаимодействующих между собой

---

[1] Ожегов, С.И. Словарь русского языка / С.И. Ожегов. – (http://slovar.plib.ru/dictionary/d19/). – Дата обращения: 02.04.2017.

[2] Матузов, Н.И. Правовые режимы: Вопросы теории и практики / Н.И. Матузов, А.В. Малько // Правоведение. – 1996. – № 1. – С. 16–29.

дозволений, запретов, а также позитивных связываний и создающих особую направленность регулирования»[1]. Следовательно, правовой режим это глубокое, содержательное правовое явление, связывающее воедино целостный комплекс правовых средств в соответствии со способами правового регулирования и его типами. С точки зрения этого подхода можно вести речь об отраслевых, межотраслевых правовых режимах.

Второй подход доминирует в административно-правовой науке и относится, в первую очередь, к характеристике «административно-правовых режимов», определяя их как «комплекс общественных отношений определенного вида деятельности, закрепленный юридическими нормами и обеспеченный совокупностью юридико-организационных средств»[2] (Д.Н. Бахрах). Выделение правового режима обусловлено: во-первых, особой специальной значимостью общественных отношений, их специфическими целями и задачами; во-вторых, использованием особых принципов, форм и методов деятельности, отражающихся в системе прав и обязанностей субъектов.

Ю.А. Тихомировым правовой режим был определен как «особый вид регулирования, в рамках которого создается и используется особая комбинация юридических, организационных и иных средств для обеспечения того или иного государственного состояния»[3].

Стоит обратить внимание, что современное законодательство и практика, как уже было показано, идет по пути применения режимов не только к сфере государственного управления или описания государственного состояния, но скорее рассматривая правовые режимы как нечто универсальное.

В сущности, следует говорить о формировании особого режимного

---

[1] Алексеев, С.С. Общие дозволения и общие запреты в советском праве / С.С. Алексеев. – М.: Юридическая литература, 1989. – С. 185.

[2] Бахрах, Д.Н. Административное право России: Учебник для вузов / Д.Н. Бахрах. – М.: Изд-во НОРМА (ИГ НОРМА-ИНФРА • М), 2002. – С. 201.

[3] Тихомиров, Ю.А. Административное право и процесс. Полный курс. – 2-е изд. / Ю.А. Тихомиров. – М., 2005. – С. 377.

подхода в изучении права и правовых явлений. Д.Н. Бахрах прямо указывает на возможность такого подхода в изучении права как примера систематизации норм, регулирующих отношения между людьми, по поводу того или иного объекта[1].

Следует согласиться с мнением В.П. Рушайло[2] и В.Б. Исакова[3], рассматривающих правовой режим как некую специфическую правовую форму воздействия на общественные отношения. Особенно это справедливо в ситуациях, требующих специфического и особого подхода к регулированию тех сфер, регулирование которых может оказаться неэффективным в общем порядке.

Еще одной особенностью правовых режимов зачастую является их комплексный характер, что подчеркивается многими авторами. Д.Н. Бахрах отмечает, что в конструировании таких режимов принимают участие нормы нескольких отраслей права (административного, конституционного и т.д.), и они затрагивают различные по характеру права и обязанности субъектов режимного регулирования[4].

Комплексный характер правовых режимов часто позволяет объединить и адаптировать правовые средства и методы воздействия к конкретным общественным отношениям. Л.К. Терещенко подчеркивает, что это «позволяет сформировать адекватный юридический инструментарий для регулирования определенной группы отношений»[5]. Исходя из этого, ею были предложены следующие характеристики правового режима информации, включая информацию ограниченного доступа:

- системность используемых средств;
- наличие специфических приемов правового регулирования;
- систематизация норм по признаку объекта;

---

[1] Бахрах, Д.Н. Административное право России / Бахрах Д.Н. – М., 2002. – С. 410.
[2] Рушайло, В.Б. Специальные административно-правовые режимы в сфере обеспечения общественной безопасности / В.Б. Рушайло. – М., 2003. – С. 34.
[3] Исаков, В.Б. Проблемы теории юридических фактов: дис. ... д-ра юрид. наук: 12.00.01 / В.Б. Исаков. – Свердловск, 1985. – С. 392.
[4] Бахрах, Д.Н. Административное право России / Д.Н. Бахрах. – М., 2002. – С. 415.
[5] Терещенко, Л.К. Правовой режим информации / Л.К. Терещенко. – М.: Юриспруденция, 2007. – С. 58.

- создание условий для достижения заданного состояния объекта;
- комплексность режима как отражение комплексности объекта;
- обусловленность режима специфичностью групп общественных отношений, а также необходимостью использования особого подхода к регулированию там, где использование общего подхода неэффективно или нецелесообразно[1].

Наличие всех этих характеристик можно проследить и в отношении правового режима персональных данных, который следует рассматривать как разновидность особого правого режима информации – режима информации ограниченного доступа.

Непосредственно рассмотрение правового режима персональных данных как информации ограниченного доступа следует начать с определения его четких границ, прежде всего в рамках общего правового режима информации ограниченного доступа. Как неоднократно упоминалось в работе, персональные данные сами по себе не являются информацией ограниченного доступа, и их конфиденциальность презюмируется. Как следствие, правовой режим персональных данных в целом имеет сложную структуру, обусловленную спецификой самого объекта регулирования. Предположительно можно выделит две основных составляющих этого режима:

- правовой режим «общедоступных персональных данных», который лежит в сфере общего правового режима информации, т.е. режима общедоступной информации;
- правовой режим персональных данных ограниченного доступа, который лежит в сфере специальных правовых режимов информации, т.е. в сфере правового режима информации с ограниченным доступом.

При этом последний также может быть разделен на несколько

[1] Терещенко, Л.К. Правовой режим информации / Л.К. Терещенко. – М., 2007. – С. 58.

составляющих[1]:

1) персональные данные, охраняемые в режиме государственной тайны;

2) персональные данные ограниченного доступа, обрабатываемые в режиме архивной информации;

3) персональные данные, охраняемые в режиме личной, семейной тайны, тайны частной жизни (т.е. без передачи сведений третьим лицам и, следовательно, не являющиеся конфиденциальной информацией);

4) конфиденциальные персональные данные, в отношении которых специальным законом (Федеральный закон «О персональных данных»[2]) устанавливается требование о соблюдении их конфиденциальности.

Несмотря на такую сложную структуру, можно говорить, что определенный интерес для настоящего исследования представляет исключительно последняя категория, которая может быть охарактеризована как персональные данные, охраняемые в условиях правового режима конфиденциальности персональных данных как информации ограниченного доступа в рамках закона о персональных данных. Правовой режим остальных категорий, хоть они и являются разновидностями информации ограниченного доступа, не ориентирован специально на защиту персональных данных как ограниченной в доступе информации и не выделяет их в общем массиве охраняемой на условиях этого режима информации. Исключением можно, пожалуй, назвать персональные данные, составляющие личную, семейную тайну и тайну частной жизни, которые сами по себе не могут быть не привязаны к конкретному индивиду. Однако в этом случае законодательное регулирование строится исключительно на признании у индивида права на эти виды тайн и возможности их самостоятельной охраны и как следствие

[1] Об информации, информационных технологиях и о защите информации: федер. закон от 29.07.2006 № 149-ФЗ (ред. от 19.12.2016). – Ст. 1.
[2] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017).

минимального объема нормативных положений, что обеспечивает большую личную свободу и соответствует идее естественных прав, но в то же время делает изучение их правового режима менее актуальным в целях настоящего исследования, суть которого автору видится, во многом, в определении прав индивида в случае передачи информации о себе третьим лицам. Именно «доверительная передача» информации индивидом другому лицу, т.е. оператору или обработчику, обуславливает ее защиту в рамках специального правового режима конфиденциальных персональных данных.

В дополнение к сказанному можно отметить – правовой режим конфиденциальности персональных данных включает в себя две основные составляющие: общий правовой режим конфиденциальности персональных данных и *правовой режим «особо чувствительных» персональных данных* (особых категорий персональных данных на основании ст. 10 Закона о персональных данных) и *правовой режим биометрических персональных данных*.

В целом общую структуру правого режима персональных данных можно представить следующим образом (см. рис.3):

Рис. 3

Что касается основных элементов и структуры правового режима информации, и персональных данных в частности, то здесь также можно

отметить некоторые расхождения во мнениях. А.А. Антопольский рассматривает исключительно правовой режим «информационного объекта», давая ему следующее определение: «совокупность правовых норм, касающихся определенного объекта урегулированных правом общественных отношений, включая его нормативное определение и обязательные правовые предписания о порядке или правилах использования данного объекта, а также об ответственности за их несоблюдение[1]». В этой связи правовой режим информационного объекта должен, по мнению того же автора, складываться из норм, регулирующих три основных составляющих: «(1) порядок создания объекта, (2) порядок его передачи и получения (включая установление режима свободного либо ограниченного доступа), (3) вопросы защиты прав субъекта в отношении данного объекта»[2]. В дополнение к этому правовой режим может включать в себя и иные (необязательные элементы), как то: нормы, регулирующие гражданско-правовой оборот объекта и другие вопросы.

Суждение о необходимости использования термина «информационный объект» вместо «информации» не разделяется автором работы и в целом не относится напрямую к рассматриваемому случаю, более того, высказанные А.А. Антопольским предположения о трех основных составляющих правового режима информации также видятся не совсем корректными.

Во-первых, в действительности правовой режим той или иной разновидности информации изначально имеет свой объект. Такой режим может быть установлен законом в отношении конкретного вида информации, как, например, в случае с персональными данными[3] законодательно устанавливается соответствующий режим, предполагая, что такая разновидность информации существует. Действие правового режима может быть распространено на ту или иную информацию, как, например, в случае с

---

[1] Антопольский, А.А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: автореф. дис. … канд. юрид. наук / А.А. Антопольский. – М., 2004. – С. 8.
[2] Там же.
[3] Там же.

коммерческой тайной[1], когда ее обладатель вправе выполнить предписанные законом действия и распространить на нее режим коммерческой тайны.

Во-вторых, «порядок получения и передачи информации (включая установление режима свободного либо ограниченного доступа)» звучит достаточно странно, учитывая, что термин «доступ» в действительности подразумевает оба эти действия, поскольку невозможен без двух взаимно корреспондирующих составляющих: права на получение информации и обязанности по ее предоставлению.

В-третьих, указание на защиту только «прав субъектов в отношении объекта» можно рассматривать как некоторое сужение реального содержания правового режима. В действительности объектом защиты, вероятнее всего, следует рассматривать сам режим. К примеру, в результате нарушения режима – порядка работы со сведениями, составляющим государственную тайну – не обязательно может произойти их «утечка», т.е. быть причинен ущерб суверенитету и безопасности государства и, как следствие, нарушению прав обладателя, в то же время – это будет рассматриваться как нарушение требований соответствующего режима и предполагать ответственность виновного лица.

Учитывая сказанное, более оптимальным следует признать выделение основных структурных элементов правового режима, предложенное Л.К. Терещенко, которая указывает на следующие элементы, присущие всем правовым режимам информации:

– «целевое назначение режима;

– объект правового регулирования;

– правовое положение субъектов правового режима;

– комплекс способов правового регулирования и средств юридического воздействия»[2].

Целью правового режима конфиденциальности персональных

---

[1] Антопольский, А.А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: автореф. дис. … канд. юрид. наук / А.А. Антопольский. – М., 2004. – С. 8–9.

[2] Терещенко, Л.К. Правовой режим информации / Л.К. Терещенко. – М.: Юриспруденция, 2007. – С. 61.

данных в таком случае следует считать установление прав и обязанностей субъектов отношений, возникающих по поводу персональных данных, как разновидности информации, их защите и обеспечении информационной безопасности с учетом сохранения баланса интересов личности, общества и государства. Именно достижение такого состояния в конечном итоге стоит рассматривать как конечную цель установления режима персональных данных.

В этой связи было бы не совсем правильным рассматривать в качестве единственной цели правового режима персональных данных «обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну», как это указывается в Законе о персональных данных[1]. С таким утверждением отчасти можно согласиться, однако говорить о том, что этим исчерпывается целевое назначение правового режима, представляется не совсем точным. Установление определенных ограничений на использование и обработку персональных данных в действительности является результатом стремления, с одной стороны, к обеспечению защищенности прав и свобод личности путем ограничения нежелательных действий с информацией персонального характера, с другой стороны, к обеспечению интересов государства и общества при обработке информации об индивидах, устанавливая для последних определенный круг прав и обязанностей, а также гарантируя им возможность, при определенных законом условиях, иметь доступ к персональным данным, обрабатывать их, действуя в своем собственном интересе.

Именно это закреплено в Доктрине информационной безопасности[2], которая подчеркивает «необходимость соблюдения баланса между потребностью граждан в свободном обмене информацией и ограничениями,

---

[1] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017). – Ст. 2.

[2] Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646). – (https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html). – Дата обращения 02.04.2016.

связанными с необходимостью обеспечения национальной безопасности, в том числе информационной». Безусловно, для личности право на информацию и право на доступ к информации являются важнейшими из конституционных прав человека и гражданина, которые связаны не только со свободным обменом информацией, но и необходимостью обеспечения защиты информации, обеспечивающей личную безопасность.

Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных в своей преамбуле ясно указывает на необходимость сохранения баланса интересов личности в части защиты его фундаментальных прав и свобод, в частности права на уважение частной жизни, в то же время признавая необходимость согласования ее с идеей свободы информации и информационного обмена между народами. Эта идея также просматривается в Преамбуле и ст. 1 Директивы № 95/46/ЕС, в которых указывается на необходимость уважения фундаментальных прав и свобод личности при обработке персональной информации при гарантиях сохранения свободного обращения информации.

Трактовка положений ст. 55 российской Конституции также вполне очевидно подразумевает необходимость учета интересов всех субъектов, подчеркивая, что ограничения прав и свобод возможно только в той мере, которая необходима для защиты прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства, и только на основании закона. Ограничение обработки персональных данных в этой связи может рассматриваться краеугольным камнем защиты прав и свобод личности в информационной сфере, что, впрочем, не исключает возможность таковой полностью – при соблюдении правил и условий, установленных законом.

Как мы видим, появление правового режима персональных данных объясняется необходимостью обеспечения личной информационной безопасности индивида, т.е. создание условий, исключающих посягательство на права и законные интересы личности с использованием персональной

информации, что стоит рассматривать в качестве основной – конечной цели установления правового режима персональных данных, при обязательном условии сохранения баланса интересов общества и государства, интересы которых могут быть связаны с необходимостью данных об индивидах.

Объектом правового режима конфиденциальности персональных данных как информации ограниченного доступа следует рассматривать отношения, возникающие в связи с обработкой персональных данных, т.е. информации, переданной индивидом другим субъектам права – «конфидентам» на условиях соблюдения ее конфиденциальности, что и позволяет рассматривать их как информацию ограниченного доступа или конфиденциальную информацию.

В этой связи можно лишь напомнить о том, что автор не ставит целью рассмотрения правового режима персональных данных в целом, как сравнительно сложной разновидности информации, которая может быть как общедоступной, так и ограниченного доступа.

Резюмируя сказанное, а также в целом содержание первой главы настоящей работы, в которой уже было дано исчерпывающее понятие персональных данных как разновидности информации, объектом специального правового режима персональных данных как информации ограниченного доступа следует рассматривать отношения, возникающие в связи с обработкой *«конфиденциальных персональных данных»* – т.е. *персональных данных, в отношении которых на основании положений закона о персональных данных установлено требование о соблюдении их конфиденциальности и, как следствие, распространяется правовой режим их конфиденциальности.*

Правовое положение субъектов правового режима конфиденциальности персональных данных. Круг субъектов специального правого режима персональных данных крайне широк и его субъектами могут быть физические и юридические лица, государственные органы, органы местного самоуправления и т.д. Однако специфика правового режима

персональных данных ориентирована на разделение всего круга потенциальных субъектов на несколько основных групп, к которым их следует отнести на основании анализа положений закона о персональных данных:

- *Субъект персональных данных* – всегда физическое лицо, информация о котором содержится в информационной системе персональных данных.
- *Оператор* – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.
- *Уполномоченный орган по защите прав субъектов персональных данных*.

Учитывая характер настоящего исследования и его цели, т.е. рассмотрение отношений, складывающихся по поводу конфиденциальных персональных данных, в этот перечень можно внести некоторые коррективы.

Как и в случаях с другими разновидностями конфиденциальной информации основными участниками таких отношений следует признать: – *обладателя информации (тайны)* и *конфидента*, которому она доверяется, т.е. которому предоставляется доступ к информации. Применительно к отношениям по поводу персональных данных, очевидно, этими лицами будут субъект персональных данных – обладатель и оператор – конфидент. Именно этот факт обуславливает достаточно типичную систему отношений между ними, которую можно описать схемой «обладатель – конфидент».

Основным отличием таких отношений является, как правило, возможность обладателя определять правила и порядок доступа к информации, фактически определять режим информации – ограничить доступ к ней или сделать общедоступной; он также вправе требовать соблюдения ее конфиденциальности в случае передачи ее конфиденту – оператору. В результате отличием правового положения субъекта

персональных данных как участника рассматриваемых отношений следует считать наличие у него, как у обладателя, безусловного права на определение режима своих персональных данных, т.е.:

- сохранить их в тайне (в режиме личной, семейной тайны, тайны частной жизни и т.д.), если иное не предусмотрено законом;
- передать их оператору на условиях сохранения их конфиденциальности (для оператора эти сведения могут находиться в условиях режима иной тайны: служебной тайны, банковской тайны, налоговой тайны и т.д.). Отметим, что необходимость сохранения конфиденциальности данных презюмируется на основании закона;
- сделать эти сведения общедоступными, т.е. распространить на них режим общедоступной информации.

Напротив, правовое положение оператора как конфидента будет обусловлено обязанностью по сохранению конфиденциальности персональных данных, которая является необходимым условием их обработки и не может быть отменена им по собственному усмотрению.

Наличие в системе отношений по обработке персональных данных органа по защите прав субъектов персональных данных обусловлено спецификой самих отношений, учитывая, что одной из сторон отношений по обработке персональных данных является индивид, который зачастую не обладает существенными возможностями по контролю за оборотом информации о себе и соблюдению в целом режима персональных данных операторами, которых может насчитываться многие десятки, если не сотни и даже тысячи. В этом отношении орган по защите прав субъектов персональных данных выступает органом административного контроля (надзора) за соблюдением законодательства о персональных данных операторами и обеспечивает защиту прав субъектов персональных данных, что обуславливает специфику его правого статута.

В то же время в отношениях по обработке персональных данных и

обеспечения их конфиденциальности присутствуют и другие субъекты, часть из которых лишь частично упоминается в законе о персональных данных:

– *работник*, состоящий в трудовых отношениях с оператором и имеющий доступ к персональным данным в рамках исполнения своих должностных обязанностей[1];

– *лицо, ответственное за организацию обработки персональных данных* в организациях[2];

– *лицо, осуществляющее непосредственно обработку персональных данных по поручению оператора (обработчик персональных данных)* в рамках гражданско-правового договора, государственного или муниципального контракта[3].

Очевидно, что все перечисленные выше субъекты имеют прямую связь с оператором и действуют от его имени или в его интересе и как следствие их правовой статус характеризуется в первую очередь обязанностью по соблюдению конфиденциальности персональных данных, к которым они имеют доступ в силу трудовых или гражданско-правовых отношений с оператором. Последний факт часто объясняет установление ответственности оператора за их действия перед субъектом, и наоборот[4]. Отметим, что указанные субъекты были введены в законодательство не так давно, начиная с середины 2011 года[5], и их появление стало результатом вполне справедливой критики в адрес законодателя. Упоминание об «обработчике» персональных данных как субъекте отношений в сфере персональных данных можно встретить у Ю.В. Травкина[6].

В целом круг субъектов специального правового режима персональных данных можно представить следующим образом (см. рис.4):

---

[1] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017). – Ст. 18.1, п. 1 (а, б); 6.
[2] Там же. – Ст. 22.1.
[3] Там же. – Ст. 6, п. 3.
[4] Там же. – Ст. 6, п. 4 и 5.
[5] О внесении изменений в Федеральный закон «О персональных данных»: федер. закон от 25.07.2011 № 261-ФЗ // Собрание законодательства Российской Федерации. – 2011. – № 31. – Ст. 4701.
[6] Травкин, Ю.В. Персональные данные. / Ю.В. Травкин. – М.: Амалданик, 2007.

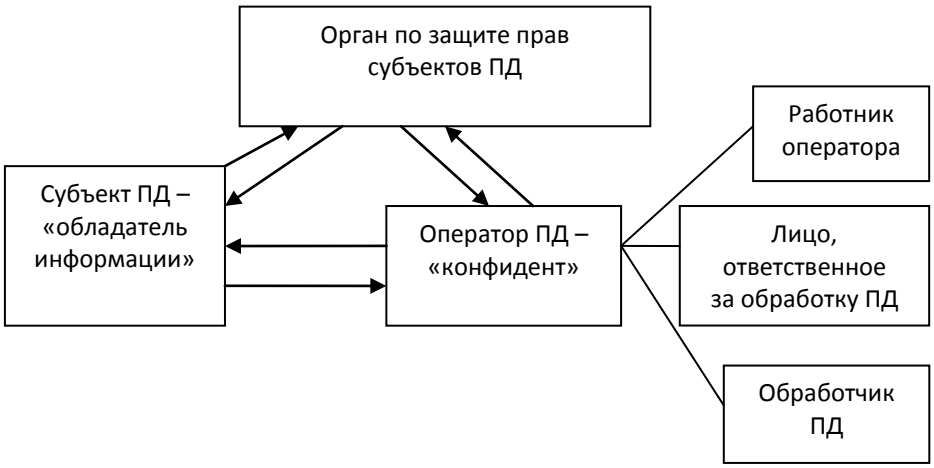

Рис. 4.

Отметим, что поскольку персональные данные достаточно универсальная категория и могут быть объектом как публично-правовых отношений (формирование государственных автоматизированных систем и другие случаи), так и частноправовых отношений (отношения по продвижению товаров и услуг на рынке), то соответственно положение субъектов может быть как равным, так и неравным. В действительности предоставление персональных данных зачастую является необходимым условием получения государственных, муниципальных и иных услуг, вступления в договорные отношения, а также неисчислимого количества иных случаев. В то же время, даже в случае отношений частного характера, сохраняется безусловное требование, обращенное к оператору по соблюдению конфиденциальности данных, а также иные обязанности перед субъектом персональных данных и уполномоченным органом, за исключением установленных законом случаев[1].

Подробнее о правовом статусе каждого из субъектов отношений по обработке персональных данных будет сказано далее.

Комплекс способов правового регулирования и средств юридического воздействия. Наиболее типичными способами правового регулирования принято считать дозволение, запрещение, позитивное обязывание. Как правило, в рамках конкретного правового режима

[1] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017). – Ст. 7.

используется не один, а несколько способов в определенном сочетании или комплексе, при этом часть из них может доминировать, что может свидетельствовать о степени «жесткости» правового режима. Вполне уместным можно считать в этой связи классификацию режимов, предложенную А.В. Деминым:

- *«явочный* режим – режим государственного невмешательства, свободы выбора поведения;
- *регламентационный* – государство формирует правовое пространство, в рамках которого – также свобода выбирать поведение;
- *уведомительный* – предусматривающий информирование государства о выбранном поведении;
- *договорный* – поведение строится в соответствии с условиями соглашения;
- *регистрационный* – предусматривающий обязанность зарегистрировать выбранное поведение;
- *разрешительный* – предусматривающий обязанность получить разрешение на выбранное поведение;
- *распорядительный* – поведение строится на основании прямых указаний государства;
- *запретительный* – режим государственной монополии либо запрет определенных вариантов поведения»[1].

Очевидно, что с такой позиции следует характеризовать правовой режим того или иного вида информации в целом, учитывая, что фактически в рамках правового режима могут быть использованы все способы правового регулирования в различной степени.

Наиболее существенное значение в определении способов и конечном итоге характера правового режима играет его конечная цель, которая должна

[1] Демин, А.В. Общие вопросы теории административного договора: монография / А.В. Демин. – Красноярск: Изд-во Краснояр. ун-та, 1998. – С. 5–7.

быть достигнута путем установления такого режима. Не является исключением в этом случае и правовой режим персональных данных, который направлен на обеспечение информационной безопасности личности через возможность ограничения свободы информации в части оборота информации персонального характера.

Учитывая также общий характер отношений по поводу персональных данных как информации ограниченного доступа, можно говорить скорее о *регламентационном* характере режима персональных данных в целом, в том числе конфиденциальных. Такой вывод обусловлен в значительной степени характеристиками правового статуса субъекта персональных данных, который вправе выбрать в установленных законом рамках наиболее оптимальный, по своему усмотрению, режим своих персональных данных (конфиденциальные и общедоступные персональные данные).

С точки зрения оператора персональных данных, рассматриваемый режим следует характеризовать скорее как *уведомительный*, поскольку закон связывает деятельность по формированию и обработке персональных данных с необходимостью уведомления о таковой уполномоченного органа по защите прав субъектов персональных данных, подразумевая, хоть это прямо и не указано в законе, что субъект персональных данных лично и добровольно передает ему данные, действуя в своем интересе, при условии сохранения их конфиденциальности.

2.3. Конфиденциальность как элемент правового режима персональных данных

Широкое использование термина «конфиденциальность» является сравнительно новым для российского законодательства и практики, которые до появления Федерального закона «Об информации, информационных технологиях и о защите информации»[1], где в ч. 1 статьи 2 было дано определение этому термину, использовали его лишь эпизодически. Впоследствии многие законодательные акты стали приводиться в соответствии с этими положениями и чаще использовать этот термин при обозначении информации с ограниченным доступом, взамен ранее использовавшегося термина «конфиденциальная информация», о чем уже ранее упоминалось в работе.

Прежде чем перейти к анализу непосредственно содержания термина «конфиденциальность», как элемента правового режима персональных данных, стоит сделать некоторое отступление, касающееся взаимоотношения понятий «информационная безопасность», «защита информации» и «конфиденциальность». Такая необходимость целесообразна, учитывая тот факт, что часто эти термины употребляются в одних и тех же текстах.

Общий анализ юридической литературы и источников позволяет говорить о некоторой взаимозаменяемости этих понятий. Наибольшие расхождения, пожалуй, могут возникнуть при трактовке термина «информационная безопасность», который в большинстве случаев, как, например, у В.Н. Лопатина[2], так же как в большинстве программных документов, например в Доктрине информационной безопасности РФ[3], определяется как «состояние защищенности личности, общества и

---

[1] Об информации, информационных технологиях и о защите информации: федер. закон от 29.07.2006 № 149-ФЗ (ред. от 19.12.2016).

[2] Лопатин, В.Н. Информационная безопасность России: Человек. Общество. Государство / В.Н. Лопатин. – Спб.: СПб ун-т МВД РФ, Фонд «Университет», 2000. – С. 79.

[3] Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646). – (https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html). – Дата обращения 02.04.2016.

государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[1]. Аналогичное по сути определение затем было использовано в Федеральном законе «Об участии в международном информационном обмене» (утратил силу)[2]. Как видно, информационная безопасность – это определенное состояние, обеспечивающее реализацию интересов личности, общества и государства в информационной сфере, которое достигается или является целью деятельности по ее обеспечению. Лишь в некоторых случаях можно встретить так называемую «узкую» трактовку термина «информационная безопасность», как например «меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия, и задержек в доступе»[3]. В этом случае речь обычно идет об информационной безопасности каких-либо объектов информации, как то: информационная система, данные или иной конкретный вид информации. Словосочетание «защита информации» является достаточно часто употребляемым, но, как правило, его трактовка отсутствовала в тексте нормативных документов и в доктринальных источниках, к тому же в юридических текстах речь обычно шла скорее о защите не собственно информации, а прав на нее, как например «защита права на доступ к информации» или «защита прав на информацию ограниченного доступа»[4].

С появлением относительно четких законодательных положений, определяющих содержание защиты информации, вопрос был в определенной

---

[1] Бачило, И.Л. Информационное право / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов. – СПб.: Юридический центр Пресс, 2005. – С. 592.

[2] Об участии в международном информационном обмене: федер. закон от 04.07.1996 № 85-ФЗ (ред. от 29.06.2004). (Утратил силу.)

[3] Введение в информационную безопасность. Компьютеры: преступления, признаки уязвимости и меры защиты. – М., 1998.

[4] Лопатин, В.Н. Информационная безопасность России: Человек. Общество. Государство / В.Н. Лопатин. – Спб.: СПб ун-т МВД РФ, Фонд «Университет», 2000. – С. 134, 170.

степени разрешен. Ст. 16 Федерального закона «Об информации, информационных технологиях и о защите информации»[1] указывает на то, что в содержание «защиты информации» входит принятие правовых, организационных и технических мер, направленных:

1) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2) соблюдение конфиденциальности информации ограниченного доступа;
3) реализацию права на доступ к информации.

Соответственно защита информации – это определенный комплекс мер правовых, организационных и технических мер, направленный на обеспечение целостности информации (воспрепятствование уничтожению, модификации, неправомерному блокированию, копированию, предоставлению, распространению и иным неправомерным действиям), соблюдение ее конфиденциальности (создание условий, исключающих неправомерный доступ к информации, ее распространение, разглашение), а также создание условий для реализации права на информацию. Безусловно, эти действия в целом направлены на обеспечение информационной безопасности – создание состояния защищенности интересов личности, общества и государства в информационной сфере и их реализацию. В этом случае следует согласиться с мнением И.Л. Бачило[2], что обеспечение информационной безопасности не ограничивается только защитой информации, которая является важнейшей, но не единственной частью этой деятельности, требующей обращения к политике информатизации в целом, к сложной оценке процессов возникновения и проявления угроз безопасности.

---

[1] Об информации, информационных технологиях и о защите информации: федер. закон от 29.07.2006 № 149-ФЗ (ред. от 19.12.2016).

[2] Бачило, И.Л. Информационное право: учебник для вузов / И.Л. Бачило. – М.: Высшее образование, Юрайт-Издат, 2009. – С. 401.

В итоге вполне можно установить определенную взаимосвязь между понятиями «информационная безопасность», «защита информации» и «конфиденциальность», которые во многом соотносятся как общее и частное. Конфиденциальность при этом можно рассматривать как один из элементов защиты информации, а последнюю – как часть информационной безопасности.

Возвращаясь к термину «конфиденциальность», можно отметить его сравнительно широкое использование в законодательных текстах, в частности, такие положения присутствуют в ст. 7 Федерального закона «О персональных данных»[1], ст. 6 Федерального закона «Об основах социального обслуживания граждан в Российской Федерации»[2], ст. 6 Федерального закона «О финансовом оздоровлении сельскохозяйственных товаропроизводителей»[3], ст. 22 Федерального закона «О третейских судах в РФ»[4], ст. 9 Федерального закона «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов»[5], в ст. 41 Закона РФ «О средствах массовой информации»[6] и многих других законодательных актов.

Одним из первых актов, где стал использоваться этот термин, является Федеральный закон «О коммерческой тайне»[7]. Практически с самого его создания термин «конфиденциальность» стал своего рода лейтмотивом закона и был использован в определении самого понятия «коммерческая тайна», которая трактовалась через «режим конфиденциальности», да и далее по тексту закона он использовался неоднократно. Действующая сейчас редакция содержит его упоминание 18 раз. Причем определение самому

---

[1] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017).

[2] Об основах социального обслуживания граждан в Российской Федерации: федер. закон от 28.12.2013 № 442-ФЗ (ред. от 21.07.2014).

[3] О финансовом оздоровлении сельскохозяйственных товаропроизводителей: федер. закон от 09.07.2002 № 83-ФЗ (ред. от 21.07.2014).

[4] О третейских судах в Российской Федерации: федер. закон от 24.07.2002 № 102-ФЗ (ред. от 29.12.2015).

[5] О государственной защите судей, должностных лиц правоохранительных и контролирующих органов: федер. закон от 20.04.1995 № 45-ФЗ (ред. от 07.02.2017).

[6] О средствах массовой информации: закон РФ от 27.12.1991 № 2124-1 (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 15.07.2016).

[7] О коммерческой тайне: федер. закон от 29.07.2004 № 98-ФЗ (ред. от 12.03.2014). – Ст. 3.

термину «конфиденциальность» так и не было дано, вплоть до его появления в Федеральном законе «Об информации, информационных технологиях и о защите информации» в 2006 году[1].

Современное законодательство трактует его как «обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя».

Надо сказать, что схожие трактовки и положения достаточно часто можно теперь встретить в целом ряде законов и нормативно-правовых актов, однако с некоторыми «нюансами». Дело в том, что термин «конфиденциальность» или те случаи, когда законодательство упоминает его, может иметь некоторые различия в трактовке или содержании.

Достаточно часто для этого используются указание на необходимость субъекта, как правило – конфидента тайны, воздерживаться от определенных действий с информацией, в частности «не передавать[2]», «не раскрывать[3]», «не разглашать[4]», «не сообщать[5]», «не предоставлять[6]», «не распространять»[7].

Такое обилие терминов, с одной стороны, выглядит странным, однако по этому поводу возможны некоторые комментарии. Если вернуться к структуре отношений по охране тайны как конфиденциальной информации, то этому вполне можно найти объяснение.

---

[1] Об информации, информационных технологиях и о защите информации: федер. закон от 29.07.2006 № 149-ФЗ (ред. от 19.12.2016).

[2] О негосударственных пенсионных фондах: федер. закон от 07.05.1998 № 75-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.01.2017). – Ст. 15.

[3] Об инвестиционном товариществе»: федер. закон от 28.11.2011 № 335-ФЗ (ред. от 21.07.2014). – Ст. 12; О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017). – Ст. 7.

[4] О финансовом оздоровлении сельскохозяйственных товаропроизводителей»: федер. закон от 09.07.2002 № 83-ФЗ (ред. от 21.07.2014). – Ст. 6.; О третейских судах в Российской Федерации: федер. закон от 24.07.2002 № 102-ФЗ (ред. от 29.12.2015). – Ст. 22.; О средствах массовой информации: закон РФ от 27.12.1991 № 2124-1 (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 15.07.2016). – Ст. 41.; О коммерческой тайне: федер. закон от 29.07.2004 № 98-ФЗ (ред. от 12.03.2014). – Ст. 11 ч. 2, п. 2.

[5] Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 28.03.2017). – Ст. 727.

[6] О Центральном банке Российской Федерации (Банке России): федер. закон от 10.07.2002 № 86-ФЗ (ред. от 28.03.2017). – Ст. 51, абз. 2.; О банках и банковской деятельности: федер. закон от 02.12.1990 № 395-1 (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.01.2017). – Ст. 26.

[7] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (ред. от 22.02.2017). – Ст. 7.

Основной обязанностью конфидента является сохранение полученных сведений в тайне и иных ограничений на обработку информации, которые установлены ее обладателем, т.е. субъектом тайны. Следовательно, все указанные термины используются для формулировки все той же обязанности конфидента по сохранению тайны сведений, т.е. ограничивают его право на какую-либо их передачу за пределы отношений «обладатель – конфидент». Однако в использовании вышеперечисленных терминов могут быть некоторые отличия. В частности, в определенных случаях предполагается, что информация как бы покидает круг отношений «обладатель – конфидент», не становясь при этом открытой и общедоступной, в таком случае, попадая к другому конфиденту, изменяется ее правовой режим у последнего. И если такие действия предполагаются, а иногда это происходит и без согласия обладателя, например в силу требований закона, то соответственно часто используется формула «не разглашать», т.е. «не предавать огласке» или, иными словами, исключить смену правового режима информации с режима информации ограниченного доступа на режим общедоступной информации.

В иных случаях, когда предполагается, что права обладателя могут быть нарушены, в том числе самим фактом передачи сведений третьим лицам пусть и на условиях соблюдения конфиденциальности отношений, т.е. «конфидент – субконфидент», то в таком случае вполне логичным будет описание обязанностей конфидента как «не сообщать», «не передавать», «не раскрывать», имея в виду в том числе и разглашение информации, как передачу ее неограниченному кругу лиц.

В целом можно говорить о том, что общий анализ существующих законодательных положений определяет термин «конфиденциальность» как требование, обращенное к конфиденту воздерживаться от действий по передаче или раскрытию информации третьим лицам, т.е. не участникам отношений «обладатель – конфидент» или неопределенному кругу лиц. При этом конфидент, по-видимому, должен воздерживаться именно от активных действий по передаче, сообщению, раскрытию, разглашению информации.

В таком случае возникает вопрос о достаточности подобных действий для защиты интересов обладателя. Как выясняется, это далеко не всегда так. В частности, Федеральный закон «О коммерческой тайне»[1] одним из первых указывает на необходимость «охраны конфиденциальности информации», которая предусматривает ряд фактически активных действий – мероприятий по выполнению этого требования. Более того, смысл статьи 10 этого закона напрямую связывает выполнение или реализацию этих мер с применением к той или иной информации режима коммерческой тайны. Эти меры могут быть также дополнены иными, как то – применение технических средств и методов защиты информации. Далее в п. 5 всё той же статьи 10 указывается на то, что применяемые меры являются разумными и достаточными, если выполнены два условия: «исключается доступ к информации, составляющей коммерческую тайну, без согласия ее обладателя и обеспечивается возможность использования информации работниками и передачи ее контрагентам без нарушения режима коммерческой тайны». Как видим, термин «конфиденциальность» в таком случае подразумевает осуществление определенных действий по защите информации от несанкционированного обладателем доступа к ней со стороны третьих лиц, невыполнение которых, по-видимому, можно рассматривать как отказ к применению в отношении этой информации режима коммерческой тайны, следовательно, о его отсутствии.

Надо сказать, что представленный в Федеральном законе «О коммерческой тайне» перечень является в некотором роде аналогичным мероприятиям по защите государственной тайны, который можно представить в упрощенном виде:

- определение объекта защиты, т.е. какая информация защищается, ее перечень;
- принятие для защиты организационных мер;
- определение лиц, имеющих право доступа;

[1] О коммерческой тайне: федер. закон от 29.07.2004 № 98-ФЗ (ред. от 12.03.2014).

- определение порядка, правил обработки, обращения информации;
- определение ответственных лиц, подразделений за организацию мероприятий по защите информации;
- учет лиц, получивших доступ, и материальных носителей информации;
- использование для защиты информации технических средств: использование программных, программно-технических, технических средств (средства аутентификации, криптографии, резервного хранения, видеонаблюдения, охраны, сигнализации, антивирусные средства и др.).

Безусловно, напрямую в Законе РФ «О государственной тайне», в отличие от Федерального закона «О коммерческой тайне», такой перечень не присутствует отдельно в одной из статей, но его вполне можно сформировать из общего системного анализа закона с поправкой на «секретность» вместо «конфиденциальности» и некоторые другие особенности.

К сожалению, другие законодательные и нормативные акты, как правило, никак не раскрывают суть того, каким образом будет обеспечиваться конфиденциальность сведений, т.е. не раскрывают, в чем состоит специальный режим той или иной тайны. Аналогичного мнения придерживается и Е.К. Волчинская[1], говоря о конфиденциальности применительно к нотариальной тайне, она отмечает отсутствие соответствующих положений в большинстве законодательных и нормативных актов, включая нормы законодательства о нотариате. Далее в своих рассуждениях Е.К. Волчинская совершенно справедливо отмечает, что конкретно режим тайны определен только в случае государственной и коммерческой тайны, а также тот факт, что без этого (т.е. без указания на конкретные меры по обеспечению «конфиденциальности») режим «нотариальной тайны» не выглядит «завершенным и убедительным».

[1] Волчинская, Е.К. Нотариальная тайна и режимы конфиденциальности / Е.К. Волчинская // Нотариальный вестник. – 2013. – № 4 (апрель). – (http://www.notariat.ru/publ/zhurnal-notarialnyj-vestnik/archive/5499/6525/). – Дата обращения 02.04.2017.

Ст. 16 Федерального закона «Об информации, информационных технологиях и о защите информации» также содержит лишь достаточно общее указание на конфиденциальность, как одно из направлений правовых, организационных и технических мер по обеспечению защиты информации, в рамках которых обладатель, оператор информационной системы должен обеспечить:

- «предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль над обеспечением уровня защищенности информации»[1].

Примечательно, что федеральный закон о персональных данных также первоначально не содержал никаких указаний на конкретные меры защиты, которые должен был предпринять оператор для защиты персональных данных в информационных системах, а лишь содержал общее требование предпринимать «организационные и технические меры» для защиты персональных данных, причем до 2009 года в обязательном порядке указывал на необходимость использования шифровальных (криптографических) средств, совершенно не делая различий между разными информационными системами, объемами данных и других обстоятельств, что серьезным образом

[1] Об информации, информационных технологиях и о защите информации: федер. закон от 29.07.2006 № 149-ФЗ (ред. от 19.12.2016).

затрудняло реализацию закона и стоимость таких мероприятий. Указанные положения неоднократно подвергались критике как со стороны операторов, так и со стороны ученых-юристов.

Итогом работы над дальнейшим совершенствованием законодательных положений стала существенная переработка статьи 19, а также появление статьи 18.1 Федерального закона «О персональных данных», которые в действующей редакции уже содержат конкретный и в достаточной степени детальный перечень мер, как организационных, так и технических, которые должные быть приняты оператором для защиты персональных данных. В целом этот перечень вполне можно уложить в уже озвученный выше алгоритм защиты информации применительно к коммерческой и государственной тайне:

1. Определение объекта защиты. Сюда можно отнести положения ст. 2 Закона, а также ст. 18 и ст. 22, которые в совокупности обязывают оператора определить объем обрабатываемых персональных данных.
2. Принятие организационных мер:
    - принятие соответствующих локальных актов и разработка политики конфиденциальности, определяющих порядок и правила обработки персональных данных оператором (ст. 18.1, ч. 1, п. 2, 4, 5; ст. 18.1, ч. 2, п. 4; ст. 19, ч. 2, п. 8);
    - назначение и определение ответственных лиц и подразделений за организацию обработки персональных данных (ст. 18.1, ч. 1, п. 1);
    - ознакомление работников оператора, непосредственно осуществляющих обработку, с нормами законодательства о персональных данных, политикой конфиденциальности и локальными нормативными актами об обработке персональных данных и их обучение, что фактически позволяет говорить о них как о специальных субъектах юридической ответственности (ст. 18.1, ч. 1, п. 6);

- учет лиц, имеющих доступ к персональным данным, и учет материальных носителей (ст. 19, ч. 2, п. 5 и 8);
- иные организационные меры по контролю (аудиту) обработки персональных данных и их защите (ст. 18.1, ч. 2, п. 6 и 9; ст. 19, ч. 1, п. 4);

3. Использование технических мер по защите информации (ст. 18.1, ч. 1, п. 3 и ст. 19, ч. 2, п. 2).

По мнению автора, более логично этот общий алгоритм изложен в утвержденном Постановлением Правительства от 21 марта 2012 года № 211[1] Перечне мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами». Несмотря на то, что Перечень относится только к одной из групп операторов – государственным и муниципальным органам, но в целом содержит общий порядок действий по организации защиты информационных систем персональных данных, укладывающийся на все 100% в существующие и уже сложившиеся алгоритмы защиты информации, используемые в случае государственной и коммерческой тайны. Отличие закона о персональных данных заключается и в значительно более подробной детализации необходимых к применению оператором организационных и технических мер, причем в зависимости от определенных параметров информационных систем персональных данных, что выглядит вполне логично, учитывая, что в первую очередь при защите персональных данных преследуются интересы субъекта, а не оператора.

Более подробно применяемые организационные и технические меры устанавливаются исходя из типов информационных систем. Так, в

[1] Постановление Правительства РФ «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» от 21.03.2012 № 211 (ред. от 06.09.2014).

соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных (далее – Требования)[1], они подразделяются на 5 основных видов, в зависимости от категорий персональных данных, обрабатываемых в них:

- информационные системы, в которых обрабатываются специальные категории персональных данных (касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных);
- информационные системы, в которых обрабатываются биометрические персональные данные;
- информационные системы, в которых обрабатываются общедоступные персональные данные;
- информационные системы, в которых обрабатываются персональные данные работников/сотрудников оператора;
- информационные системы, в которых обрабатываются иные категории персональных данных.

В то же время в соответствии с Требованиями выбор организационных и технических мер защиты информации в информационных системах персональных данных зависит от 3 критериев:

- *Категорий персональных данных*. Соответственно обработка в информационной системе специальных категорий персональных данных или биометрических персональных данных существенно повышает требования к их защищенности, в то время как обработка только общедоступных персональных данных существенно их снижает.
- *Объема данных*. Требования защищенности информационной системы повышаются с возрастанием количества субъектов персональных данных, данные о которых содержатся в системе.

[1] Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 01.11.2012 № 1119.

- *Видов угроз*, которые актуальны для информационной системы в части появления недокументированных (недекларированных) возможностей в системном или прикладном программном обеспечении. Всего три типа угроз: для 1-го типа вероятны недокументированные (недекларированные) возможности в системном программном обеспечении; для 2-го типа – в прикладном программном обеспечении, для 3-го типа – иные недокументированные (недекларированные) возможности.

Используя эти критерии, устанавливаются 4 уровня защищенности, каждый из которых со своим обязательным перечнем организационных и/или технических мер, обусловленных определенной комбинацией названных выше критериев. Соответствие уровня защищенности вышеуказанным критериям можно представить в виде следующей таблицы (см. табл. 1).

Таблица 1

Требуемый уровень защищенности	Предполагаемый тип угроз			Категории персональных данных				Объем данных (количество субъектов, данные о которых содержит ИСПД[1])	
	1-й тип	2-й тип	3-й тип	Спец. кат. ПД[2]	Биометрич. ПД	Иные ПД	Общедоступные ПД	Более 100 тыс.	Менее 100 тыс.
1-й уровень	X			X	X				
		X		X				X	
2-й уровень	X						X		
		X		X					X
		X			X				
		X						X	
		X				X		X	
			X	X				X	
3-й уровень		X					X		X
		X				X			X

[1] ИСПД – информационная система персональных данных
[2] ПД – персональные данные

			X	X					X
			X		X				
			X			X		X	
4-й уровень			X				X		
			X			X			X

В соответствии с данными таблицы для установления того и ли иного уровня защищенности достаточно наличия у информационной системы одного из наборов соответствующих показателей, каждый набор при этом соответствует одной из строчек таблицы, т.е. для установления, к примеру, 1 ровня защищенности достаточно наличия одного из двух наборов критериев, а для 2-го — шести и т.д.

Каждый уровень защищенности обеспечивается путем выполнения оператором информационной системы персональных данных соответствующих требований, которые целесообразно представить также в виде таблицы (см. табл. 2):

Таблица 2

Уровни защищенности ИСПД				Требования, необходимые к выполнению оператором	№
1-й уровень	2-й уровень	3-й уровень	4-й уровень	Организация режима обеспечения безопасности помещения, где размещается ИСПД, препятствующего возможности неконтролируемого проникновения или пребывания, лиц, не имеющих доступа	•
				Обеспечение сохранности носителей ПД	•
				Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к ПД, обрабатываемым в ИС, необходим для выполнения ими служебных (трудовых) обязанностей	•
				Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз	•

				Назначение должностного лица (работника), ответственного за обеспечение безопасности ПД в ИС	•
				Автоматическая регистрация в журнале безопасности изменений полномочий сотрудника оператора по доступу к ПД, содержащимся в ИС	•
	Не применяются	Не применяются	Не применяются	Создание структурного подразделения, ответственного за обеспечение безопасности ПД в ИС либо возложение ее на имеющееся структурное подразделение	•

Анализ приведенных данных позволяет говорить о том, что объем требований, а, следовательно, и уровень защищенности информационной системы повышается от четвертого уровня к первому уровню. Наиболее защищенным является первый уровень, для реализации которого к оператору предъявляется наибольший объем требований.

Приведенные перечни требований к организационным и техническим мерам защиты информационных систем персональных данных были еще более подробно раскрыты в Приказе ФСТЭК от 18 февраля 2013 года, который уже детально раскрывает состав и содержание организационных и технических мер по защите персональных данных при их обработке в информационных системах персональных данных. На основании этого документа в зависимости от требуемого уровня защищенности оператору необходимо применять следующие меры по обеспечению безопасности информационных систем персональных данных:

- «идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и

(или) обрабатываются персональные данные;

- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее – инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных»[1].

Приведенные меры могут иметь различное содержание и также варьируются в зависимости от требуемого уровня защищенности информационной системы и предполагаемых типов угроз, описанных ранее, на основании чего формируется базовый набор мер, соотношение которых подробно раскрывается в Приложении к составу и содержанию мер по обеспечению безопасности персональных данных в информационных системах персональных данных. Предполагается, что оператор на основании анализа информационной системы и ее параметров адаптирует указанный

[1] Приказ ФСТЭК России Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. № 21.

базовый набор мер, исходя из структурно-функциональных ее характеристик. При этом оператор обязан проводить оценку эффективности принимаемых мер не реже одного раза в 3 года, как самостоятельно, так и с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите информации.

В соответствии с частью 1 статьи 12 Федерального закона «О лицензировании отдельных видов деятельности»[1] к лицензируемым видам деятельности относятся: деятельность по разработке и производству средств защиты конфиденциальной информации и деятельность по технической защите конфиденциальной информации. На основании этих положений приняты соответствующие постановления Правительства «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» и «О лицензировании деятельности по технической защите конфиденциальной информации». Оба эти документа не проводят никакого различия между различными видами конфиденциальной информации, а, следовательно, в одинаковой степени применимы для оценки применяемых оператором мер по защите конфиденциальности персональных данных, в тех случаях, когда требуется использование технических средств. Последнее еще более показывает на общность мероприятий, методик и алгоритмов защиты информации ограниченного доступа, включая обеспечение ее конфиденциальности.

Таким образом, конфиденциальность информации является, с одной стороны, необходимым элементом защиты информации ограниченного доступа, с другой стороны, определенным ее состоянием, когда исключается неправомерный доступ к ней, достигаемым путем реализации комплекса мер правового, организационного и технического характера.

Соответственно «*конфиденциальность* следует трактовать как –

[1] О лицензировании отдельных видов деятельности»: федер. закон от 04.05.2011 № 99-ФЗ (ред. от 30.12.2015) (с изм. и доп., вступ. в силу с 01.01.2017).

элемент правового режима информации ограниченного доступа, выражающегося в реализации конфидентом комплекса мероприятий правового, организационного и технического характера, направленного на исключение возможности неправомерного доступа к ней».

Конфиденциальность в определенном смысле можно рассматривать и как необходимое «режимное» требование, обращенное к конфиденту – оператору, работнику, иному лицу, которое имеет доступ к конфиденциальной информации на законном основании. Указанное требование может быть установлено обладателем информации или на основании закона. Требует также определенного пояснения и тот факт, что требование конфиденциальности может иметь различное содержание, в том числе и применительно к различным видам правоотношений. Все вышесказанное в большей степени применимо к административным, информационным, гражданско-правовым отношениям, тогда как в трудовых отношениях требование «конфиденциальности» может иметь несколько иное значение, которое скорее можно рассматривать как часть должностных обязанностей, связанных с определенным порядком работы с информацией при их исполнении.

ГЛАВА 3. ФОРМИРОВАНИЕ РОССИЙСКОГО И ЗАРУБЕЖНОГО ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Современные тенденции развития законодательства о персональных данных в зарубежных странах

Проблема защиты персональных данных уже давно не является чем-то новым для большинства государств мира. Законодательная основа для правового регулирования персональных данных начала формироваться уже более 40 лет назад. В Европе, равно как и в США, в конце 1960-х годов, как результат оценки рисков для прав и свобод в условиях развития новых информационных технологий обработки информации, появляются законы о защите персональных данных. Первый закон о персональных данных был принят в Германии в федеральной земле Гессен еще в 1970 году, и впоследствии лег в основу федерального закона, принятого в 1977 году. Первые законы о защите данных при их автоматической обработке на национальном уровне появились в 1973 в Швеции, и в 1974 году в США (Акт о защите частной жизни – Privacy Act)[1].

В целом в мире, по данным организации Прайваси Интернэшенал, законодательство о защите персональной информации принято более чем в 100 странах, в число которых вошла и Россия[2]. Законодательство о защите неприкосновенности частной жизни и защите персональных данных имеет схожие тенденции развития, что объясняется, в определенной степени, принятием на международном уровне соответствующих документов, направленных на гармонизацию национальных законов, а также общими целями защиты – защита прав и свобод субъекта (индивида) при обработке данных.

---

[1] The Privacy Act of 1974, 5 U.S.C. § 552a. – (https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf). – Дата обращения 02.05.2017.

[2] Banisar, D. National Comprehensive Data Protection / D. Banisar // Privacy Laws and Bills. – 2016. – 28 Nov. – (https://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416). – Дата обращения 02.05.2017.

Нормативные и декларативные документы о защите данных приняты в рамках некоторых региональных и универсальных объединений государств. В то же время в связи с обилием этих документов целесообразным видится рассмотрение не всех их, а наиболее «авторитетных источников», которые оказали значительное влияние на формирование национальных систем защиты персональных данных, т.е. с анализа и правовой оценки источников международного права, которые могут дать общее представление о развитии законодательства в области защиты данных, являясь своего рода обобщением национального опыта и практики, отмечая при этом характерные особенности в правовом регулировании отдельных стран. Международные источники рассмотрены далее преимущественно в хронологическом порядке их появления, их места в системе источников права соответствующих международных организаций, а также с точки зрения их влияния на национальное законодательство и практику.

Организация по экономическому развитию и сотрудничеству

Первым документом такого рода стали «Основные положения Организации по экономическому развитию и сотрудничеству (ОЭСР), о защите неприкосновенности частной жизни и международных обменов персональными данными» (далее по тексту – Основные положения), которые были приняты 23 сентября 1980 года[1]. Предпосылкой для создания документа стала необходимость объединения усилий государств в области защиты персональных данных при их трансграничной передаче, исходя из того, что различия в национальном законодательстве могут вызвать серьезные проблемы в важных секторах экономики (банковском деле, страховании и т.д.). Разработчиком выступила приглашенная группа экспертов во главе с судьей М.Д. Кирби, председателем австралийской комиссии по реформированию судебной системы, которая и подготовила текст Рекомендаций Совета ОЭСР в области защиты неприкосновенности

[1] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. – (http://www.oecd.org /sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm). – Дата обращения: 02.04.2017.

частной жизни и международных обменов персональными данными[1]. Основной целью принятия рассматриваемого документа было скорее упрощение международного трансграничного обмена персональными данными между государствами-участниками при условии соблюдения необходимых гарантий неприкосновенности частной жизни, что должно было способствовать экономическому и социальному развитию государств[2].

В целом сферу действия Основных положений можно сформулировать как «автоматизированная обработка персональных данных в государственном и частном секторе экономики, которая может нести угрозу нарушения неприкосновенности частной жизни и других индивидуальных свобод»[3]. При этом упоминалась возможность распространения действия Основных положений не только на автоматизированную обработку персональных данных, но и возможность установления государствами-участниками ОЭСР в своем законодательстве дополнительных мер защиты неприкосновенности частной жизни и индивидуальных свобод. В качестве исключений для применения Основных положений к обработке данных были названы суверенитет и безопасность государства и публичный порядок, с упоминанием того, что такие случаи должны быть «редкими» и обязательно известны общественности.

Основу правового механизма защиты прав индивида, предложенного Основными положениями, составляет ряд принципов, изложенных в части 2 документа, к которым были отнесены:

– ограничение объема данных;

– качество данных;

– конкретизация целей;

– ограничение на использование данных;

– обеспечение безопасности;

– открытость;

[1] Там же. – EXPLANATORY MEMORANDUM.
[2] Там же. – Часть первая, § 2 и 3.
[3] Там же. – Часть первая, § 2 и 3.

– индивидуальное участие (контроль субъекта данных);

– ответственность.

Именно эти 8 принципов стали в итоге основой для формирования национального законодательства в странах-участницах ОЭСР. В отношениях между собой государства-участники обязывались принимать разумные и должные меры к обеспечению непрерывного и безопасного международного обмена персональными данными, единственным исключением к созданию препятствий и ограничений рассматривалась невозможность обеспечения защиты персональных данных другим государством-участником.

В качестве механизма реализации обязательств, вытекающих из Основных положений, государствам предлагалось: принять соответствующее внутреннее законодательство, поощрять и поддерживать саморегулирование, обеспечить наличие разумных механизмов реализации прав субъекта, предусмотреть санкции и иные средства защиты прав субъекта, обеспечить недискриминационное отношение к субъектам данных.

Обязательства по реализации Основных положений взяли на себя 34 государства-участника ОЭСР: Австралия, Австрия, Бельгия, Канада, Чехия, Дания, Франция, Германия, Венгрия, Исландия, Италия, Япония, Корея, Нидерланды, Новая Зеландия, Норвегия, Польша, Испания, Швейцария, Великобритания, США, т.е. почти все ведущие страны Европы, а также страны с развитой экономикой по всему миру[1]. Кроме этого, по собственной инициативе присоединилось еще одно государство, не являющееся участником ОЭСР – Албания. Обязательства по рассматриваемому документу были выполнены еще в 1998 году всеми государствами-участниками ОЭСР, как было заявлено на встрече министров в Оттаве[2].

В дальнейшем в рамках ОЭСР была создана система мониторинга реализации государствами Основных положений, а также, учитывая

[1] The OECD Privacy Framework, 2013 OECD. – (http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf). – Дата обращения 02.05.2017. – P. 2.

[2] Report on the Cross-Boarder Enforcement of the Privacy Laws, OECD 2006. – (http://www.oecd.org/sti/ieconomy /informationsecurityandprivacy.htm). – Дата обращения 02.05.2017. – P. 12.

масштабы глобализации электронной торговли, – специальная рабочая группа по информационной безопасности и защите частной жизни. Последняя совместно с Секретариатом ОЭСР регулярно, раз в 2 года, по итогам мониторинга подготавливает доклады о состоянии реализации участниками своих обязательств[1]. По оценкам специалистов рабочей группы, во всех государствах-участниках ОЭСР, несмотря на наличие иногда существенных отличий в подходах государств к регулированию обработки персональных данных, выполнены обязательства, указанные в Основных положениях.

Среди этих государств, особняком выделяются государства ЕС и Совета Европы, где помимо Основных положений фактором гармонизации можно назвать Конвенцию Совета Европы о защите личности в связи с автоматической обработкой персональных данных, а также Директиву ЕС 95/46/ЕС[2]. В этих государствах были приняты законодательные акты, в полной мере охватывающие все обязательства, вытекающие из Основных положений. Типичным органом защиты прав субъекта персональных данных в этих государствах стали комиссары, специальные уполномоченные по защите данных или специальные комиссии. Остальные государства ОЭСР также приняли специальное законодательство в области защиты персональных данных, возложив обязанности по контролю на уже существующие органы государственной власти. Канада, Австралия, Новая Зеландия выполнили все требования по принятию законодательства, учредив в качестве уполномоченного органа по защите данных специальных комиссаров по защите данных. Особый подход отмечен лишь у США, где наиболее сложная система уполномоченных органов, поскольку их четыре, и каждый отвечает за свой аспект. Аналогичным образом устроено и законодательство, причем урегулирован на уровне федерального законодательства в целом лишь публичный сектор, тогда как частный в

[1] Report on the Cross-Boarder Enforcement of the Privacy Laws, OECD 2006. – (http://www.oecd.org/sti/ieconomy /informationsecurityandprivacy.htm). – Дата обращения 02.05.2017. – P. 12–18.
[2] Там же.

большей степени действует на основе принципа саморегулирования. Более подробно особенности правового регулирования персональных данных в США будут рассмотрены далее.

В 2013 году рабочая группа экспертов ОЭСР подготовила новую версию Основных положений, которая была утверждена Советом ОЭСР 11 июля 2013 года[1]. Основанием к подготовке обновленной версии Основных положений стало признание существенной роли, которую стали играть персональные данные в экономике, обществе и повседневной жизни. Причиной этого стали глубокие и значительные изменения в информационной среде и экономике, которые создают дополнительные угрозы правам человека. Согласно отчету экспертов рабочей группы, изменения коснулись трех концептуальных идей (концептов):

– *формирование национальной стратегии защиты частной жизни (приватности)*, требующей координации на самом высоком правительственном уровне, при наличии эффективных национальных законов о персональных данных;

– *формирование эффективных управленческих практик по защите частной жизни*, которые могут стать ключевым звеном в фактическом или практическом обеспечении прав личности;

– *извещение о нарушении безопасности (конфиденциальности) персональных данных*, при этом информация о нарушении должна доводиться не только до сведения контролирующего органа, но и непосредственно до субъекта данных.

Как следствие в обновленной версии Основных положений появились положения, касающиеся обязанностей оператора, расширения прав субъектов персональных данных, а также положения о контролирующем органе, включая его понятие.

[1] The OECD Privacy Framework, 2013 OECD. – (http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf). – Дата обращения 02.05.2017. – P. 3.

Примечательно, что Россия предприняла ряд усилий по вступлению в число стран ОЭСР, и в 2007 году Совет ОЭСР принял Дорожную карту по присоединению Российской Федерации к Конвенции об Учреждении ОЭСР[1]. В то же время среди указанных направлений сотрудничества на тот момент, как, впрочем, и в последующем, вопросы, касающиеся защиты персональных данных не были обозначены. По сообщению сайта ОЭСР процесс вступления Российской Федерации официально временно приостановлен с 13 марта 2014 года[2].

Совет Европы

В рамках Совета Европы можно говорить о двух аспектах правового регулирования обработки персональных данных. Первый связан с существующим наднациональным механизмом защиты прав субъекта персональных данных через уже имеющийся и эффективно функционирующий механизм Конвенции о защите прав человека и его основных свобод (далее по тексту – Конвенция)[3]. Речь идет о деятельности Европейского суда по правам человека (далее по тексту – Суд) в рамках толкования и защиты права на уважение частной жизни, предусмотренного статьей 8 Конвенции. Данный документ, как и практика Суда, являются в соответствии с Протоколом № 11[4] обязательными для стран-участниц, а это 47 европейских государств, включая Россию[5].

Несмотря на то, что напрямую в Конвенции ничего не говориться о персональных данных и правовом регулировании их обработки и многих других подобных аспектах, действие ее распространяется на правовое регулирование персональных данных в той части, которая затрагивает

[1] Дорожная карта присоединения Российской Федерации к Конвенции об учреждении ОЭСР (принята на 1163-й сессии Совета ОЭСР 30 ноября 2007). – (http://oecdru.org/zip/ROADMAP_RUS.doc). – Дата обращения 02.05.2017.

[2] Вступление России в ОЭСР. – (http://oecdru.org/roadmap.html). – Дата обращения 02.05.2017.

[3] Конвенция о защите прав человека и основных свобод (заключена в Риме 04.11.1950) (с изм. от 13.05.2004). Вместе с Протоколом № 1 (подп. в Париже 20.03.1952); Протоколом № 4 об обеспечении некоторых прав и свобод помимо тех, которые уже включены в Конвенцию и первый Протокол к ней (подп. в Страсбурге 16.09.1963); Протоколом № 7 (подп. в Страсбурге 22.11.1984).

[4] Протокол № 11 к Конвенции о защите прав человека и основных свобод о реорганизации контрольного механизма, созданного в соответствии с Конвенцией (подп. в Страсбурге 11.05.1994).

[5] Государства-члены Совета Европы // Официальный сайт Совета Европы. – (http://www.coe.int/ru/web/about-us/our-member-states). – Дата обращения 02.05.2017.

нарушение прав и свобод, предусмотренных текстом Конвенции. В первую очередь это касается права на уважение частной жизни. За последние десятилетия в практике Суда накоплено значительное количество дел, прямо или косвенно затрагивающих те или иные аспекты защиты персональных данных. В некоторых случаях Суд прямо указывает на тесную связь персональных данных со смыслом и содержанием статьи 8 Конвенции. К примеру, в деле *S. & Marper v. United Kingdom* Судом было заявлено, что «само хранение персональных данных о частной жизни лица должно рассматриваться в качестве вторжения в частную жизнь в контексте статьи 8 Европейской конвенции о защите прав человека и его основных свобод. Последующее использование сохраненной информации не меняет этого вывода»[1].

Общий анализ существующей судебной практики Европейского суда по правам человека позволяет выделить целый ряд проблемных аспектов, которые так или иначе были им исследованы или затронуты.

Сбор персональных данных

В практике Европейского суда по правам человека можно назвать ряд решений, в которых были затронуты отдельные аспекты, связанные с обработкой персональных данных, такие как: сбор, хранение, раскрытие, разглашение и доступ субъекта к информации (данным) о нем, а также необходимость гарантировать защиту, т.е. сохранять конфиденциальность данных в отдельных случаях. Одним из первых дел стало дело Гаскина против Соединенного Королевства, в котором «Суд постановил, что поскольку в личном деле заявителя содержатся сведения сугубо личного характера о его детстве, развитии и последующей жизни, получение такой информации необходимо для того, чтобы узнать и понять свое детство, ранние этапы развития»[2]. Подобные «данные, таким образом, являются

[1] Case of S. and Marper v. The United Kingdom. Judgement of 04.12.2008. – (http://hudoc.echr.coe.int/eng?i=001-90051)/ – Дата обращения 02.05.2017. – § 67.
[2] Case of Gaskin v. The United Kingdom. Judgement of 07.07.1989. – (http://hudoc.echr.coe.int/eng?i=001-57491). – Дата обращения 02.05.2017. – § 89.

«главным источником информации о его прошлом и годах развития» и ограничение доступа к ним Суд посчитал нарушением ст. 8, а процедуры, существующие в Соединенном Королевстве, не обеспечивающими уважения права заявителя на частную и семейную жизнь»[1]. Другим примером, где было подчеркнута идея необходимости сохранения конфиденциальности персональной информации, может быть дело «Z против Финляндии», где Европейский суд по правам человека указал, что уважение тайны данных о здоровье человека является важнейшим принципом правовых систем всех участников Совета Европы. Поэтому внутреннее законодательство должно предоставлять гарантии для предотвращения распространения или разглашения сведений о здоровье человека, в особенности сведений о наличии у лица ВИЧ-инфекции. Исключение в этом случае возможно лишь в интересах расследования и наказания преступлений и обеспечения гласности судебного производства[2]. Также Суд исследовал вопрос о регулировании «использования имени и фамилии – вопрос о фамилии отдельного человека относится к его/ее личной и семейной жизни, поскольку он подразумевает вопрос персональной идентификации. Тот факт, что может существовать общественный интерес в вопросе о регламентировании использования фамилии, не является достаточным, чтобы вывести вопрос о фамилии отдельного лица из-под защиты положения об уважении личной и семейной жизни. Те же принципы применимы и к именам, которые тоже имеют отношение к личной и семейной жизни, поскольку этот вопрос относится к проблеме идентификации личности в рамках своих семей и сообщества»[3].

Как нетрудно заметить, практика Суда лишь косвенным образом содержит регулирование – определенные казуальные нормы, которыми государства-участники должны руководствоваться, чтобы избежать

---

[1] Там же.

[2] Case of Stjerna v. Finland. Judgement of 25.11.1994. – (http://hudoc.echr.coe.int/eng?i=001-57912)/ – Дата обращения 02.05.2017.

[3] Case of Guillot v. France. Judgement of 24.10.1996. – (http://hudoc.echr.coe.int/eng?i=001-58069). – Дата обращения 02.05.2017.

нарушений статьи 8 Конвенции о защите прав человека и его основных свобод, в том числе и при обработке персональных данных.

В целом практика Суда становится все более разнообразной, что объяснимо как с позиции развития представлений о праве на уважение частной жизни и тех правомочий, которые теперь вкладываются в содержание этого понятия, так и с точки зрения развития современных информационных технологий, которые формируют новые виды угроз правам человека, в том числе и связанные с персональными данными. Так, в частности, за последние несколько лет можно назвать, по крайней мере, десяток достаточно известных дел, касающихся сбора, хранения и использования персональных данных спецслужбами и правоохранительными органами. Часть из этих дел напрямую касались России. В 2011 году Суд признал практику по созданию «базы данных наблюдения», используемой для сбора информации о передвижениях поездом, самолетом в пределах России, и о задержаниях лиц, занимающихся правозащитной деятельностью, противоречащей ст. 8 Конвенции[1]. В 2013 году в деле Avilkina and Others v. Russia[2] требование следственного органа, в связи с расследованием уголовного дела в отношении Свидетелей Иеговы, к публичным клиникам сообщать о фактах отказа последователями секты от переливания крови было также признано противоречащим Конвенции, несмотря на то, что в целом жалоба заявителей была отклонена как неприемлемая. В одном из последних дел в отношении России в деле Roman Zakharov v. Russia, решение по которому было принято в 2015 году, Европейский суд по правам человека указал на нарушение требований государством статьи 8 Конвенции в части наличия законодательных норм, обязывающих операторов связи

[1] Case of Shimovolos v. Russia. Judgement of 21.06.2011. – (http://hudoc.echr.coe.int/eng?i=001-105217)/. – Дата обращения 02.05.2017.
[2] Case of Avilkina and Others v. Russia. Judgement of 06.06.2013. – (http://hudoc.echr.coe.int/eng?i=001-120071). – Дата обращения 02.05.2017.

устанавливать оборудование для сбора данных о телефонных переговорах и управляемое непосредственно спецслужбами[1].

Безусловно, Россия является далеко не единственной страной, практика защиты персональных данных которой была рассмотрена Европейским судом в последние годы. В частности, в 2009 году законодательство Франции, устанавливающее возможность формирования органами полиции базы данных о лицах, совершивших преступления сексуального характера, также была признана противоречащей статье 8 Конвенции. В сущности, таких примеров, когда в объектив Суда попадают законодательство и практика государств в области защиты персональных данных, становится все больше и что, вероятно, в дальнейшем потребует отдельного детального изучения.

Второй аспект напрямую связан со специальным регулированием обработки персональных данных и созданием наднациональных механизмов гармонизации законодательства стран-участниц Совета Европы. Проблема защиты прав и свобод личности при обработке данных начала обсуждаться в Европе еще в середине 70-х годов прошлого века. В 1973 и 1974 гг. Комитет министров Совета Европы принял две резолюции о защите неприкосновенности частной жизни в связи с созданием электронных банков данных – одну для частного, другую для государственного сектора[2]. Обе эти резолюции содержат рекомендации правительствам стран – членов Совета Европы принять меры к обеспечению соблюдения базовых принципов защиты, относящихся к получению данных, качеству данных и праву частного лица на получение информации о своих персональных данных и способах их использования. Позднее Совет Европы, выполняя инструкции своего Комитета министров, начал подготовку международной Конвенции о защите неприкосновенности частной жизни в отношении зарубежной

[1] Case of Roman Zakharov v. Russia. Judgement of 04.12.2015. – (http://hudoc.echr.coe.int/eng?i=001-159324). – Дата обращения 02.05.2017.

[2] Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. – (https://rm.coe.int/16800ca434). – Дата обращения 02.05.2017. – Part 4.

обработки персональных данных и передачи данных через государственные границы. С ноября 1976 года по май 1979 года Комитет по защите данных провел четыре заседания[1]. Рабочая группа, составленная из экспертов, представляющих Австрию, Бельгию, Францию, ФРГ, Италию, Нидерланды, Испанию, Швецию, Швейцарию и Великобританию, несколько раз собиралась между пленарными заседаниями Комитета, с тем чтобы разработать общую философию, а также уточнить детали проекта Конвенции. В апреле 1980 года другой комитет экспертов пересмотрел и доработал текст. Он был одобрен Европейским комитетом по правовому сотрудничеству и утвержден Комитетом министров 17 сентября 1980 г. Конвенция получила название – «О защите личности в связи с автоматизированной обработкой персональных данных», также известная, как Конвенция Совета Европы № 108 (далее по тексту – Конвенция)[2], вобравшая в себя весь предшествующий опыт и ставшая основным документом в этой области для стран-участниц Совета Европы.

Конвенция оказалась более объёмным документом по сравнению с Основными положениями ОЭСР и, как следствие, более проработанным. Несмотря на схожесть отдельных положений, в качестве принципиальных отличий можно указать упоминание в Конвенции в качестве одной из основных целей – не только гарантировать защиту прав и свобод личности при трансграничной передаче информации, но и поставить проблему защиты личности при принятии решений, затрагивающих его права и свободы, на основании персональных данных, подвергающихся автоматизированной обработке как государственными, так и частными структурами. Кроме этого, следует отметить расширение и более качественную проработку понятийного аппарата Конвенции, в особенности появление определений: «автоматизированная база данных», «автоматическая обработка», «контролер

[1] Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. – (https://rm.coe.int/16800ca434). – Дата обращения 02.05.2017. – § 17.

[2] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в Страсбурге 28.01.1981) // Сайт компании «КонсультантПлюс». – (http://www.consultant.ru/document/cons_doc_LAW_121499/). – Дата обращения: 02.04.2017.

базы данных», что существенным образом конкретизировало сферу ее применения в этой части. Как и Основные положения ОЭСР, Конвенция в качестве основной области применения оговаривала именно автоматизированную обработку персональных данных в частном и публичном секторах, при этом предлагая государствам определенную гибкость в сфере установления определенных категорий персональных данных под особой защитой, а также распространения действия положений Конвенции на данные, не подвергающиеся автоматической обработке, о чем сторона должна была сделать соответствующее одностороннее заявление, без права требовать от другой стороны подобных же действий[1].

Самым главным отличием Конвенции стал сам характер документа, как международного договора, который имеет обязательную силу для его участников, т.е. государства обязались реализовать его положения – имплементировать их во внутреннее законодательство, о чем следует из положений ст. 4 и ст. 7, тогда как Основные положения имели рекомендательных характер и предусматривали обязательства как добровольное волеизъявление сторон. Ключевой в определении механизма регулирования обработки персональных данных, предложенного Конвенцией, следует назвать главу 2 «Основные принципы защиты данных». Механизм защиты описан через установление основных требований, предъявляемых к обработке данных, как то: законность и добросовестность получения и обработки (ст. 5 п. a); законность целей обработки (ст. 5 п. b); соответствие объема персональных данных целям обработки (ст. 5 п. c); точность (ст. 5 п. d); ограниченность времени хранения персональных данных, позволяющих идентификацию, целями обработки (ст. 5 п. e). Также упоминается об особых категориях персональных данных – о национальной принадлежности, политических взглядах, религиозных и иных убеждениях и т.д., при обработке, которых должны быть предусмотрены специальные

[1] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в Страсбурге 28.01.1981) // Сайт компании «КонсультантПлюс». – (http://www.consultant.ru/document/cons_doc_LAW_121499/). – Дата обращения: 02.04.2017. – Ст. 3 ч. 3.

гарантии. Существенную часть в описании механизма регулирования обработки данных занимают права (гарантии) субъекту, которые заключаются в предоставлении прав по контролю обработки персональных данных о себе через возможность:

- доступа к ним и к информации о контролере;
- требовать их уточнения, уничтожения, в случае нарушений правил обработки;
- обращения за судебной защитой, которые должны быть гарантированы субъекту, при этом каждая сторона вправе установить дополнительные меры защиты[1].

Одновременно Конвенция с достаточной точностью сформулировала допустимые исключения и ограничения из установленных требований к обработке персональных данных. Исключения допускаются лишь на основании закона в целях охраны государственной и общественной безопасности, денежных интересов государства, пресечения преступлений, для защиты прав субъекта данных, прав и свобод других лиц. Ограничения могли быть установлены только в исследовательских и статистических целях, при условии гарантирования прав и свобод субъекта[2].

Остальные главы Конвенции, за исключением, пожалуй, главы 3, где описывается общее обязательство государств-участников не препятствовать трансграничному обмену данных, иначе как при отсутствии надлежащей защиты данных с другой стороны, носят скорее процедурный характер и посвящены взаимодействию участников Конвенции между собой посредством оказания взаимной помощи, через взаимодействие уполномоченных органов по защите данных, через создание специального Консультативного комитета, а также процедуре вступления Конвенции в

---

[1] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в Страсбурге 28.01.1981) // Сайт компании «КонсультантПлюс». – (http://www.consultant.ru/document/cons_doc_LAW_121499/). – Дата обращения: 02.04.2017. – Ст. 8.

[2] Там же. – Ст. 9.

силу и порядка внесения поправок, односторонних заявлений сторон, оговорок, касательно исполнения ею отдельных положений.

Касательно реализации Конвенции и ее имплементации во внутренние законодательные системы государств-участников, надо сказать, что этот процесс еще не завершен. Почти все государства в качестве средства имплементации выбрали принятие национального закона о защите данных или же внесения соответствующих поправок в уже существующие законы (Франция). В течение первых 4–5 лет после принятия законы о защите данных были приняты и вступили в силу лишь в 7 государствах Европы (Австрия, Дания, Франция, ФРГ, Люксембург, Норвегия, Швеция)[1]. До 2000 года к ним присоединились еще 13 государств (Бельгия, Дания, Финляндия, Греция, Венгрия, Исландия, Ирландия, Италия, Нидерланды, Португалия, Словения, Швейцария, Великобритания). В целом на 2017 год из 47 государств-участников Конвенция была ратифицирована и имплементирована в той или иной степени во всех, т.е. за последние 17 лет она была имплементирована еще в 27 государствах. В числе самых отстающих оказались: Российская Федерация (2013), Сан-Марино (2015) и Турция (2016)[2]. Стоит отметить еще одну небольшую группу государств, в которых вопрос о защите персональных данных был закреплен и на конституционном уровне (ст. 35 Конституции Португалии 1976 года, ст. 18 Конституции Испании 1978 года, ст. 1 Закона о персональных данных Австрии 1978 года)[3].

Однако принятием Конвенции деятельность Совета Европы в области правового регулирования персональных данных не ограничилась. Комитетом министров государств – членов Совета Европы были приняты также специальные Рекомендации, касающиеся использования и защиты

---

[1] Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. – (https://rm.coe.int/16800ca434). – Дата обращения 02.05.2017.

[2] Chart of signatures and ratifications of Treaty 108 “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data» (Status as of 20.05.2017). – (http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=I4WkWbbB). – Дата обращения 20.05.2017.

[3] Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. – (https://rm.coe.int/16800ca434). – Дата обращения 02.05.2017. – § 5.

персональных данных в разных областях жизнедеятельности общества и государства: медицины (1981); научных исследований и статистики (1983); маркетинга (1985); социального обеспечения (1986); в секторе полиции (1987); занятости (1989); в отношениях, связанных с финансовыми выплатами и сделками (1990); в отношениях, связанных с передачей данных третьим лицам (1991); в сфере защиты персональных данных в области телесвязи, специфических телефонных услуг (1995); защиты медицинских и генетических данных (1997); защиты персональных данных при сборе и обработке в статистических целях (1997); о защите частной жизни при использовании сети Интернет (1999); о защите персональных данных при страховании индивидов (2002); о защите индивидов при автоматической обработке персональных данных при создании профайлов (2010); о защите прав личности при использовании социальных сетей (2012); о защите прав личности при использовании поисковых систем (2012); о принятии Руководства по защите прав личности для интернет-пользователей (2014); об обработке персональных данных при трудоустройстве (2015); об обеспечении свободы выражения мнений и защите прав на неприкосновенность частной жизни и сохранении «сетевого нейтралитета» (2016)[1]. Очевидно, что работа в этом направлении активно продолжается, отвечая на актуальные вызовы современного информационного общества.

Европейский союз

Комиссия Европейских сообществ озаботилась проблемой правового регулирования персональных данных, также в целях обеспечения гармонизации национальных законов государств-участников, практически одновременно с Советом Европы и даже на первых порах в тесном сотрудничестве[2].

Однако процесс принятия мер по гармонизации национальных законов растянулся на длительное время, отчасти, по-видимому, из-за того, что

[1] Legal Instruments for Data Protection, Council of Europe. – (http://www.coe.int/en/web/data-protection/legal-instruments). – Дата обращения 20.05.2017.
[2] Braibant, G. Données personnelles et société de l'information / G. Braibant. – Paris, 2000. – P. 55–56.

многие государства-участники на тот момент уже приняли соответствующие законодательные меры, как участники Совета Европы, а отчасти и ввиду, того, что деятельность Сообществ в целом не была направлена на охрану прав и свобод человека. Процесс активизировался уже после принятия Маастрихтского договора в 1992 году, а также ввиду расширения Европейского союза. Окончанием этого процесса стало принятие широко известной Директивы 95/46/ЕС Европейского парламента и Совета Европейского союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных[1] (далее по тексту – Директива). Она стала основным документом, который установил соответствующие стандарты в области правового регулирования персональных данных в ЕС, а также, по мнению многих авторов, одним из наиболее авторитетных нормативных источников в этой сфере.

Первоначально в качестве основной цели и одновременно юридической основы для принятия Директивы стали не только необходимость гарантирования прав и свобод, но и во многом экономические причины, а именно – формирование единого рынка[2]. Юридической основой для принятия стала ст. 7 Договора, о чем неоднократно делается ссылка в преамбуле Директивы[3], где говорится о необходимости обеспечения свободного движения данных с одновременным гарантированием фундаментальных прав и свобод индивида между государствами-участниками, без чего невозможно свободное передвижение товаров, людей, услуг, как основы единого рынка. В условиях возрастающих потоков данных между государствами, Европейский союз обоснованно посчитал различия в

[1] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Дата обращения: 02.04.2017.
[2] The First Report on the implementation of the Data Protection Directive (95/46/EC) (COM(2003) 265. – 2004. – 24 February. – (http://www.statewatch.org/news/2004/mar/data-prot-ep.pdf). – Дата обращения 20.05.2017.
[3] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Дата обращения: 02.04.2017. – п. 27 Преамбулы.

правовом регулировании персональных данных на национальном уровне негативным фактором.

Принятая Директива стала важным фактором гармонизации законодательства европейских стран в сфере защиты персональных данных, учитывая ее статус и юридическую силу. В рамках ЕС директивы имеют обязательную юридическую силу в отношении государств-участников при свободе выбора средств их реализации, но при этом могут иметь прямое действие на их территории в случае невыполнения государством своих обязательств в установленные сроки или противоречия внутренней практики директивам[1].

В качестве сферы применения Директива указывает автоматизированную обработку персональных данных, а также неавтоматизированную обработку, в тех случаях, когда она осуществляется схожим образом, путем организации информации в виде файлов, папок, позволяющим быстрый доступ к необходимой информации. Директива не применяется к обработке данных:

– осуществляемой физическим лицом в личных и бытовых целях;

– осуществляемой в целях, которые выходят за рамки компетенции ЕС – обеспечение обороны и безопасности государства, иной публичный интерес.

В сравнении с уже рассмотренными документами Директива содержит еще более подробный понятийный аппарат, что также конкретизирует сферу ее деятельности. Принципиальным отличием понятийного аппарата Директивы стало закрепление в ней терминов, «файл персональных данных», «лицо, которому поручена обработка персональных данных (обработчик)», «третье лицо», «получатель», «согласие субъекта персональных данных».

Основу механизма правового регулирования составляет установление принципов обработки персональных данных, которые делятся на две

[1] Халиев, К.Р. Нормативная сила «директив» ЕС / К.Р. Халиев // Актуальные проблемы экономики и права. – Казань: Познание, 2008. – № 3 (7). – С. 163–166.

категории: требования к качеству персональных данных и требования к их обработке. К первым отнесены принципы в ст. 6:

– законность и добросовестность обработки;

– сбор данных только в установленных целях;

– достаточность, относимость к делу, неизбыточность;

– точность и актуальность;

– ограничение срока хранения целями обработки.

Вторая группа требований относится к критериям законности обработки персональных данных в ст. 7, в число которых входят:

– наличие согласия субъекта данных;

– необходимость исполнение договора, стороной которого является субъект данных, а равно принятие необходимых мер до заключения договора, по просьбе субъекта;

– необходимость исполнения лицом, ответственным за обработку персональных данных, своих законных обязательств;

– необходимость защиты жизненных интересов субъекта данных;

– необходимость обработки в связи с осуществлением публичных полномочий или в рамках исполнения полномочий публичным органом власти, которые поручены лицу, ответственному за обработку данных, или сообщены третьему лицу;

– необходимость обработки в связи с защитой законных интересов лица, ответственного за обработку данных, или третьих лиц, которым они сообщены, при условии, что это не перевешивает интересы защиты основных прав и свобод, в том числе права на уважение частной жизни.

Так же, как и Конвенция Совета Европы № 108, Директива выделяет особую группу так называемых «чувствительных» данных (данные о расовой, этнической принадлежности, политических взглядах, философской и религиозной принадлежности, членстве в профсоюзах, здоровье и интимных сторонах жизни), к обработке которых предъявляет особые

требования, при этом раскрывая их. Такие данные запрещены к обработке за исключением случаев, если:

– субъект выразил свое согласие, за исключением случаев, когда этого недостаточно в соответствии с законом государства;
– обработка необходима для осуществления обязательств лица, ответственного за обработку данных, в сфере трудовых отношений, если это разрешено законодательством и при наличии соответствующих гарантий;
– обработка необходима для защиты жизни и здоровья субъекта или другого лица, при условии невозможности, физической или юридической, получения согласия субъекта;
– обработка осуществляется некоммерческими объединениями в отношении данных о своих членах в политических, религиозных, профсоюзных целях, при условии соответствующих гарантий;
– обработка касается только явно общедоступных данных или является необходимой для защиты лицом своих прав в суде.

Перечень в этом случае не является исчерпывающим (ст. 8, п. 4), и государства вправе устанавливать иные исключения при установлении соответствующих гарантий и извещения об этом Европейской комиссии (ст. 8, п. 6). Директива позволяет также вести обработку рассматриваемой категории данных в целях осуществления превентивной медицины, медицинской диагностики, здравоохранения, при условии сохранения «профессиональной тайны». Примерно схожее требование касается и данных о правонарушениях и привлечении к уголовной ответственности или о применении к лицу мер предварительного характера (мер пресечения), если только они не осуществляются специальным уполномоченным законом органом при наличии гарантий прав субъекта.

Следует подчеркнуть еще две особенности этого документа. Во-первых, Директива фактически (ст. 8, п. 7) четко распространила свое действие на так называемые «персональные идентификаторы», которые

также могут быть предметом обработки данных, т.е. быть включены в состав персональных данных. Во-вторых, Директива закрепила соотношение необходимости защиты персональных данных со свободой выражения мнения. В этой связи она допускает исключения и отступления от требований, предусмотренных в ней, в целях осуществления журналистской деятельности, художественного, литературного творчества при условии баланса между правом на частную жизнь и свободой выражения мнений в соответствии с национальным законодательством, к сожалению, не предлагая какого-либо конкретного варианта.

Механизм Директивы содержит гарантии соблюдения прав субъекта, к которым можно отнести:

– право на доступ к данным о себе;

– на возражение против их обработки;

– гарантии при автоматизированном принятии решений;

– юридические гарантии защиты прав, нарушенных в связи с обработкой персональных данных, и возмещение вреда, ими причиненного.

При обработке (сборе) данных Директива требует соответствующего информирования об этом субъекта, причем в достаточно подробной форме, с указанием информации о лице, ответственном за обработку данных, целях обработки, иную информацию (о правах субъекта данных на доступ ним, информацию о получателях данных и т.д.). Кроме этого, субъект и сам вправе получить подробную информацию об обработке по своему запросу, в частности подтверждение об обработке данных, информацию о получателях данных, алгоритм принятия решений на основании данных при их автоматизированной обработке, и требовать извещения третьих лиц, которым сообщены данные, обо всех изменениях, в них внесенных[1]. В случае несогласия лица с обработкой его персональных данных он вправе возражать

[1] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Дата обращения: 02.04.2017. – Ст. 12

против нее, прежде всего в случаях, если его согласие не было получено[1]. Автоматическое принятие решений на основании персональных данных допускается только при условии надлежащих гарантий со стороны закона или в случае заключения/исполнения договора, если при этом существует возможность высказать свое мнение субъектом[2]. Если права субъекта нарушены, то национальное законодательство должно предоставить субъекту надлежащие средства их защиты посредством обращения в суд или уполномоченный орган по контролю обработки персональных данных[3] и право требовать возмещения ущерба[4], а также установить надлежащие санкции за нарушения в сфере обработки персональных данных[5].

Отдельное внимание Директива отводит вопросам защиты данных и контроля их обработки. Обработка персональных данных должна осуществляться только конфиденциально, по поручению или с согласия лица, ответственного за нее[6]. Государства-участники при этом обязаны требовать от последнего принятия организационно-технических мер по защите данных от незаконных или случайных действий (доступа, уничтожения, распространения и т.д.)[7]. О любом случае обработки персональных данных должно быть предварительно сообщено лицом, ответственным за нее уполномоченному органу по контролю[8], который определяется государством самостоятельно, с указанием полной информации об обработке (информация об ответственном лице, характере, объеме данных, целях обработки, информация о получателях и т.д.), за исключением обработки данных о свих членах некоммерческими объединениями и других случаев. установленных национальным законодательством[9]. Сведения,

[1] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Дата обращения: 02.04.2017. – Ст. 14.
[2] Там же. – Ст. 19.
[3] Там же. – Ст. 22.
[4] Там же. – Ст. 23.
[5] Там же. – Ст. 24.
[6] Там же. – Ст. 16.
[7] Там же. – Ст. 17.
[8] Там же. – Ст. 29.
[9] Там же. – Ст. 19.

указанные в извещении об обработке данных, должны быть общедоступными и уполномоченный орган по контролю в сфере персональных данных ведет соответствующий их реестр[1].

Исключения из представленного механизма правового регулирования Директива допускает на основании национального законодательства лишь в целях защиты превалирующего публичного интереса, как то: защита и безопасность государства, общественная безопасность, предотвращение, пресечение правонарушений, существенный экономический или финансовый интерес, защита прав других лиц, а также в случаях, когда невозможно нанести ущерб правам субъекта данных (обезличивания данных) в статистических, научно-исследовательских целях[2].

В отношении трансграничной передачи данных положения Директивы принципиально схожи с другими международными документами, но более подробны и касаются третьих стран, не участников ЕС. Передача данных возможна лишь при наличии определенных гарантий защиты прав субъекта получателем, за исключением случаев получения согласия субъекта, необходимости исполнения соглашения, защиты жизни и здоровья субъекта и других случаев[3].

Как и рассмотренные ранее Основные положения ОЭСР, Директива уделяет внимание и существованию дополнительного механизма регулирования отношений в сфере обработки персональных данных, как то: поощрение государствами-участниками ЕС разработки «кодексов поведения» различного рода профессиональными ассоциациями лиц, ответственных за обработку данных, которые бы способствовали реализации национального законодательства о персональных данных[4].

---

[1] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Дата обращения: 02.04.2017. – Ст. 21.
[2] Там же. – Ст. 13.
[3] Там же. – Ст. 25–26.
[4] Там же. – Ст. 27.

В заключении Директива сосредотачивается на уполномоченном органе (органах) по контролю за исполнением законодательства о персональных данных, который должен быть предусмотрен каждым государством-участником. В полномочия такого органа в обязательном порядке должны входить: полномочия по расследованию, с правом доступа к данным и получения иной необходимой информации для осуществления надзора; полномочия по вмешательству в процесс обработки данных (приостанавливать и запрещать обработку); полномочия обращаться в правоохранительные органы и суд в случае обнаружения нарушений, а также самостоятельно рассматривать обращения (заявления) физических лиц[1].

Для координации усилий государств-участников, в соответствии с Директивой создается Группа по защите лиц в связи с обработкой персональных данных, в состав которой входят представители уполномоченных органов по контролю за исполнением законодательства о персональных данных государств-участников. Она исполняет консультативные функции, связанные с реализацией Директивы в национальном законодательстве, а также консультирует Еврокомиссию по проектам ее изменений и других решений в сфере персональных данных. Для реализации Директивы и контроля ее реализации со стороны ЕС был также создан Комитет, состоящий из представителей государств-участников, основной функцией которого была помощь Еврокомиссии при принятии решений, касающихся персональных данных[2].

В соответствии с заключительными положениями по истечении трех лет Еврокомиссия должна была сделать первый доклад о ходе реализации Директивы, т.е. в 1998 году. Однако не все государства-участники на тот момент имплементировали ее и приняли специальные законодательные акты или внесли изменения в уже имеющиеся, поскольку на момент принятия

[1] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Дата обращения: 02.04.2017. – Ст. 29.
[2] Там же. – Ст. 32.

Директивы в 13 из 15 государств-участников уже имелись общие законодательные акты о защите данных[1]. В этой связи объемный доклад был сделан Еврокомиссией лишь в 2004 году[2]. В докладе в первую очередь было указано, что, несмотря на задержки в реализации директивы государствами-участниками, основные цели ее принятия были достигнуты и препятствия свободному обращению данных были устранены, одновременно при высокой степени защиты прав субъекта, поскольку механизм регулирования обработки персональных данных содержит одни из наиболее строгих требований в мире по защите прав личности. В то же время было отмечено, что иногда значительная разница в законодательстве стран-участников по-прежнему представляет трудности для определения общеевропейской политики в области персональных данных. Одновременно в Докладе содержалось детальное научное, в том числе и социологическое, исследование последствий введения Директивы в национальное законодательство, а также отношение к проблемам обработки персональных данных со стороны граждан, организаций, органов государственной власти, при этом в разных секторах общественной жизни и экономики во всех странах ЕС[3]. На основании этих исследований было выявлено, что к 2003 году порядка 60% опрошенных граждан в ЕС обеспокоены (из них 25% крайне обеспокоены) проблемой защиты своих прав при обработке персональных данных. В то же время только 10,4% опрошенных высказались за то, что уровень защиты их данных является достаточным, большая часть (81%) посчитали его недостаточным, плохим ли очень плохим, и лишь 3,46% нашли его хорошим или очень хорошим). Опубликованные позднее результаты опросов среди лиц, ответственных за обработку данных, показал, что они нашли уровень защиты данных, обусловленный национальным

[1] Braibant, G. Données personnelles et société de l'information / G. Braibant. – Paris, 2000. – P. 64
[2] The First Report on the implementation of the Data Protection Directive (95/46/EC) (COM(2003) 265. 24 February 2004. – (http://www.statewatch.org/news/2004/mar/data-prot-ep.pdf). – Дата обращения 20.05.2017.
[3] Там же.

законодательством, средним (54%) или высоким (27%) и лишь 10% заявили, что он низкий[1].

На основании столь всеобъемлющего исследования были выявлены проблемы, как то: отсутствие необходимых ресурсов для выполнения Директивы, небрежное отношение к обработке данных со стороны ответственных за нее лиц, низкий уровень информированности субъектов данных о своих правах[2]. В качестве возможных путей решения были предложены не только обсуждение мер по повышению эффективности реализации Директивы в национальное законодательство и меры по гармонизации последнего, но, в частности, и консультации, рекомендации для государств, вступающих в ЕС, которые должны были также принять меры к ее реализации, а также призвать все государства способствовать развитию технологий защиты данных и «саморегулирования» на основе добровольных «кодексов поведения», предусмотренных главой 5 Директивы[3].

На сегодняшний момент во всех 28 государствах ЕС приняты базовые законы о защите данных[4], часть из них была принята еще до официального вступления, в рамках так называемого переходного периода. Одними из последних законы приняли Эстония (2003), Кипр (2003), Литва (2004), Польша (2004). В основном наиболее явным отличием являются различия в органах по контролю в сфере персональных данных. В основном были избраны несколько вариантов:

- *комиссар* (единоличный орган) по защите данных (омбудсмен, регистратор), например: в Ирландии, Великобритании, Люксембурге;

[1] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Дата обращения: 02.04.2017.
[2] Там же. – С. 15
[3] Там же.
[4] Data protection bodies. – (http://ec.europa.eu/justice/data-protection/bodies/index_en.htm). – Дата обращения 20.05.2017.

- *коллегиальный орган* (комиссия) по защите данных – Франция, Финляндия, Греция, Португалия, Австрия;
- *представительный коллегиальный орган*, включающий в себя представителей работодателей, предпринимателей, профсоюзов, общественных организаций и т.д.) – Швеция, Испания[1].

Принятием Директивы 95/46/ЕС нормативное регулирование обработки данных со стороны ЕС не ограничилось, хотя она и явилась основой для последующих действий и решений. Далее действия и решения органов ЕС касались уже отдельных сфер защиты персональных данных. Среди этих документов следует отметить еще одну основополагающую Директиву – Директиву 2002/58/ЕС Европейского парламента и Совета Европейского союза от 12 июля 2002 года о конфиденциальности и электронных средствах связи, касающуюся обработки персональных данных и защиты частной жизни в сфере электронных коммуникаций[2], с изменениями, внесенными Директивой 2006/24/ЕС, и заменившую ранее принятую Директиву 97/66/ЕС Европейского парламента и Совета Европейского союза от 15 декабря 1997 года касательно использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций. Названная Директива посвящена регулированию вопросов хранения данных о соединении в интересах оперативной деятельности правоохранительных органов, рассылке нежелательных сообщений, использованию файлов с информацией о соединениях (т.н. cookies), а также включению персональных данных в публичные справочники. В целом Директивой были установлены категории

[1] Data protection bodies. – (http://ec.europa.eu/justice/data-protection/bodies/index_en.htm). – Дата обращения 20.05.2017.

[2] Директива Европейского Парламента и Совета Европейского союза 2002/58/ЕС от 12 июля 2002 г. в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи) (Текст в редакции Директивы 2006/24/ЕС Европейского парламента и Совета ЕС от 15 марта 2006 г., Директивы 2009/136/ЕС Европейского парламента и Совета ЕС от 25 ноября 2009 г.). – (http://isafety.ru/wp-content/uploads/2015/07/005_Директива-2002-58-ЕС.pdf). – Дата обращения 20.05.2017.

сохраняемых данных, сроки хранения, условия просмотра данных о соединении, принципы защиты данных в сфере электронных коммуникаций.

Часть актов в рамках ЕС, например, Решения Еврокомиссии 2001/497/ЕС, 2004/535/ЕС, 2004/915/ЕС, касались такого важного вопроса, как заключение межгосударственных соглашений с третьими государствами о передаче данных и предлагали типовые варианты таких соглашений, в том числе и в отношении конкретных стран (США).

Отдельно можно упомянуть и еще один показательный документ – это Регламент 45/2001/ЕС Европейского парламента и Совета Европейского союза от 18 декабря 2000 года, касающийся защиты частных лиц при обработке персональных данных институтами и органами ЕС и свободы обращения данных. На основании Регламента был гарантирован физическим лицам повышенный уровень защиты данных, также был создан специальный орган по контролю в сфере персональных данных и реализации положений данного документа органами и институтами ЕС[1].

В одном из сообщений Еврокомиссии Европейскому парламенту и Совету была отмечена в целом успешная реализация Директивы 95/46/ЕС[2], хотя при этом по-прежнему были названы некоторые проблемы (независимость органов по контролю в сфере персональных данных, существенные различия национального законодательства). Более того, Еврокомиссия особо высказала надежду на усиление работы в указанном направлении в свете процесса принятия государствами ЕС нового конституционного договора ЕС, который в ст. II-68 содержит положение о праве на защиту персональных данных, как части права на частную жизнь, и сверх этого ст. I-51 содержит юридическую основу для принятия ЕС

[1] Regulation (EC) № 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. – (http://data.europa.eu/eli/reg/2001/45/oj). – Дата обращения 20.05.2017.

[2] Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century. – (http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX: 52012DC0009). – Дата обращения 20.05.2017.

положений, регулирующих обработку персональных данных в других сферах экономики, помимо теле- и электронных коммуникаций.

Другие международные организации

Другие международные организации также последовали примеру ОЭСР, Совета Европы и Европейского союза. Однако их документы, в отличие от ранее упомянутых, в основном были рекомендательного характера и не оказали такого эффекта на национальное законодательство. В частности, среди таких международных организаций можно назвать: ООН, МОТ, ВТО, Организацию стран по азиатско-тихоокеанскому экономическому сотрудничеству (ОАТС), СНГ.

В ООН первый документ такого рода был принят Генеральной ассамблеей в 1990 году (Резолюция № 45/95 от 14 декабря 1990 года[1]). В этой резолюции также были установлены общие положения касательно минимальных гарантий защиты прав личности при обработке персональных данных. Их отличие от Основных положений ОЭСР принципиально заключается в установлении более подробного описания гарантий при обработке «чувствительных» персональных данных, переносе акцента на защиту прав субъекта, в том числе в рамках международных организаций, а также впервые в закреплении положений о необходимости существования уполномоченного органа по контролю в сфере обработки персональных данных, чего не было сделано в Конвенции Совета Европы № 108.

МОТ приняла соответствующий ряд решений рекомендательного характера[2], которые могут быть использованы при разработке национального законодательства о труде и заключении коллективных соглашений.

Страны азиатско-тихоокеанского сотрудничества озаботились проблемой обработки персональных данных скорее ввиду экономических

---

[1] Резолюция Генеральной Ассамблеи ООН «Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера» от 14 декабря 1990 г. № 45/95 // Система ГАРАНТ. – (http://base.garant.ru/2565319/#ixzz4hcq10mD5). – Дата обращения 20.05.2017.

[2] Protection of workers' personal data. ILO code of practice. – (http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_engl.pdf). – Дата обращения 20.05.2017.

причин и в целях поддержания экономических связей со странами Европы, где действующее законодательство области персональных данных может создать препятствия экономическим отношениям. В этой связи разработка рекомендаций была поручена Группе по развитию электронной торговли, которая и сосредоточила на этом внимание, взяв за основу все те же Основные положения ОЭСР[1].

В рамках СНГ для гармонизации законодательства стран-участниц Межпарламентской ассамблеей был разработан и принят Модельный закон «О персональных данных» (Постановление № 14-19 от 16 октября 1999 года)[2]. Отличительными особенностями его стали: более расширенный понятийный аппарат, введения положений о лицензировании деятельности в области обработки данных, а также описание действий по обработке персональных данных и требований к ним. В то же время документ, безусловно, имел рекомендательный характер и не имел положений об обязательствах государств по его реализации. Во многом сложно говорить о том, какое влияние он оказал на национальные правовые системы стран-участников, поскольку те государства, которые приняли соответствующие законы о защите данных или высказались за его принятие, являются одновременно участниками Конвенции Совета Европы № 108 (Молдова, Украина, Россия, Грузия).

Зарубежная практика (США – Европа)

После рассмотрения вопроса об инструментах гармонизации национального законодательства и предложенных механизмах правового регулирования обработки персональных данных в рамках международных

[1] APEC Privacy Framework. – (http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx). – Дата обращения 20.05.2017.

[2] Модельный закон «О персональных данных» принят на 14-м пленарном заседании Межпарламентской ассамблеи государств-участников СНГ (Постановление № 14-19 от 16 октября 1999 года) // Межпарламентская Ассамблея государств-участников Содружества Независимых Государств: Информационный бюллетень. – 2000. – № 23. – С. 315–326.

организаций возможно говорить о некоторых общих тенденциях в зарубежной практике.

В этой связи, естественно, выделяются страны европейского континента, где степень гармонизации законодательства достигла наибольшего уровня. В настоящий момент законодательство о защите персональных данных принято более чем в 100 странах, и 28 из них – это страны ЕС, к которым можно прибавить еще 22 государства-члена Совета Европы. Таким образом, получается, что практически половина государств, в которых существует специальное законодательство о персональных данных и которые включились в процесс гармонизации своих норм с законодательством других стран, расположены на европейском континенте.

В основном их законодательство строится на основе общих принципов обработки данных, установлении гарантий прав субъекту при обработке его данных, а также при их трансграничной передаче. Различия касаются лишь некоторых положений в допускаемых рамках, установленных актами о гармонизации (Директивой и Конвенцией Совета Европы № 108), о чем уже шла речь выше – вопрос об уполномоченном органе по контролю обработки данных, установление различного рода исключений, в случае где присутствует превалирующий публичный интерес, установление положений при обработке особых категорий данных и т.д.

За пределами Европы находится сравнительно небольшое количество стран, которые также озаботились проблемами защиты прав индивида при обработке персональных данных (большая часть из них входит в ОЭСР: Австралия, Канада, Япония, Южная Корея, Новая Зеландия, США) и, как уже было сказано, также приняли ряд законодательных мер для защиты данных. Среди этих государств немногие смогли достичь уровня защиты персональных данных, который существует в странах Европейского союза. В частности, Европейская комиссия назвала лишь 12 стран вне рамок ЕС, в которых, по ее мнению, существует адекватный уровень защиты персональных данных: Андорра, Аргентина, Канада, Швейцария, Фарерские

острова, Гернси, Израиль, Мэн, Джерси, Новая Зеландия, США, Уругвай[1]. В отношении других стран, при трансграничной передаче данных требуется предоставление соответствующего уровня защиты данных, как правило, путем заключения соответствующего соглашения. Одним из самых известных таких соглашений можно назвать Соглашение между ЕС и США о передаче персональных данных об авиапассажирах, после заключения которого уровень защиты данных об авиапассажирах из стран ЕС был признан соответствующим[2].

Пожалуй, по-прежнему достаточным своеобразием и серьезными отличительными чертами обладает механизм защиты персональных данных, предусмотренный законодательством США, причем настолько, что вполне можно говорить о другом подходе к правовому регулированию персональных данных, чем тот, который распространен в большинстве европейских государств и который заслуживает отдельного упоминания.

США уже давно известны как страна, где право на уважение частной жизни получило широкое признание и уважение, учитывая, что и сами термины «частная жизнь» или «право на частную жизнь» во многом появляются как интерпретация термина “right of privacy”, введенного в употребление американскими юристами, о чем уже ранее говорилось.

В течение долгого периода американской истории, именно понятие “privacy” (прайваси) – становится ключевым словом-концепцией для всей американской системы права. Первоначально данная концепция описывала лишь достаточно ограниченные аспекты частной жизни, подлежащие защите на основании текста 4-й поправки к Конституции США, однако, благодаря гибкости и адаптивности конституционного права количество правомочий постоянно возрастало.

---

[1] Commission decisions on the adequacy of the protection of personal data in third countries. – (http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm). – Дата обращения: 20.05.2017.

[2] The EU-U.S. Privacy Shield. – (http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm). – Дата обращения 20.05.2017.

В частности, «прайваси» в первую очередь затрагивала такие аспекты, как право на жилище, на тайну переписки, а затем и телефонных переговоров, электронных и иных сообщений, т.е. так называемых privacy rights.

Развитие компьютерных технологий обработки информации, в которых США является одним из бесспорных лидеров и в настоящее время, привело к неизбежному вопросу защиты «прайваси» (частной жизни), в первую очередь – в условиях автоматизированной обработки информации о физических лицах в электронных базах данных.

Для изучения вопроса Департаментом здравоохранения, образования и социальной защиты (Department of Health, Education and Welfare) была создана специальная комиссия по изучению вопроса, которая еще в 1973 году в своем докладе обратилась с рекомендациями к Конгрессу по принятию специального законодательства – Кодекса честной информационной практики (Code of Fair Information Practice[1]), основанного на следующих принципиальных положениях:

- отсутствие баз персональных данных, существование которых скрывается или является секретным;
- предоставление индивиду права знать, какая информация содержится о нем в базе данных и как она используется;
- предоставление права индивиду воспрепятствовать использованию информации, полученной с определенной целью, в других целях или передаче другим лицам без его согласия;
- индивид должен иметь право требовать внесения изменений, исправлений или дополнения информации о нем, в случае ее недостоверности;
- организация, осуществляющая создание, поддержание, использование и распространение персональных данных, должна

[1] FTC Fair information practice principles. – (http://inflection.com/privacy/frameworks-were-watching/ftc-fair-information-practice-principles). – Дата обращения 20.05.2017.

обеспечить достоверность персональных данных, а также принять меры к предотвращению их ненадлежащего использования.

Кроме этого, специальный доклад содержал рекомендации для организаций, ведущих обработку персональной информации о необходимости защиты последней, а также о необходимости ежегодного опубликования сведений о базах данных и содержащейся в них информации.

Большая часть положений доклада легла в основу принятого год спустя Акта о защите частной жизни 1974 года (The Privacy Act of 1974[1], далее – Акт).

История принятия этого документа стала компромиссом между двумя законопроектами, которые появились одновременно, один в Палате представителей, а другой – в Сенате. Отличались они в основном порядком возмещения вреда, причиненного субъекту данных. Законопроект Сената в этом отношении был более суров, и для возмещения вреда было достаточно лишь установления факта нарушения, тогда как законопроект Палаты представителей предусматривал возможность возмещения лишь в том случае, если будет доказано, что нарушения были умышленными и грубыми. В итоге смешанная комиссия пришла к общему мнению, согласовав общий текст будущего закона, который предусматривал, что для отдельных нарушений требовалось доказывать их преднамеренный характер для получения возмещения. В остальном – положения двух законопроектов были практически идентичны и легли в основу принятого Акта.

Сам Акт является интересным документом для изучения и в полной мере характеризует своеобразность американского подхода к правовому регулированию обработки персональной информации, в связи с чем автору видится логичным рассмотреть его положения более детально.

Первое, что стоит упоминания, – это сфера действия Акта, которую можно назвать достаточно ограниченной. Акт, в частности, предоставлял

[1] The Privacy Act of 1974 (Pub. L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552a). – (https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf). – Дата обращения 20.05.2017.

права в сфере обработки персональной информации, включая право на судебную защиту, исключительно гражданам и постоянным резидентам. Однако положения Акта применялись исключительно в отношении федеральных правительственных агентств, за исключением 7-го раздела касательно номера социальной защиты (Social Security Number – SSN), применяемого в отношении федеральных, местных органов власти и органов власти штатов. Номер социальной защиты может быть предоставлен исключительно на основании федерального закона, в котором в обязательном порядке указывается, является ли такое сообщение SSN добровольным или обязательным. Впрочем, это никак не мешало штатам принимать специальное законодательство, которое бы предусматривало правила обработки персональной информации органами штатов и местными органами власти, помимо положений 7-го раздела Акта. Таким образом, различные федеральные агентства, подчиняющиеся федеральному правительству, в полной мере попали под действие положений Акта, среди них стоит назвать: почта США, департамент образования, Федеральное бюро расследований и многие другие. Еще одним ограничением стало упоминание в тексте рассматриваемого закона понятия “system of records” – «система записей/файлов», которая определялась как любая совокупность записей/файлов, где информацию об индивиде можно было получить по его имени или индивидуальному идентификатору, что исключало применение закона к базам данных, устроенным по иным принципам доступа, но которые также могли содержать информацию персонального характера.

В Акте прямо была закреплена обязанность федеральных агентств ежегодно публиковать сведения о своих базах данных в Федеральном регистре. В рамках такой публикации в обязательном порядке было необходимо указать цель использования базы данных и порядок обращения в агентство заинтересованных лиц в целях предоставления письменных данных, заключений или обоснований. Кроме этого, любые значительные изменения в порядке ведения базы данных должны быть заблаговременно

рассмотрены Комитетом по государственным операциям Палаты представителей, Комитетом по государственным делам Сената, а также Кабинетом по управлению и бюджету, которые проводят оценку с точки зрения возможного или предполагаемого ущерба правам индивида предлагаемых изменений.

Права субъекта данных (любого физического лица) предусматривали право на доступ к информации о нем. Субъекту при этом предоставляется право знакомиться и делать копии информации о себе, а также требовать внесения изменений в случае неточности или ошибок.

Основное требование к операторам данных (федеральных агентств) на основании Акта можно изложить как запрет их раскрытия (disclosure) – передачи третьим лицам или неопределенному кругу лиц, т.е. сохранения их конфиденциальности, за исключением прямо предусмотренных 12 случаев-условий, к которым подразделом b было отнесено:

1) раскрытие данных служащему агентства, который ведет их обработку и которые ему необходимы для реализации его должностных обязанностей;

2) раскрытие в соответствии с требованиями Акта о свободе информации (Freedom Information Act[1]);

3) раскрытие в соответствии с «обычной практикой» (routine use);

4) раскрытие для Бюро переписи населения США (US Census Bureau[2]) для осуществления переписи населения;

5) раскрытие по заранее полученному запросу в целях статистических исследований, при условии передачи обезличенных данных (без идентифицирующей личность информации);

6) передача записей (данных) в администрации национальных архивов и записей в качестве записи/файла, имеющей историческую ценность;

[1] The Freedom of Information Act (FOIA) (5 U.S.C. § 552). – (https://www.gpo.gov/fdsys/pkg/STATUTE-80/pdf/STATUTE-80-Pg250.pdf). – Дата обращения 20.05.2017.
[2] US Census Bureau. – (https://www.census.gov/).

7) передача записей в целях осуществления уголовного и гражданского правосудия;

8) раскрытие в целях защиты жизни и здоровья лица, при условии сообщения ему о факте раскрытия его данных;

9) раскрытие информации Конгрессу или его комитетам, подкомитетам;

10) раскрытие Генеральному аудитору (Comptroller General[1]) для осуществления деятельности Генерального счетного комитета (the General Accounting Office);

11) раскрытие на основании решения суда (судебного приказа);

12) раскрытие информации о потребителе в соответствии с требованием специального закона.

При раскрытии персональной информации агентства должны вести ее учет, т.е. хранить в течение не менее 5 лет информацию: о времени запроса; субъекте, который ее запросил, включая его контактную информацию; описание переданной информации. Субъект данных вправе ознакомиться с такой учетной записью, за исключением информации по запросам, связанным с осуществлением правосудия.

Качество и объем информации, содержащейся у агентства (оператора), регулировались путем установления принципов достоверности информации, а также принципа минимального объема информации, который необходим для реализации законной деятельности агентства, т.е. только необходимая и относящаяся к делу информация (relevant and necessary). Сверх этого было разрешено осуществлять сбор информации только в том случае, если недостаточность информации может негативно отразиться для индивида (по ограничению прав, интересов, преимуществ). В таких случаях агентства вправе собирать всю доступную информацию непосредственно от индивида. Положения Акта также предусматривали возможность сопоставления,

[1] The Comptroller General of the United States. – (http://www.gao.gov/cghome/index.html). – Дата обращения 20.05.2017.

объединения данных агентствами при условии письменного соглашения, которое должно быть сообщено Комитету по государственным делам Сената и Комитету по государственным операциям Палаты представителей, а также находиться в публичном доступе. В соглашении в обязательном порядке предусматриваются: цель и орган, который будет ответственен за объединение данных; ожидаемые результаты и обоснование необходимости объединения баз данных; описание данных, которые будут объединяться. В каждом агентстве, которое собирается участвовать в программе сопоставления и объединения данных, Акт требовал создания специального органа (Data Integrity Board), который бы следил за исполнением соглашений об обмене и сопоставлении данных, их соответствием законодательству.

Для защиты прав индивида Актом установлена гражданская и уголовная ответственность за нарушения отдельных его положений. В частности, гражданская ответственность предусмотрена за необоснованный отказ индивиду в доступе к файлу/записи или во внесении в него изменений и в некоторых иных случаях. Уголовная ответственность предусмотрена за умышленные: раскрытие персональной информации, несообщение о создании баз данных с персональной информацией, необоснованный запрос персональной информации по ложному основанию и т.д.

Как видно из анализа рассматриваемого документа, становится очевидным, что он распространяется на достаточно узкий круг отношений, связанных с обработкой персональной информации, к тому же содержит некоторые положения, которые не всегда гарантируют адекватную защиту прав индивида. В частности, вызывает опасения применение Акта исключительно к базам данных, организованным по имени индивида, особому номеру, фотографии, что на момент его принятия в 1974 году могло гарантировать адекватную защиту. Тогда как сейчас, в условиях формирования информационных систем с самыми различными вариантами их организации и поиска в них персональной информации, такое положение

можно охарактеризовать как не совсем удачное и ограничивающее сферу его действия.

По мнению части авторов[1], особую озабоченность вызывает присутствие в числе исключений возможности раскрытия данных в рамках «обычной практики» (routine use disclosure), которая часто очень широко трактуется правительственными агентствами. Сам Акт определяет это как возможность раскрытия данных в целях, сопоставимых/схожих с целями, определенными при их сборе. Такое положение дел ведет к указанию федеральными агентствами самых общих целей при сборе информации о гражданах и оставляет им значительное пространство для возможных злоупотреблений.

На основании изложенного нетрудно сделать вывод о том, что Прайваси Акт регулирует только отношения по обработке данных правительственными агентствами, т.е. органами государственной власти, однако это не означает, что в США отсутствуют нормы, которые регулируют вопросы защиты прав индивида при обработке его данных в частном секторе экономики. В этом заключается еще одно существенное отличие американского подхода к регулированию обработки персональных данных.

Все дело в том, что в остальных случаях в США доминирует так называемый отраслевой подход к правовому регулированию обработки данных, а некоторые авторы даже называют его скорее практикой ad hoc[2]. Не случайно, что в своем отчете о принятых мерах на национальном уровне в рамках ОЭСР Соединенные Штаты заявили сразу четыре органа, уполномоченных в сфере контроля реализации законодательства о защите данных:

– Департамент юстиции – в сфере осуществления правосудия;

---

[1] Коровяковский, Д.Г. Российский и зарубежный опыт в области защиты персональных данных / Д.Г. Коровяковский // Национальные интересы: приоритеты и безопасность. – 2009. – № 5. – С. 49–50.

[2] Reidenberg, J.R. Privacy Protection and the Interdependence of Law Technology and Self-Regulation / J.R. Reidenberg // Variations sur le Droit de la Société de l'Information. – Bruxelles: Bruylant, 2001. – C. 128.

– Департамент здравоохранения и социальной защиты – в сфере здравоохранения и социальной защиты;
– Федеральное банковское агентство – в банковской и финансовой сфере;
– Федеральная торговая комиссия – в сфере торговли.

При этом такой перечень нельзя назвать исчерпывающим, учитывая, что существует специальное регулирование для некоторых других отраслей, равно как и наличие в каждом таком случае специально уполномоченного органа по контролю, а равно учитывая, что штаты также вправе принимать собственные законы о защите данных и учреждать контролирующие органы[1].

Особым образом законодательство и практика в США подходит в целом к регулированию обработки персональных данных в частном секторе, рассматривая в основном ее с позиции защиты конкуренции и прав потребителей, неслучайно употребляя вместо термина «субъект персональных данных» или «индивид», понятие «потребитель» (consumer). В качестве примера можно привести Акт о прайваси в финансовой сфере (The Right to Financial Privacy Act 1978[2]) и Акт о защите прайваси в электронных коммуникациях (The Electronic Communication Privacy Act 1986[3]), где намеренно используется именно указанный термин применительно к обозначению индивидов, и это не является исключением[4].

В целом американское законодательство в области защиты прав потребителей при обработке их персональной информации достаточно избирательно.

---

[1] Report on the Cross-Boarder Enforcement of the Privacy Laws / OECD. – 2006. – P. 13–14.
[2] The Right to Financial Privacy Act of 1978 (RFPA; codified at 12 U.S.C. ch. 35, § 3401 et seq.). – (https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg3641.pdf). – Дата обращения 20.05.2017.
[3] The Electronic Communications Privacy Act of 1986 (ECPA) (18 U.S.C. § 2510 et seq.). – (https://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf). – Дата обращения 20.05.2017.
[4] Автор намеренно использует термин «прайваси» в обоих случаях, так как само содержание указанных актов не позволяет использование другого термина, поскольку названные документы в большей степени посвящены ограничению вмешательства государства в указанные сферы, нежели обеспечению неприкосновенности частной жизни в целом.

В качестве наиболее «урегулированных сфер» можно назвать: финансовую сферу[1], медицинские услуги[2], услуги по кредитованию[3], услуги видеопроката[4], кабельное телевидение[5], «онлайн» деятельность детей до 13 лет[6], образовательные услуги[7], регистрация транспортных средств[8], телемаркетинг[9].

Значительную роль в регулировании вопросов защиты частной жизни в США, включая защиту персональных данных, играют решения Верховного суда, основанные на толковании 4-й поправки Конституции. Такие решения принимаются достаточно часто и, как правило, носят казуальный характер. В частности, Верховный суд рассматривал вопрос о данных владельцев транспортных средств, признав их коммерческий характер и возможность регулировать их обработку федеральным правительством[10]. В 2001 году Верховный суд признал отсутствие нарушений Акта о семейных образовательных правах и частной жизни и 4-й поправки Конституции в случае выставления рейтинга учащихся и его оглашения вслух[11].

Многие вопросы в области регулирования обработки данных разрешаются на основе саморегулирования, т.е. на основе внутренних

---

[1] The Right to Financial Privacy Act of 1978 (RFPA; codified at 12 U.S.C. ch. 35, § 3401 et seq.). – (https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg3641.pdf). – Дата обращения 20.05.2017.

[2] The Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104–191). – (https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm). – Дата обращения 20.05.2017.

[3] The Fair Credit Reporting Act of 1970 (Pub. L. No. No. 91-508 (1970)). – (https://www.gpo.gov/fdsys/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf). – Дата обращения 20.05.2017.

[4] The Video Privacy Protection Act (Pub. L. No. 100-618 (1988)). – (https://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg3195.pdf). – (дата обращения 20.05.2017).

[5] The Cable Communications Policy Act of 1984 (Pub. L. No. 98-549 (1984)). – (https://www.gpo.gov/fdsys/pkg/STATUTE-98/pdf/STATUTE-98-Pg2779.pdf). – Дата обращения 20.05.2017.

[6] The Children's Online Privacy Protection Act of 1998 (COPPA) (Pub. L. No. 105-277 (1998)). – (https://www.gpo.gov/fdsys/pkg/PLAW-105publ277/html/PLAW-105publ277.htm). – Дата обращения 20.05.2017.

[7] The Family Educational Rights and Privacy Act of 1974 (FERPA or the Buckley Amendment) (Pub. L. No. 93-380 (1974)). – (http://www.legisworks.org/GPO/STATUTE-88-Pg484.pdf). – Дата обращения 20.05.2017.

[8] The Driver's Privacy Protection Act of 1994 (Pub. L. No. 103-322 (1994)). – (https://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap123-sec2721.pdf). – Дата обращения 20.05.2017.

[9] The Telephone Consumer Protection Act of 1991 (Pub. L. No. 102-243 (1991)). – (https://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapII-partI-sec227.pdf). – Дата обращения 20.05.2017.

[10] Reno v. Condon, 528 U.S. 141 (2000). – (https://supreme.justia.com/cases/federal/us/528/141/case.html). – Дата обращения 20.05.2017.

[11] Owasso Independent School District v. Falvo, 534 U.S. 426 (2001). – (https://supreme.justia.com/cases/federal/us/534/426/case.html). – Дата обращения 20.05.2017.).

корпоративных норм и рыночной целесообразности[1], что существенным образом сказывается на уровне защиты данных и сохранения их конфиденциальности и приводит к существованию своего рода рынка данных об индивиде, о котором он может и не знать. В качестве одного из ярких примеров можно назвать наличие самостоятельного и весьма прибыльного рынка информации о гражданах-потребителях, о чем можно судить на основании ставшего широко известным дела Lotus, когда информация (CD-диск) об образе жизни около 20 миллионов американских семей стала предметом продажи и распространения и была впоследствии изъята из оборота под давлением потребителей[2].

Подводя итог анализу зарубежной и международной практики, можно условно выделить два основных подхода (модели) правового регулирования персональных данных – *европейский* и *американский*.

Основными и наиболее характерными чертами первой модели следует признать:

1) признание за индивидом неотъемлемого права контролировать обработку информации о себе, как части «информационной самоидентификации» личности в демократическом обществе;

2) наличие специального закона, устанавливающего общие требования к обработке персональных данных в частной и публичной сфере, т.е. установление общего режима конфиденциальности, заключающегося в особом режиме доступа к ним и их распространения, преимущественно с согласия индивида;

3) наличие единого, независимого уполномоченного органа по контролю над соблюдением законодательства о персональных данных (специальная комиссия или омбудсмен), который полномочен самостоятельно рассматривать жалобы граждан;

---

[1] Reidenberg, J.R. Privacy Protection and the Interdependence of Law Technology and Self-Regulation / J.R. Reidenberg // Variations sur le Droit de la Société de l'Information. – Bruxelles: Bruylant, 2001. – P. 131.

[2] Cadoux, L. La Vie Privée: un Avenir sous Haute Surveillance / L. Cadoux // Liberté d'Expression et Nouvelles Technologies. – Paris: IQ Collectif, 1998. – P. 121

4) использование механизмов саморегулирования в частной сфере в качестве дополнительного (субсидиарного).

В качестве несомненных положительных черт такого подхода следует признать ориентацию на приоритет прав личности, признание защиты персональных данных в качестве одной из сторон прав и свобод человека, в связи с чем он более ориентирован на государственное регулирование обработки персональных данных, независимо от сферы ее осуществления и установление гарантий прав субъекта.

Отрицательными чертами в таком случае стоит признать тот факт, что часто гармонизация законодательства о персональных данных оставляет существенное «поле для маневра» для государств-участников ЕС, что иногда приводит к существенным расхождениям в его содержании.

Для *американского* похода, напротив, характерно:

1) использование категории «прайваси» для частной и публичной сферы для ограничения вмешательства государства и его органов в частную жизнь индивида;

2) отраслевой подход к правовому регулированию вопросов защиты данных о физических лицах, где наиболее урегулированной сферой на уровне законодательства является «публичная сфера (сфера государственного управления)» и отсутствует единый документ, устанавливающего единые принципы защиты данных для частной и публичной сфер экономики;

3) преобладание в частном секторе (в экономике) рыночных механизмов регулирования в вопросах защиты прав индивида, а также рассмотрение в целом проблемы регулирования обработки данных частными компаниями с позиций «добросовестной конкуренции» и «защиты прав потребителя»;

4) отсутствие единого уполномоченного органа по контролю за соблюдением законодательства в сфере персональных данных и

распределение этих функций между различными органами, в соответствии с их компетенцией и отраслевой направленностью.

Существенный недостаток данного подхода во многом очевиден – это ориентация на рыночные механизмы регулирование в частной сфере, что не лучшим образом гарантирует защиту прав субъекта данных, поскольку, вне всякого сомнения, в случае противоречий индивиду будет гораздо сложнее противостоять частным компаниям, а также требовать от них информирования об использовании данных о себе в отсутствие законодательно закрепленной обязанности. К примеру, деятельности специализированных агентств, предоставляющих информацию о кредитных историях, урегулирована, тогда как компании, занимающиеся адресным (прямым) маркетингом, не связаны в аналогичном случае какими-либо правилами. Положительной чертой в этом походе является как раз «специальный», или даже в некоторой степени «адресный», подход к регулированию защиты прав субъекта, учитывающий специфику той или иной отрасли экономики, государственного управления, в том числе и при установлении средств судебной защиты, поскольку в каждом случае обычно упоминается размер или порядок определения размера возмещения в гражданском судопроизводстве и размеры уголовного наказания за возможные нарушения.

Говоря о распространенности названных выше подходов среди государств мира, можно сказать, что *европейский* получил более широкое распространение и в настоящий момент это порядка 50 государств Совета Европы, расположенных на европейском континенте, а также Канада, Аргентина, Австралия, Новая Зеландия, Южная Корея, Буркина Фасо.

Американский подход менее распространен и помимо самих Соединенных Штатов Америки аналогичным образом «отраслевое»

регулирование обработки персональных данных характерно для Японии, Парагвая, Тайваня, Тайланда[1].

[1] Параскевов, А.В. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом / А.В. Параскевов, А.В. Левченко, Ю.А. Кухоль // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГУ, 2015. – № 110. – С. 866–894.

3.2. Особенности формирования российского подхода к правовому регулированию персональных данных

В российском праве долгое время вопрос о правовом регулировании персональных данных оставался открытым, прежде всего в плане принятия специального закона в этой области. При этом невозможно говорить о том, что отдельные аспекты, связанные с обработкой персональных данных, не были урегулированы. На конституционном уровне следует упомянуть статьи 23 и 24 Конституции РФ 1993 года, устанавливающие право индивида на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых телеграфных и иных сообщений, а также право индивида и на доступ к информации о себе и обязанность государственных органов и органов местного самоуправления обеспечить ему возможность последнего. Вне всякого сомнения, эти статьи, несмотря на то что в них содержатся лишь отдельные аспекты правового регулирования обработки данных о физических лицах, послужили своего рода отправной точкой для дальнейшего формирования законодательства о защите частной жизни при обработке персональных данных.

Впервые термин «персональные данные» (информация о гражданах) был введен в законодательство с принятием Федерального закона «Об информации, информатизации и о защите информации»[1] в 1995 году, где в статье 2 содержалось уже рассмотренное автором определение их как «сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность». Однако детального регулирования обработки данных в указанном законе, по понятным причинам, не содержалось, но предлагалась его общая концепция, а также содержалась отсылка к специальному законодательству, которое, как, по-видимому, предполагалось, должно быть принято. На основании анализа

[1] Об информации, информатизации и защите информации: федер. закон от 20.02.1995 № 24-ФЗ. (Утратил силу.)

статьи 9 и 14, принципиально можно было прийти к следующим основным выводам о концептуальных положениях предполагаемого тогда специального закона:

- персональные данные являются информацией ограниченного доступа и относятся к конфиденциальной информации[1];
- перечень персональных данных должен быть установлен федеральным законом;
- персональные данные напрямую связаны с защитой права на неприкосновенность частной жизни, личную и семейную тайну и права на тайну переписки, телефонных переговоров, телеграфных и иных сообщений;
- сбор, хранение, использование и распространение персональных данных допускается лишь с согласия индивида или по решению суда;
- персональные данные не могут быть использованы для причинения имущественного и морального вреда индивиду;
- персональные данные о расовой, национальной, языковой, религиозной и партийной принадлежности не могут быть использованы для дискриминации (ограничения прав) физических лиц;
- ответственность за нарушения порядка сбора, хранения, использования и распространения персональных данных несут владельцы информационных ресурсов, их содержащих;
- субъект персональных данных (индивид) вправе знакомиться с содержанием персональных данных (иметь доступ к ним), требовать их уточнения, а также вправе знать, кто и в каких целях их использует, за исключением случаев, предусмотренных законом;

[1] В соответствии с положениями рассматриваемого закона информация ограниченного доступа подразделялась на две основные категории – государственная тайна и конфиденциальная информация.

– обязанность предоставить возможность ознакомления со своими персональными данными возлагается на владельца информационных ресурсов, отказ которого может быть обжалован в суд.

Основанному на указанных принципах федеральному закону так и не суждено было появиться, а от некоторых из перечисленных выше положений пришлось отказаться. В частности, были подвергнуты критике: ориентированность закона в первую очередь на граждан; установление в качестве основного критерия для выделения персональных данных лишь «идентификации»; стремление установить закрытый перечень категорий информации, относимой к персональным данным, что уже было подробно рассмотрено автором в первой главе работы.

За период с 1995 по 1998 год было подготовлено 12 редакций законопроекта, в которых осуществлялся учет замечаний и предложений рецензентов. Проект дважды обсуждался на секции Научно-технического совета Комитета при Президенте РФ по политике информатизации. Дважды проект прошел международную экспертизу специалистами Совета Европы. Обсуждался проект также на общественных слушаниях в Парламентском центре Федерального собрания РФ, в российско-американском пресс-центре с участием представителей средств массовой информации, на семинаре по проблемам информационной безопасности в рамках Международного конгресса «Народы Содружества Независимых Государств накануне третьего тысячелетия» в Санкт-Петербурге, на «круглом столе», проводимом отделением «Информатика и право» Международной академии информатизации, и др.[1]

Окончательным итогом этой работы стало появление проекта федерального закона «Об информации персонального характера», внесенного для рассмотрения в Государственную думу 3 апреля 1998 года группой

[1] Пояснительная записка к проекту федерального закона «Об информации персонального характера» (Законопроект № 98028850-2, внесен в Государственную думу 03.04.1998). – (http://asozd2.duma.gov.ru /main.nsf/%28SpravkaNew%29?OpenAgent&RN=98028850-2&02). – Дата обращения 20.05.2017.

депутатов – О.А. Финько, Ю.М. Нестеровым, Г.К. Волковым, Р.Г. Габидуллиным, В.Е. Цоем[1], но так и не был принят. Проект закона был разработан на основе и в соответствии с нормами Директивы 95/46/ЕС Европейского парламента и Совета Европы. Он содержал шесть глав (общие положения; условия законности работы с персональными данными; права субъекта персональных данных; права и обязанности держателя (обладателя) по работе с массивами персональных данных; государственное регулирование работы с персональными данными; Уполномоченный по правам субъектов персональных данных при Президенте РФ), тридцать шесть статей.

Само название выбивалось уже тогда из общепринятой терминологии, поскольку уже названный закон «Об информации, информатизации и защите информации» содержал в качестве базового термина «персональные данные», который также был использован Указом Президента РФ № 188 «Об утверждении перечня сведений конфиденциального характера»[2]. В итоге в основу законопроекта был положен механизм обработки персональных данных, соответствующий общепринятым европейским принципам и нормам в области защиты персональных данных[3].

Одной из особенностей законопроекта была попытка предложить перечень случаев законного сбора, обработки и использования персональных данных, который диктовался, по мнению авторов, необходимостью обеспечить эффективную защиту прав личности в отношении его персональных данных. Персональные данные, получаемые в результате деятельности субъектов федерального закона «Об оперативно-розыскной деятельности», на основании статьи 10 были выделены фактически в особую

---

[1]Законопроект № 98028850-2 «Об информации персонального характера» (внесен в Государственную думу 03.04.2017). – (http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=98028850-2&02). – Дата обращения 20.05.2017.

[2] Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера» от 06.03.1997 № 188 (ред. от 13.07.2015).

[3] Законопроект «Об информации персонального характера» № 17844-3. Внесен депутатами Государственной думы ФС РФ А.А. Кравцом, О.А. Финько, Ф.А. Клинцевичем, И.В. Лебедевым, Б.А. Мартыновым, А.В. Шубиным, К.В. Ветровым, П.И. Коваленко // Справочная информационная система «КонсультантПлюс». – Ст. 4.

категорию наряду с традиционно выделяемой категорией «чувствительных данных». Но все же важнейшей новеллой законопроекта стала попытка введения института Уполномоченного по правам субъектов персональных данных. Для обеспечения действенности этого правового института предполагалось гарантировать независимость его деятельности. В законопроекте избран путь формирования названного института при Президенте РФ[1].

В целом данный законопроект был вполне доброжелательно встречен и в научных кругах, в частности за его принятие высказывались О.Б. Просветова[2] и В.Н. Лопатин[3], хотя при условии определенной доработки в дальнейшем. Несмотря на очевидную актуальность законопроекта в целях защиты прав и свобод граждан, законопроект фактически лег «на полку», поскольку процесс рассмотрения в Федеральном собрании фактически остановился его обсуждением на Совете Государственной думы[4], который впоследствии принял окончательное решение о его снятии уже только после того, как началась работа над новым проектом специального закона в 2006 году[5], отложив тем самым принятие законодательных мер в рассматриваемой области еще на 6 лет.

Стоит отметить, что примерно в этот период параллельно Межпарламентской ассамблеей государств-участников СНГ принимается модельный закон «О персональных данных», разработчиками которого стали В.Н. Лопатин и А.В. Федоров[6], существенным образом похожий отдельными положениями и общей концепцией на уже упомянутый законопроект «Об

---

[1] Законопроект «Об информации персонального характера» № 17844-3. Внесен депутатами Государственной думы ФС РФ А.А. Кравцом, О.А. Финько, Ф.А. Клинцевичем, И.В. Лебедевым, Б.А. Мартыновым, А.В. Шубиным, К.В. Ветровым, П.И. Коваленко // Справочная информационная система «КонсультантПлюс». – Гл. 6.

[2] Просветова, О.Б. Защита персональных данных: дис. … канд. юрид. наук / О.Б. Просветова. – М., 2005. – С. 94.

[3] Лопатин, В.Н. Правовые основы информационной безопасности: курс лекций / В.Н. Лопатин. – М.: МИФИ, 2000. – С. 88.

[4] Рассмотрен 24.10.2000 Советом ГД ФС РФ (Протокол № 49, п. 66).

[5] Снят 09.02.2006 с рассмотрения Советом ГД ФС РФ (Протокол № 138, п. 19).

[6] Лопатин, В.Н. Модельный закон «О персональных данных» для государств-участников СНГ / В.Н. Лопатин, А.В. Федоров // Сб. мат-лов междунар. науч.-практич. конф. 29 ноября 1998 г. «Новые технологии в практике правоохранительных органов». – СПб., 1998. – С. 61–73.

информации персонального характера». Впрочем, его принятие никоим образом не ускорило принятие российского закона.

Существенные изменения в отношении к рассматриваемой проблематике со стороны российского законодателя произошли, пожалуй, после активизации отношений между Россией, Советом Европы и Европейским союзом. Первым шагом к этому стало подписание 7 ноября 2001 года Российской Федерацией уже не раз упоминавшейся здесь Конвенции Совета Европы № 108 о защите личности в связи с автоматизированной обработкой данных[1]. Примечательно, что ее ратификация, которая потребовала от России имплементации и принятия специального закона о защите персональных данных, состоялась лишь спустя 5 лет. Проект нового федерального закона «О персональных данных» уже рассматривался практически параллельно с проектом закона о ратификации названной Конвенции Совета Европы[2].

Новый проект закона о персональных данных был подготовлен Правительством РФ и в сентябре 2005 года поступил в Государственную думу[3]. Первоначально в нем содержался ряд положений, которые вызвали множество критики, в первую очередь со стороны правозащитников. Это касалось положений статьи 24 варианта законопроекта по итогам первого чтения. В ней, в частности, предлагалась к созданию единая база персональных данных о населении России – «Государственный регистр населения Российской Федерации», куда подлежали занесению идентификаторы персональных данных всех физических лиц, постоянно или временно проживающих или пребывающих на территории России. В качестве «идентификаторов персональных данных» при анализе статьи 23

---

[1] Chart of signatures and ratifications of Treaty 108 «Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data» (Status as of 20/05/2017). – (http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=I4WkWbbB). – Дата обращения 20.05.2017.

[2] ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» № 160-ФЗ от 19.12.2005 // Справочная информационная система «КонсультантПлюс».

[3] Законопроект № 217352-4 «О персональных данных» (внесен в Государственную думу РФ 23.09.2005). – (http://asozd2.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=217352-4). – Дата обращения 20.05.2017.

того же варианта законопроекта подразумевались различного рода персональные номера, которые используются в информационных системах государственными и местными органами для удобства обработки данных о физических лицах. Такими идентификаторами, безусловно, являются индивидуальный номер налогоплательщика (ИНН), предусмотренный ст. 84 Налогового кодекса РФ[1], и страховой номер индивидуального лицевого счета в системе обязательного пенсионного страхования в соответствии со ст. 7 ч. 1 федерального закона «Об обязательном (персонифицированном) учете в системе обязательного пенсионного страхования»[2], номер полиса обязательного медицинского страхования. Создание такого «Государственного регистра населения РФ» правительство объясняло необходимостью их уточнения, отмечая, что в нем будут содержаться лишь общедоступные персональные данные, а также персональные идентификаторы, например ИНН, которые с точки зрения закона не являются информацией ограниченного доступа[3]. Однако отстоять целесообразность существования такой единой базы данных правительству не удалось. Уже на стадии обсуждения в комитетах Государственной думы против этого были выдвинуты, в качестве серьезных, следующие аргументы: во-первых, оператор потенциально получал в таком случае доступ к информации, превышающий его полномочия; во-вторых, учитывая сложности с охраной конфиденциальной информации в России в целом, существование подобного регистра создало бы серьезную угрозу несанкционированного доступа к самым разнообразным сведениям о субъекте; в-третьих, появление регистра могло вызвать серьезное недоверие со стороны населения и повысить социальную напряженность. Таким образом, предлагаемая концепция государственного регистра населения представлялась создающей условия для

[1] Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 №146-ФЗ (ред. от 28.12.2016).
[2] Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования: федер. закон от 01.04.1996 № 27-ФЗ (ред. от 28.12.2016).
[3] Текст законопроекта № 217352-4 «О персональных данных» к первому чтению (внесен в Государственную думу РФ 23.09.2005). – (http://asozd2.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=217352-4). – Дата обращения 20.05.2017.

необоснованного ограничения и прямого нарушения прав граждан, что противоречит целому ряду положений Конституции Российской Федерации (статья 23, части 1 и 2; статья 24, часть 1; статья 55, части 2 и 3), что и послужило ее изъятию из текста законопроекта после второго чтения.

В дальнейшем сколь-нибудь серьезные изменения в документ не вносились, и законопроект успешно прошел все стадии и был опубликован 29 июля в «Российской газете»[1], став федеральным законом.

Оценивая текст законопроекта в целом, следует отметить его явную близость «европейской традиции», поскольку многие его правовые конструкции явным образом ориентированы на Конвенцию № 108 Совета Европы и с Директивой 95/46/CE. Причем начальные положения по своей конструкции и содержанию столь очевидно напоминают положения последней, что не могут не вызывать ассоциации об аналогии. В таком положении дел не стоит усматривать чего-то негативного, скорее наоборот, многими российскими авторами, уже неоднократно упомянутыми в работе, именно «европейская модель» правового регулирования оборота персональных данных рассматривалась в качестве основы для разработки закона. К тому же предшествующий законопроект «Об информации персонального характера» также был ориентирован на законодательную практику стран Европейского союза. Проводя аналогии к, безусловно, сильным сторонам принятого федерального закона «О персональных данных» можно отнести проработанность правовых конструкций, в части описания собственно правового режима обработки персональных данных, как информации персонального характера, в плане определения принципов и условий обработки, прав субъектов персональных данных, обязанностей обладателя и оператора систем персональных данных. Однако явным минусом, безусловно, явился отказ от института независимого уполномоченного органа по защите прав субъектов персональных данных – Уполномоченного по правам субъекта данных.

[1] Российская газета. Федеральный выпуск. – 2006. – № 4131 (0). – 29 июля.

Законодательная деятельность в области правового регулирования персональных данных, разумеется, не сосредоточилась только на принятии специального закона. В период с 1995 года по настоящий момент был принят целый ряд законодательных положений отраслевого характера, которые регулировали обработку баз персональных данных в конкретных областях общественной деятельности и для которых новый закон стал своего рода связующим звеном. Такие положения, упоминающие о базах персональных данных, содержатся: в Трудовом кодексе[1], в главе 14 «Защита персональных данных работника»; в ст. 84 Налогового кодекса РФ[2]; в ст. 85.1 Воздушного кодекса РФ[3]; в федеральных законах: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»[4], «О банках и банковской деятельности»[5], «О связи»[6], «О правовом положении иностранных граждан в РФ»[7], «О государственной автоматизированной системе ГАС «Выборы»[8], «О государственном банке о детях оставшихся без попечения родителей»[9], «Об актах гражданского состояния»[10], «Об обязательном страховании гражданской ответственности владельцев транспортных средств»[11], «О воинской обязанности и военной службе»[12], «О системе государственной гражданской службы РФ»[13] и многих других.

---

[1] Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 01.05.2017).
[2] Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ (ред. от 28.12.2016).
[3] Воздушный кодекс Российской Федерации от 19.03.1997 № 60-ФЗ (ред. от 06.07.2016).
[4] Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования: федер. закон от 01.04.1996 № 27-ФЗ (ред. от 28.12.2016).
[5] О банках и банковской деятельности: федер. закон от 02.12.1990 № 395-1 (ред. от 01.05.2017) (с изм. и доп., вступ. в силу с 16.06.2017).
[6] О связи: федер. закон от 07.07.2003 № 126-ФЗ (ред. от 17.04.2017).
[7] О правовом положении иностранных граждан в Российской Федерации: федер. закон от 25.07.2002 № 115-ФЗ (ред. от 17.04.2017).
[8] О Государственной автоматизированной системе Российской Федерации «Выборы: федер. закон от 10.01.2003 № 20-ФЗ (ред. от 12.03.2014).
[9] О государственном банке данных о детях, оставшихся без попечения родителей: федер. закон от 16.04.2001 № 44-ФЗ (ред. от 08.03.2015).
[10] Об актах гражданского состояния: федер. закон от 15.11.1997 № 143-ФЗ (ред. от 01.05.2017).
[11] Об обязательном страховании гражданской ответственности владельцев транспортных средств: федер. закон от 25.04.2002 № 40-ФЗ (ред. от 28.03.2017).
[12] О воинской обязанности и военной службе: федер. закон от 28.03.1998 № 53-ФЗ (ред. от 01.05.2017).
[13] О системе государственной службы Российской Федерации: федер. закон от 27.05.2003 № 58-ФЗ (ред. от 23.05.2016).

За последние несколько лет можно говорить и том, что концепция «защиты персональных данных», т.е. защиты личности в условиях бурного развития информационных технологий, также меняется и развивается, о чем свидетельствуют многочисленные и достаточно существенные изменения в законодательстве о персональных данных как в России, так и в мире.

В частности, российский закон о персональных данных претерпел за последние 10 лет значительные изменения. Даже простое арифметическое сравнение объема и содержания закона на момент его принятия (примерно 5500 слов и 41000 знаков) и действующей редакции (примерно 9900 слов и 72000 знаков) говорит о том, что закон «потяжелел» почти вдвое. Если первые 5 лет текст закона практически не менялся, в том числе и благодаря тому, что его вступление в силу откладывалось, сначала в декабре 2010 года[1], а затем в какой-то степени в июле 2011 года[2]. Во многом это объяснялось «неготовностью» экономики, т.е. операторов персональных данных к реализации требований нового на тот момент законодательства, отдельные положения которого в то время не раз подвергались резкой критике со стороны бизнес-сообщества и научной общественности. Многие из этих проблем были предметом обсуждений в ходе Парламентских слушаний[3] Комитета по безопасности Государственной думы РФ еще в октябре 2009 года.

Результатом этой работы стала первая существенная переработка положений закона о персональных данных в июле 2011 года, когда серьезным образом были переработаны более 10 статей закона и появились еще две новые (ст. 18.1 и 22.1)[4]. В наибольшей степени эти изменения коснулись самого механизма закона в части установления обязанностей

[1] О внесении изменения в статью 25 Федерального закона «О персональных данных»: федер. закон от 23.12.2010 № 359-ФЗ.
[2] О внесении изменений в Федеральный закон «О персональных данных»: федер. закон от 25.07.2011 № 261-ФЗ.
[3] Парламентские слушания на тему: «Актуальные вопросы развития и применения законодательства о защите прав граждан при обработке персональных данных» 20 октября 2009 г. / Сайт Комитета по безопасности Государственной думы РФ. – (http://komitet2-16.km.duma.gov.ru/Novosti_Komiteta/item/24812). – Дата обращения 20.05.2017.
[4] О внесении изменений в Федеральный закон «О персональных данных»: федер. закон от 25.07.2011 № 261-ФЗ.

оператора по обеспечению защиты персональных данных от любых неправомерных действий с ними, и прежде всего – в части принятия правовых, организационных и технических мер по защите информации (персональных данных). Указанные положения в совокупности с рядом уже упомянутых в работе подзаконных актов внесли ощутимую ясность в определение режимных требований к операторам при обеспечении конфиденциальности персональных данных.

В дальнейшем целый ряд изменений закона о персональных данных был связан с его фактической «подстройкой» под существующие реалии при обработке персональных данных в государственных органах и публичных целях. Как оказалось, законодательство о персональных данных было принято без учета существующей практики и особенностей обработки персональных данных сразу в нескольких сферах, таких как: жилищно-коммунальное хозяйство[1], деятельность органов прокуратуры[2], потребительское кредитование[3], при решении вопросов о гражданстве[4].

Среди последних и наиболее обсуждаемых изменений в законодательстве о персональных данных можно назвать:

- изменения в ст. 18 закона, устанавливающие правило о локализации на территории РФ хранения и отдельных процессов обработки персональных данных о гражданах РФ[5];
- принятие законодательных положений о «праве на забвение», т.е. устанавливающих право индивида требовать удаления

[1] О внесении изменений в Жилищный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»: федер. закон от 04.06.2011 № 123-ФЗ (ред. от 21.07.2014).

[2] О внесении изменений в отдельные законодательные акты Российской Федерации в связи с уточнением полномочий органов прокуратуры Российской Федерации по вопросам обработки персональных данных»: федер. закон от 23.07.2013 № 205-ФЗ.

[3] О внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации в связи с принятием Федерального закона «О потребительском кредите (займе)»: федер. закон от 21.12.2013 № 363-ФЗ.

[4] О внесении изменений в статьи 6 и 30 Федерального закона «О гражданстве Российской Федерации» и отдельные законодательные акты Российской Федерации»: федер. закон от 04.06.2014 № 142-ФЗ (ред. от 03.07.2016).

[5] О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях: федер. закон от 21.07.2014 № 242-ФЗ (ред. от 31.12.2014).

несоответствующей действительности информации о нем из результатов поиска в сети Интернет[1];

– принятие новой редакции статьи 13.11 КоАП РФ, предусматривающей усиление административной ответственности в области нарушения законодательства о персональных данных, как в части увеличения размера штрафа, так и в части увеличения составов правонарушений[2].

Все эти многочисленные изменения демонстрируют дальнейшее развитие идеи защиты персональных данных и были приняты в ответ на текущие угрозы правам и законным интересам физических лиц при обработке персональных данных. В частности, требование локализации баз персональных данных о гражданах РФ и отдельных процессов их обработки было вызвано очевидным стремлением обеспечить защиту данных в условиях, когда с учетом существующих бизнес-моделей компаний, активно предлагающих услуги в сети Интернет, в том числе с помощью облачных сервисов, невозможно однозначно определить, где же в итоге осуществляется обработка данных и под юрисдикцией какого государства? И, что немаловажно, гарантирует ли последнее должный уровень защиты персональных данных?

Во втором случае проблема еще интереснее и глубже. Впервые о праве на забвение было заявлено в деле *Google Spain*[3] в 2014 году. Итогом его рассмотрения стало появление новой нормы, предусматривающей для индивида возможность требовать удаления из результатов поиска поисковой системы Google ссылки на информацию, которую он считает устаревшей или неактуальной. Такое требование Европейский суд ЕС обосновал в

[1] О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»: федер. закон от 13.07.2015 № 264-ФЗ и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации.

[2] О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: федер. закон от 07.02.2017 № 13-ФЗ.

[3] Judgment of the court (Grand Chamber) 13 May 2014. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. – (http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=EN)/ – Дата обращения 20.05.2017.

положениях Директивы № 95/46/ЕС, признав фактически поисковую систему оператором персональных данных и, как следствие, право лица требовать прекращения обработки персональных данных.

Российское законодательство, несмотря на порой резкую критику со стороны интернет-сообщества[1] и некоторых ученых[2], на удивление быстро приняла аналогичные положения, которые вступили в силу с 1 января 2016 года. В 2016 году одна из крупнейших российских интернет-компаний «Яндекс» опубликовала первые результаты применения «закона о праве на забвение», заявив, что только в начале 2016 года поисковая система получила более 3600 обращений, удовлетворив только 27% из них[3]. Компания Google, которая уже давно принимает аналогичные обращения, по состоянию на 2017 год получила уже более 730000 запросов об удалении информации из поиска, дав положительный ответ более чем в 40 случаях[4]. В целом полемика о природе и сущности «права на забвение», его влиянии на развитие Интернета, на обеспечение баланса между правом на уважение частной жизни и свободой выражения мнений еще далека от завершения, о чем свидетельствуют периодически появляющиеся публикации на эту тему[5].

Более того, соответствующие положения о «праве на забвение» были включены в абсолютно новый документ – General Data Protection Regulation (Общие правила регулирования защиты данных; далее – Общие правила)[6], который в самое ближайшее время должен прийти на смену Директиве № 95/46/ЕС.

---

[1] Поисковики отреагировали на законопроект «О праве на забвение» в интернете // Информационный портал «Лента.ру». – (https://lenta.ru/news/2015/05/29/searchanswer/). – Дата обращения 20.05.2017.

[2] Разина, Е. Свобода слова, или право на забвение / Е. Разина // Справочно-правовой портал «Гарант.ру». – (http://www.garant.ru/ia/opinion/author/razina/637159/). – Дата обращения 20.05.2017.

[3] О применении закона «О праве на забвение»// Блог «Яндекса». – (https://yandex.ru/blog/company/o-primenenii-zakona-o-prave-na-zabvenie). – Дата обращения 20.05.2017.

[4] Удаление результатов поиска по личным запросам от граждан ЕС // Поисковая система «Googleh». – (https://www.google.com/transparencyreport/removals/europeprivacy/). – Дата обращения 20.05.2017.

[5] Byrum, K. The European right to be forgotten: A challenge to the United States Constitution's First Amendment and to professional public relations ethics / K. Byrum / Public Relations Review. – 2017. – Vol. 43. – No. 1. – P. 102–111.

[6] General Data Protection Regulation (GDPR) 2012. – (http://ec.europa.eu/transparency/regdoc/rep/1/2012/EN/1-2012-11-EN-F1-1.Pdf). – Дата обращения 20.05.2017.

Появление последних можно назвать одной из самых серьезных и глобальных реформ европейской системы защиты персональных данных с 1995 года. Указанные Общие правила стали итогом длительной подготовки и согласования текста нового «систематизирующего» закона о персональных данных ЕС со странами-участниками. Сам их текст был подготовлен еще в 2011 году и окончательно был принят лишь в апреле 2016 года. В настоящее время идет так называемый переходный период для адаптации и гармонизации текстов национальных законов о персональных данных с окончанием 25 мая 2018 года, когда Общие правила должны вступить в силу.

Причины принятия Общих правил были объяснены и подробно изложены в пояснительной записке[1], предваряющей текст нормативного акта, среди них были названы две основные:

– общее развитие информационного общества, с которым связано появление новых угроз правам индивида при обработке данных;

– «фрагментарность» национального законодательства о персональных данных в странах-участницах ЕС.

Среди наиболее существенных изменений, предлагаемых Общими правилами в сравнении с положениями Директивы 95/46/ЕС, можно назвать:

1) совершенствование понятийного аппарата и появление новых терминов;

2) введение новых принципов при обработке персональных данных – принципа прозрачности и принципа комплексной и адекватной ответственности оператора данных;

3) закрепление права на забвение и права требования прекращения обработки и удаления данных;

4) обязательное назначение ответственных лиц за обработку персональных данных для публичного сектора и крупного бизнеса и т.д.

[1] General Data Protection Regulation (GDPR) 2012. – (http://ec.europa.eu/transparency/regdoc/rep/1/2012/EN/1-2012-11-EN-F1-1.Pdf). – Дата обращения 20.05.2017.

В дополнение к Общим правилам реформа европейской модели защиты персональных данных затронула и сферу правоохранительной деятельности. В общем пакете изменений вместе с Правилами была принята специальная директива, регулирующая вопросы обработки персональных данных органами, компетентными проводить уголовное преследование и расследование, а также осуществлять исполнение уголовных наказаний[1]. Само появление этого документа в некоторой степени является само по себе «новинкой», учитывая, что ранее Директива 95/46/ЕС не распространяла действие своего механизма о защите данных на такой случай, называя его в числе исключений. Теперь же, наоборот, страны Европы получат единый документ, регламентирующий основные положения об обработке данных правоохранительными органами. Сам предлагаемый механизм и его ключевые принципы очень схож с положениями Директивы 95/46/ЕС и Общих правил, но в несколько усеченном виде и скорее направлен на то, чтобы гарантировать соблюдение принципа законности при обработке персональных данных. Среди интересных «новинок» стоит отметить желание разделить персональные данные, обрабатываемые правоохранительными органами, на ряд категорий, исходя из особенностей субъекта, к которому они относятся. В частности, новые положения предписывают национальным правоохранительным органам и странам-участницам делать различие между персональными данными подозреваемых, потерпевших (жертв), обвиняемых и иных участников уголовного процесса, что не лишено смысла и требует дальнейшего изучения и осмысления.

Если говорить о развитии и совершенствовании национального законодательства и практики в области защиты персональных данных в странах Европы, то можно отметить общую тенденцию на активное привлечение к разработке отраслевых норм о защите персональных данных

[1] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. – (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&qid=1497555625791&from=en). – Дата обращения 20.05.2017.

саморегулирующих организаций и объединений предпринимателей для конкретных секторов экономики. Примером этого может служить информация, размещенная на сайте Информационного комиссара Великобритании[1], где приведены подробные инструкции и руководства по организации системы защиты персональных данных в различных секторах экономики, чтобы организация могла грамотно и правильно организовать свои бизнес-процессы в соответствии с европейскими и национальными нормами о защите данных. Аналогичные разделы сайта и направления деятельности есть у многих уполномоченных органов по защите прав субъектов персональных данных в европейских странах: Комиссия по защите частной жизни Бельгии[2], Национальная комиссия по информатике и свободам во Франции[3], Комиссар по защите данных в Ирландии[4], Национальный комиссар по защите данных Португалии[5] и т.д.

Существенным отличием в текущей деятельности, деятельности по защите прав субъектов персональных данных и деятельности по контролю и надзору за соблюдением законодательства о персональных данных у этих органов как раз считается взаимодействие с операторами и субъектами персональных данных по предоставлению консультаций о применении законодательства о персональных данных. Примером может служить достаточно свежая статистика Национальной комиссии по информатике и свободам, где ключевым показателем является не количество проверок, или количество составленных протоколов и поступлений в бюджет государства, что характерно для ее российского аналога[6], а в большей степени количество консультаций, оказанных гражданам и организациям, количество выданных

[1] Information Commissioner's Office. – (https://ico.org.uk/for-organisations/). – Дата обращения 20.05.2017.
[2] Commission de la protection de la vie privée. – (https://www.privacycommission.be/fr/legislation-comites-sectoriels). – Дата обращения 20.05.2017.
[3] Commission Nationale de l'Informatique et des Libertés (CNIL). – (https://www.cnil.fr/fr/). – Дата обращения 20.05.2017.
[4] Data Protection Commissioner. – (https://www.dataprotection.ie/docs/Guidance-Material-Menu-Page/m/219.htm). – Дата обращения 20.05.2017.
[5] Comissão Nacional de Protecção de Dados. – (https://www.cnpd.pt/bin/orientacoes/orientacoes.htm). – Дата обращения 20.05.2017.
[6] Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2015 год. – (https://rkn.gov.ru/docs/Otchet_ZPD_rus2015.pdf htm). – Дата обращения 20.05.2017.

разрешений и количество заключений на проекты нормативных актов различного уровня[1].

Еще одним крайне интересным направлением деятельности Национальной комиссии по информатике и свободам является организация добровольной аккредитации бизнес-процессов компаний-операторов с точки зрения их соответствия законодательству о персональных данных и выдача им особого знака соответствия (Label CNIL)[2], что повышает степень доверия к ней со стороны потребителей услуг и проверяющего органа. Так в частности за 2016 год Комиссией было выдано 92 таких знака соответствия[3], которые могут быть использованы компаниями при предоставлении своих услуг и размещаться на их сайтах. Помимо возможности получить такой знак соответствия заинтересованные организации, а чаще всего их объединения, могут обратить в Комиссию для получения одобрения своих внутренних корпоративных правил обработки персональных данных[4]. Такая процедура обеспечивает большую прозрачность деятельности ассоциаций предпринимателей и их участников для органа контроля и надзора и позволяет им привести свои бизнес-процессы в соответствие с законодательством о персональных данных.

Безусловно, это далеко не все происходящие изменения в зарубежном законодательстве и практике, но с учетом российского опыта они были бы, на взгляд автора, наиболее полезными и актуальными для дальнейшего изучения и возможной адаптации к российским реалиям.

---

[1] Commission Nationale de l'Informatique et des Libertés. Rapport d'Activites 2016. – (https://www.cnil.fr/sites/default/files/atoms/files/cnil-37e_rapport_annuel_2016.pdf htm). – Дата обращения 20.05.2017.

[2] Les labels CNIL. – (https://www.cnil.fr/fr/les-labels-cnil htm). – Дата обращения 20.05.2017.

[3] Commission Nationale de l'Informatique et des Libertés. Rapport d'Activites 2016. – (https://www.cnil.fr/sites/default/files/atoms/files/cnil-37e_rapport_annuel_2016.pdf htm). – Дата обращения 20.05.2017.

[4] Les BCR (règles internes d'entreprise). – (https://www.cnil.fr/fr/les-bcr-regles-internes-dentreprise htm). – Дата обращения 20.05.2017.

ЗАКЛЮЧЕНИЕ

Очевидно, что стремительное распространение новых информационных технологий и поразительная быстрота, с которой они внедряются в жизнедеятельность общества, государства, бизнеса, личности, требует нового адекватного современным реалиям правового регулирования, позволяющего учесть баланс интересов между правами и свободами личности, общественными и государственными интересами. Совершенно естественно, что такие изменяющиеся реалии требуют осмысления их каждый раз по-новому в попытке найти новую точку баланса этих интересов. Как уже было заявлено в исследовании, идея защиты частной жизни при автоматизированной обработке данных, появившаяся на рубеже 70–80-х годов XX века в значительной степени эволюционировала за прошедшие 40 лет. Появились новые реалии и новые технологии, новые возможности для обработки данных о физических лицах.

В действительности, современный мир информационных технологий, активно использующий сейчас технологии «больших данных», «интернета вещей», «умных домов», «облачных вычислений», «Интернет-технологии web 2.0» и т.п., сделал жизнь человека более комфортной и удобной, но в тоже время и более уязвимой для внешнего вмешательства. Информационный след, оставляемый индивидом повсюду, не просто хранится, но подвергается глубокому и всестороннему анализу.

В противовес этому эволюционирует и идея личной свободы, которая теперь позволяет не только свободно располагать собой, но и информацией об индивиде, и в первую очередь – путем определения круга субъектов, допущенных к ее обработке. Именно возможность контролировать и определять параметры правового режима персональных данных, как информации ограниченного доступа, лежит в основе построения системы защиты персональных данных.

Итогом исследования, проведённого автором при решении поставленных задач, является предлагаемая автором концепция соотнесения

режима персональных данных, установленного специальным Федеральным законом «О персональных данных», с существующими правовыми режимами информации ограниченного доступа и сделаны следующие выводы.

Правовой режим персональных данных как информации имеет сложную структуру. Персональные данные могут быть как общедоступной информацией, в тех случаях, когда того требует норма закона или субъект сам дал на то свое согласие, либо, наоборот, находится в условиях режима информации ограниченного доступа. При этом в рамках последнего следует выделить особо правовой режим конфиденциальности персональных данных, который устанавливается специальным федеральным законом и включает в себя отдельно режим особых категорий персональных данных, режим биометрических персональных данных.

При этом наиболее сложным вопросом по-прежнему остается вопрос о соотнесении режима конфиденциальности персональных данных с другими режимами информации ограниченного доступа, и в частности режимами различного рода «тайн». Фактически в большинстве случаев, когда речь идет о профессиональных тайнах, чаще всего информацией, охраняемой на условиях таких режимов, оказываются именно персональные данные (врачебная тайна, тайна ЗАГС, нотариальная тайна, тайна исповеди, тайна связи и т.д.) Более того, персональные данные, как оказывается, могут находиться и в условиях иных режимов информации ограниченного доступа, включая государственную и служебную тайну.

В связи с этим и учитывая общие конституционные принципы, устанавливающие приоритет прав и свобод личности, следует рассматривать режимные требования специального закона о персональных данных как приоритетные, за исключение отдельных случаев, когда уже действующие режимные требования гарантируют более высокую степень защиты информации (государственная тайна).

При этом автором полагает целесообразным установление еще одного принципа регулирования обработки персональных данных – «презумпции

конфиденциальности» персональных данных, в том числе путем включения его в специальный закон о персональных данных.

Автором также отмечается, что неразрешенность множества проблем, связанных с определением содержания режима конфиденциальности персональных данных, объясняется общими теоретическими проблемами информационного права. Среди российских ученых по-прежнему нет единого мнения о понятии и содержании термина «тайна» и системе информации ограниченного доступа.

В целом представленное диссертационное исследование позволило уточнить понятие и содержание персональных данных и их режима, а также обосновать и сформулировать предложения по дальнейшему совершенствованию российского законодательства в этой сфере.

Настоящее исследование, безусловно, не исчерпывает всего перечня и содержания затрагиваемой проблематики в области персональных данных. К примеру, за пределами исследования остались вопросы об обеспечении защиты персональных данных и прав личности в условиях развития технологий «больших данных», «умных вещей», «Интернета вещей», которое вполне могут стать предметом самостоятельного исследования в этих областях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Нормативные правовые акты и другие официальные документы

1.1. Международные нормативные правовые акты

1. Всеобщая декларация прав человека. Принята и провозглашена Генеральной Ассамблеей ООН 10 декабря 1948 г. // Российская газета. – 1998. – 10 дек.
2. Конвенция о защите прав человека и основных свобод от 04.11.1950 // СЗ РФ. – 1998. – №20. – Ст. 2143.
3. Международный пакт о гражданских и политических правах от 16.12.1966 // Ведомости ВС СССР. – 1976. – № 17. – Ст. 291.
4. Конвенция о защите физических лиц при автоматизированной обработке персональных данных. Заключена в Страсбурге, 28 января 1981 г. // СЗ РФ. – 2014. – № 5. – Ст. 419.
5. Таможенный кодекс Таможенного союза: приложение к Договору о Таможенном кодексе Таможенного союза, принятому Решением Межгосударственного совета ЕврАзЭС на уровне глав государств от 27.11.2009 № 17 // СЗ РФ. – 2010. – № 50. – Ст. 6615.2.
6. Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» // Информационно-правовой портал «ГАРАНТ.РУ». – (http://base.garant.ru/2569783/). – Дата обращения: 02.04.2017.
7. Regulation (EC) № 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. – (http://data.europa.eu/eli/reg/2001/45/oj). – Дата обращения 20.05.2017.
8. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention,

investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. – (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&qid=1497555625791&from=en). – Дата обращения 20.05.2017.

9. General Data Protection Regulation (GDPR) 2012. – (http://ec. europa.eu/transparency/regdoc/rep/1/2012/EN/1-2012-11-EN-F1-1.Pdf). – Дата обращения 20.05.2017.

10. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. – (http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm). – Дата обращения: 02.04.2017.

11. Модельный закон «О персональных данных» принят на 14-м пленарном заседании Межпарламентской ассамблеи государств-участников СНГ (Постановление № 14-19 от 16 октября 1999 г.) // Межпарламентская ассамблея государств-участников Содружества Независимых Государств. Информационный бюллетень. – 2000. – № 23. – С. 315–326.

1.2. Законодательные акты Российской Федерации

12. Конституция (Основной закон) Российской Федерации от 12.12.1993 // Российская газета. – 1993. – 25 дек.

13. О чрезвычайном положении: федер. конституционный закон от 30.05.2001 № 3-ФКЗ // СЗ РФ. – 2001. – № 23. – Ст. 2277.

14. О лицензировании отдельных видов деятельности: федер. закон от 04.05.2011 № 99-ФЗ // СЗ РФ. – 2011. – № 19. – Ст. 2716.

15. Об участии в международном информационном обмене: федер. закон от 04.07.1996 № 85-ФЗ // СЗ РФ. – 1996. – № 28. – Ст. 3347. (Утратил силу.)

16. О средствах массовой информации: Закон Российской Федерации от 27.12.1991 № 2124-1 // Ведомости Съезда народных депутатов и Верховного Совета РСФСР. – 1992. – № 7. – Ст. 300.

17. Основы законодательства Российской Федерации об охране здоровья граждан от 22.07.1993 № 5487-1 // ВСНД и ВС РФ. 1993. – № 33. – Ст. 1318.

18. О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации: федер. закон от 13.01.1995 № 7-ФЗ // СЗ РФ. 1995. – № 3. – Ст. 170.

19. Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования: федер. закон от 01.04.1996 № 27-ФЗ // СЗ РФ. – 1996. – № 14. – Ст. 1401.

20. О социальном обслуживании граждан пожилого возраста и инвалидов: федер. закон от 02.08.1995 № 122-ФЗ (ред. от 25.11.2013) // СЗ РФ. – 1995. – № 32. – Ст. 3198. (Утратил силу.)

21. О Центральном банке Российской Федерации (Банке России): федер. закон от 10.07.2002 № 86-ФЗ // СЗ РФ. – 2002. – № 28. – Ст. 2790.

22. Об особенностях эмиссии и обращения государственных и муниципальных ценных бумаг: федер. закон от 29.07.1998 № 136-ФЭ // СЗ РФ. – 1998. – № 31. – Ст. 3814.

23. Об обязательном страховании гражданской ответственности владельцев транспортных средств: федер. закон от 25.04.2002 № 40-ФЗ // СЗ РФ. – 2002. – № 18. – Ст. 1720.

24. О правовом положении иностранных граждан в Российской Федерации: федер. закон от 25.07.2002 № 115-ФЗ // СЗ РФ. – № 30. – Ст. 3032.

25. О несостоятельности (банкротстве) кредитных организаций: федер. закон от 25.02.1999 № 40-ФЗ // СЗ РФ. 1999. – № 9. – Ст. 1097.

26. Об информации, информатизации и защите информации: федер. закон от 20.02. 1995 № 24-ФЗ // СЗ РФ. – 1995. – № 8. – Ст. 609.

27. О государственном банке данных о детях, оставшихся без попечения родителей: федер. закон от 16.04.2001 № 44-ФЗ // Российская газета. – 2001. – 20 апр.

28. О государственной защите судей, должностных лиц правоохранительных и контролирующих органов: федер. закон от 20.04.1995 № 45-ФЗ // СЗ РФ. – 1995. – № 17. Ст. – 1455.

29. О присяжных заседателях федеральных судов общей юрисдикции в Российской Федерации: федер. закон от 20.08.2004 № 113-ФЗ // СЗ РФ. – 2004. – № 34. – Ст. 3528.

30. О системе государственной службы Российской Федерации: федер. закон от 27.05.2003 № 58-ФЗ // СЗ РФ. – 2003. – № 22. – Ст. 2063.

31. О воинской обязанности и военной службе: федер. закон от 28.03.1998 № 53-ФЗ // СЗ РФ. – 1998. – № 13. – Ст. 1475.

32. О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных: федер. закон от 19.12.2005 № 160-ФЗ // СЗ РФ. – 2005. – № 52 (ч. 1). – Ст. 5573.

33. Об основах охраны здоровья граждан в Российской Федерации: федер. закон от 21.11.2011 № 323-ФЗ // СЗ РФ. – 2011. – № 48. – Ст. 6724.

34. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // СЗ РФ. – 2002. – № 1 (ч. 1). – Ст. 1.

35. Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации: федер. закон от 12.06.2002 № 67-ФЗ // СЗ РФ. – 2002. – № 24. – Ст. 2253.

36. О государственной автоматизированной системе Российской Федерации «Выборы»: федер. закон от 10.01.2003 № 20-ФЗ // Российская газета. – 2003. – 15 янв.

37. О государственной регистрации юридических лиц и индивидуальных предпринимателей: федер. закон от 08.08.2001 № 129-ФЗ // СЗ РФ. – 2001. – № 33 (ч. 1). – Ст. 3431.

38. О финансовом оздоровлении сельскохозяйственных товаропроизводителей: федер. закон от 09.07.2002 № 83-ФЗ // СЗ РФ. – 2002. – № 28. – Ст. 2787.

39. О третейских судах в Российской Федерации: федер. закон от 24.07.2002 № 102-ФЗ // СЗ РФ. – 2002. – № 30. – Ст. 3019.

40. Об архивном деле в Российской Федерации: федер. закон от 22.10.2004 № 125-ФЗ // СЗ РФ. 2004. – № 43. – Ст. 4169.

41. О порядке рассмотрения обращений граждан Российской Федерации: федер. закон от 02.05.2006 № 59-ФЗ // СЗ РФ. 2006. – № 19. – Ст. 2060.

42. О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации: федер. закон от 18.07.2006 № 109-ФЗ // СЗ РФ. – 2006. – № 30. – Ст. 3285.

43. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ // СЗ РФ. – 2006. – № 31. – Ст. 3448.

44. Об информации, информатизации и защите информации: федер. закон от 20.02.1995 № 24-ФЗ // СЗ РФ. – 1995. – № 8. – Ст. 609. (Утратил силу.)

45. Об официальном статистическом учете и системе государственной статистики в Российской Федерации: федер. закон от 29.11.2007 № 282-ФЗ // СЗ РФ. – 2007. – № 49. – Ст. 6043.

46. Об обеспечении доступа к информации о деятельности судов в Российской Федерации: федер. закон от 22.12.2008 № 262-ФЗ // СЗ РФ. – 2008. – № 52 (ч. 1). – Ст. 6217.

47. Об организации предоставления государственных и муниципальных услуг: федер. закон от 27.07.2010 № 210-ФЗ // СЗ РФ. – 2010. – № 31. – Ст. 4179.

48. О защите детей от информации, причиняющей вред их здоровью и развитию: федер. закон от 29.12.2010 № 436-ФЗ // СЗ РФ. – 2011. – № 1. – Ст. 48.

49. О государственной тайне: Закон Российской Федерации от 21.07.1993 № 5485-1 // СЗ РФ. – 1997. – № 41. – Ст. 8220.

50. Гражданский кодекс Российской Федерации от 21.10.1994 № 15-ФЗ (ч. 1) // СЗ РФ. 1994. – № 32. – Ст. 3301.

51. О внешней разведке: федер. закон от 10.01.1996 № 5-ФЗ // СЗ РФ. – № 3. – Ст. 143.

52. О рынке ценных бумаг: федер. закон от 22.04.1996 № 39-ФЗ // СЗ РФ. – № 17. – 1996. – Ст. 1918.

53. О государственной охране: федер. закон от 27.05.1996 № 57-ФЗ // СЗ РФ. – 1996. – № 22. – Ст. 2594.

54. Об обороне: федер. закон от 31.05.1996 № 61-ФЗ // СЗ РФ. – 1996. – № 23. – Ст. 2750

55. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. – 1996. – № 25. – Ст. 2954.

56. Об актах гражданского состояния: федер. закон от 15.11.1997 № 143-ФЗ // СЗ РФ. – 1997. – № 47. – Ст. 5340.

57. Налоговый кодекс Российской Федерации от 31.07.1998 № 146-ФЗ, часть первая //СЗ РФ. – 1998. – № 31. – Ст. 3824.

58. О почтовой связи: федер. закон от 17.07.1999 № 176-ФЗ // СЗ РФ. – 1999. – №29. – Ст. 3697.

59. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // СЗ РФ. – 2002. – № 1 (ч. 1). – Ст. 3.

60. О военном положении: федер. конституционный закон от 30.01.2002 № 1-ФКЗ // СЗ РФ. – 2002. – № 5. – Ст. 375.

61. О связи: федер. закон от 07.07.2003 № 126-ФЗ // СЗ РФ. – 2003. – № 28. – Ст. 2895.

62. О лотереях: федер. закон от 11.11.2003 № 138-ФЗ // СЗ РФ. – 2003. – № 46 (ч. 1). – Ст. 4434.

63. О коммерческой тайне: федер. закон от 29.07.2004 № 98-ФЗ // Российская газета. – 2004. – 5 авг.

64. О кредитных историях: федер. закон от 30.12.2004 № 218-ФЗ // СЗ РФ. – 2005. – № 1 (ч. 1). – Ст. 44.

65. О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ // Российская газета. – 2006. – 29 июля.

66. О безопасности: федер. закон от 28.12.2010 № 390-ФЗ // СЗ РФ. – 2011. – № 1. – Ст. 2.

67. Об электронной подписи: федер. закон от 06.04.2011 № 63-ФЗ // СЗ РФ. – 2011. – № 15. – Ст. 2036.

68. Воздушный кодекс Российской Федерации: федер. закон от 19.03.1997 № 60-ФЗ // СЗ РФ. – 1997. – № 12. – Ст. 1383.

69. О негосударственных пенсионных фондах: федер. закон от 07.05.1998 № 75-ФЗ // СЗ РФ. – 1998. – № 19. – Ст. 2071.

70. О банках и банковской деятельности: федер. закон от 02.12.1990 № 395-1 // СЗ РФ. – 1996 . – № 6. – Ст. 492.

71. О Всероссийской переписи населения: федер. закон от 25.01.2002 № 8-ФЗ // СЗ РФ. – 2002. – № 4. – Ст. 252.

1.3. Нормативные правовые акты Президента Российской Федерации:

72. Об утверждении перечня сведений конфиденциального характера: указ Президента Российской Федерации от 06.03. 1997 № 188 // СЗ РФ. – 1997. – № 10. – Ст. 1127.

73. Доктрина информационной безопасности Российской Федерации от 09.09.2000 № ПР-1895 // Российская газета. – 2000. – 28 сент. (Утратил силу.)

74. Доктрина информационной безопасности Российской Федерации утверждена Указом Президента РФ от 05.12.2016 г. № 646 // Российская газета. – 2016. – 6 дек.

75. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. Утверждена Указом Президента Российской Федерации от 9 мая 2017 г. № 203 // Российская газета. – 2017. – 10 мая.

76. Стратегия развития информационного общества в Российской Федерации от 07.02.2008 № Пр-212 // Российская газета. – 2008. – 16 февр.

1.4. Нормативные правовые акты Правительства Российской Федерации

77. Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или

муниципальными органами: постановление Правительства РФ от 21.03.2012 № 211 (ред. от 06.09.2014).

78. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 01.11.2012 № 1119.

79. «О государственной программе Российской Федерации «Информационное общество (2011–2020 годы)»: распоряжение Правительства Российской Федерации от 20.10.2010 № 1815-р // Российская газета. – 2010. – 6 нояб.

1.5. Нормативные правовые акты федеральных органов исполнительной власти

80. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18.02.2013 № 21.

1.6. Законодательство субъектов Российской Федерации

81. Об информационных ресурсах и информатизации города Москвы: Закон г. Москвы от 24.10.2001 № 52 // Вестник Мэрии Москвы. – 2001. – № 44.

1.7. Законодательные и нормативные акты иностранных государств

82. Personuppgiftslagen (PuL), 1998. – (http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204; http://www.datainspektionen.se/in-english/legislation/the-personal-data-act/). – Дата обращения: 02.04.2017.

83. Wet bescherming persoonsgegevens, 2000. – (https://compri.eu/assets/documentatie/8/origineel/wbp.pdf). – Дата обращения: 02.04.2017 г.

84. Loi n 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. – (http://www.cnil.fr/en-savoir-plus/textes-fondateurs/loi78-17/). – Дата обращения: 02.04.2017.

85. The Cable Communications Policy Act of 1984 (Pub. L. No. 98-549 (1984)). – (https://www.gpo.gov/fdsys/pkg/STATUTE-98/pdf/STATUTE-98-Pg2779.pdf). – Дата обращения 20.05.2017.

86. The Children's Online Privacy Protection Act of 1998 (COPPA) (Pub. L. No. 105-277 (1998)). – (https://www.gpo.gov/fdsys/pkg/PLAW-105publ277/html/PLAW-105publ277.htm). – Дата обращения 20.05.2017.

87. The Driver's Privacy Protection Act of 1994 (Pub. L. No. 103-322 (1994)). – (https://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap123-sec2721.pdf). – Дата обращения 20.05.2017.

88. The Electronic Communications Privacy Act of 1986 (ECPA) (18 U.S.C. § 2510 et seq.). – (https://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf). – Дата обращения 20.05.2017.

89. The Fair Credit Reporting Act (Pub. L. No. 91-508 (1970)). – (https://www.gpo.gov/fdsys/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf). – Дата обращения 20.05.2017.

90. The Family Educational Rights and Privacy Act of 1974 (FERPA or the Buckley Amendment) (Pub. L. No. 93-380 (1974)). – (http://www.legisworks.org/GPO/STATUTE-88-Pg484.pdf). – Дата обращения 20.05.2017.

91. The Freedom of Information Act (FOIA) (5 U.S.C. § 552). – (https://www.gpo.gov/fdsys/pkg/STATUTE-80/pdf/STATUTE-80-Pg250.pdf). – Дата обращения 20.05.2017.

92. The Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191). – (https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm). – Дата обращения 20.05.2017.

93. The Privacy Act of 1974 (Pub.L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552a). – (https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf). – Дата обращения 20.05.2017.

94. The Right to Financial Privacy Act of 1978 (RFPA; codified at 12 U.S.C. ch. 35, § 3401 et seq.). – (https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg3641.pdf). – Дата обращения 20.05.2017.

95. The Telephone Consumer Protection Act of 1991 (Pub. L. No. 102-243 (1991)). – (https://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapII-partI-sec227.pdf). – Дата обращения 20.05.2017.

96. The Video Privacy Protection Act (Pub. L. No. 100-618 (1988)). – (https://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg3195.pdf). – Дата обращения 20.05.2017.

2. Книги (монографии, учебники, учебные пособия)

2.1. Специальная научная литература

97. Алексеев, С.С. Проблемы теории права / С.С. Алексеев. – Свердловск, 1972.

98. Алексеев, С.С. Теория права / С.С. Алексеев. – М., 1993.

99. Арешев, А.Г. Персональные данные в структуре информационных ресурсов. Основы правового регулирования / А.Г. Арешев, И.Л. Бачило, Л.А. Сергиенко. – М., 2006.

100. Батурин, Ю.М. Право и политика в компьютерном круге / Ю.М. Батурин. – М.: Наука, 1987. – 109 с.

101. Батурин, Ю.М. Проблемы компьютерного права / Ю.М. Батурин. – М.: Юридич. лит-ра, 1991. – 272 с.

102. Бахрах, Д.Н. Административное право России: учебник для вузов / Д.Н. Бахрах. – М.: Изд-во НОРМА (ИГ НОРМА-ИНФРА • М), 2002. – 640 с.

103. Бачило, И.Л. Информационное право: учебник для вузов / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов / Под ред. Б.Н. Топорнина. – СПб.: Юридич. центр Пресс, 2005. – 789 с.

104. Бачило, И.Л. Информационное право: учебник / И.Л. Бачило. – М.: Юрайт; ИД Юрайт, 2009. – 401 с.

105. Венгеров, А.Б. Право и информация в условиях автоматизации управления: Теоретические вопросы / А.Б. Венгеров. – М.: Юридич. лит-ра, 1978. – 208 с.

106. Винер, Н. Кибернетика и общество / Н. Винер. – М.: Иностр. лит-ра, 1958. – 200 с.

107. Винер, Н. Мое отношение к кибернетике, ее прошлое и будущее / Н. Винер. – М.: Советское радио, 1969.

108. Владимиров, Л.Е. Учение об уголовных доказательствах. Части Общая и Особенная / Л.Е. Владимиров. – Спб., 1910.

109. Войниканис, Е.А. База данных как объект правового регулирования: учебное пособие для вузов / Е.А. Войниканис, В.О. Калятин / Исследовательский центр частного права при Президенте РФ. – М.: Статут, 2011. – 174 с.

110. Войниканис, Е.А. Информация. Собственность. Интернет. Традиция и новеллы в современном праве / Е.А. Войниканис, М.В. Якушев. – М.: Волтерс Клувер, 2004. – 176 с.

111. Гомьен, Д. Европейская конвенция о правах человека и Европейская социальная хартия: право и практика / Д. Гомьен, Д. Харрис, Л. Зваак. – М., 1998.

112. Городов, О.А. Информационное право: учебник / О.А. Городов. – М., Проспект, 2008.

113. Информационное право: актуальные проблемы теории и практики / Под ред. И.Л. Бачило. – М., 2009. – 530 с.

114. Иванский, В.П. Правовая защита информации о частной жизни граждан. Опыт современного правого регулирования: монография / В.П. Иванский. – М.: Изд-во РУДН, 1999.

115. Климонтович, Н.Ю. Без формул о синергетике / Н.Ю. Климонтович. – Минск, Вышэйшая школа, 1986. – С. 132.

116. Красавчикова, Л.О. Личная жизнь под охраной закона / Л.О. Красавчикова. – М., 1983.

117. Копылов, В.А. Информационное право: учебное пособие / В.А. Копылов. – М.: Юристъ, 1997. – 472 с.

118. Килкэли, У. Европейская конвенция о защите прав человека и его основных свобод. Статья 8: Право на уважение частной и семейной жизни, жилища и корреспонденции. Прецеденты и комментарии / У. Килкэли, Е.А. Чефранова. – М., 2001.

119. Лапина, М.А. Информационное право / М.А. Лапина, Г.А. Ревин, В.И. Лапин. – М.: Юнити-Дана, 2004.

120. Лопатин, В.Н. Информационная безопасность России: Человек. Общество. Государство: монография / В.Н. Лопатин. – СПб.: СПб. ун-т МВД России; фонд «Университет», 2000. – 428 с.

121. Лопатин, В.Н. Правовые основы информационной безопасности: курс лекций / В.Н. Лопатин. – М.: МИФИ, 2000.

122. Люшер, Ф. Конституционная защита прав и свобод личности / Ф. Люшер. – М., 1993.

123. Мазуров, В.А. Тайна: государственная, коммерческая, банковская, частной жизни. Уголовно-правовая защита: учебное пособие / В.А. Мазуров / Под научн. рук. д-ра юрид. наук, проф. С.В. Землюкова. – М.: Издательско-торговая корпорация «Дашков и К^{о}», 2003.

124. Морозов, А.В. Система правовой информации Минюста России / А.В. Морозов. – М.: Триумф», 1999. – 464 с.

125. Наумов, В.Б. Право и Интернет: очерки теории и практики / В.Б. Наумов. – М.: Книжный дом «Университет», 2002. – 432 с.

126. Маковей, М. Европейская конвенция о защите прав человека и основных свобод. Статья 10: Право на свободу выражения своего мнения. Прецеденты и комментарии / М. Маковей, Е.А. Чефранова. – М., 2001.

127. Петрыкина, Н.И. Правовое регулирование оборота персональных данных. Теория и практика / Н.И. Петрыкина. – М.: Статут, 2011. – 134 с.

128. Полякова, Т.А. Правовые основы информационной безопасности в России: монография / Т.А. Полякова. – М.: Триумф, 2007. – 189 с.

129. Правовая информатика и кибернетика / Под ред. Н.С. Полевого. – М.: Юридич. лит-ра, 1993. – 528 с.

130. Пресман, А.С. Организация биосферы и ее космические связи / А.С. Пресман. – М., 1977.

131. Рассолов, И.М. Теоретические проблемы интернет-права / И.М. Рассолов. – М.: РПА МЮ РФ, 2002. – 284 с.

132. Розенберг, В. Промысловая тайна / В. Розенберг. – СПб.: Типогр. редакции Министерства финансов, 1910.

133. Рушайло, В.Б. Специальные административно-правовые режимы в сфере обеспечения общественной безопасности: монография / В.Б. Рушайло. – М.: Спутник-Плюс, 2003. – 153 с.

134. Смолькова, И.В. Проблемы охраняемой законом тайны в уголовном процессе / И.В. Смолькова. – М.: Луч, 1999.

135. Стрельцов, А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы / А.А. Стрельцов. – Минск: Беллитфонд, 2005. – С. 291.

136. Теоретические основы информатики и информационной безопасности / Под ред. В.А. Минаева, В.Н. Саблина. – М.: Радио и связь, 2000.

137. Терещенко, Л.К. Правовой режим информации: монография / Л.К. Терещенко. – М.: ИД «Юриспруденция», 2007. – 192 с.

138. Терещенко, Л.К. Модернизация информационных отношений и информационного законодательства / Л.К. Терещенко. – М.: ИД «ИНФРА-М», 2013. – 227 с.

139. Тихомиров, Ю.А. Административное право и процесс – 2-е изд. / Ю.А. Тихомиров. – М., 2005. – 377 с.

140. Тихомиров, М.Ю. Юридическая энциклопедия / М.Ю. Тихомиров. – М., 1997.

141. Травкин, Ю.В. Персональные данные / Ю.В. Травкин. – М.: Амалданик, 2007. – 432 с.

142. Фатьянов, А.А. Тайна и право (основные системы ограничений на доступ к информации в российском праве): монография / А.А. Фатьянов. – М.: МИФИ, 1998. – 268 с.

143. Фатьянов, А.А. Правовое обеспечение безопасности информации в Российской Федерации: учебное пособие / А.А. Фатьянов. – М.: Юрист, 2001. – 412 с.

144. Хабриева, Т.Я. Теория современной конституции / Т.Я. Хабриева, В.Е. Чиркин. – М.: НОРМА, 2007. – 265 с.

145. Шеннон, К. Работы по теории информации и кибернетики: Пер. с англ. / К. Шеннон / Под. ред. Р.Л. Добрушина, О.Б. Лупанова. – М.: Иностр. лит-ра, 1963. – 830 с.

2.2. Статьи, периодические издания

146. Алексенцев, А.И. О составе защищаемой информации / А.И. Алексенцев // Безопасность информационных технологий. – 1999. – № 2. – С. 5–7.

147. Баранов, В.М. Категория «частная жизнь» / В.М. Баранов // Право граждан на информацию и защита неприкосновенности частной жизни. – Н. Новгород. – 1999. – С. 34–37.

148. Бачило, И.Л. Информационное право. Роль и место в системе права Российской Федерации / И.Л. Бачило // Государство и право. – 2001. – № 2. – С. 5–14.

149. Бачило, И.Л. Информация и информационные отношения в праве / И.Л. Бачило // НТИ. – 1999. – № 8. – Сер. 1.

150. Бачило, И.Л. Методология решения правовых проблем в области информационной безопасности / И.Л. Бачило // Информатика и вычислительная техника. – 1992. – № 2–3. – С. 21–25.

151. Бачило, И.Л. Право на информацию / И.Л. Бачило // Проблемы информатизации. – 1995. – № 1. – С. 67–72.

152. Бундин, М.В. Система информации ограниченного доступа и конфиденциальность // Вестник Нижегородского университета им. Н.И. Лобачевского. – Н. Новгород: Изд-во Нижегор. гос. ун-та. – 2015. – № 1. – С. 120–130.

153. Бундин, М.В. Персональные данные как информация ограниченного доступа / М.В. Бундин // Информационное право. – 2009. – № 1. – С. 10–14.

154. Бундин, М.В. Персональные данные как термин российского законодательства / М.В. Бундин // Правовые вопросы связи. – 2009. – № 1. – С. 4–6.

155. Волчинская, Е.К. Коммерческая тайна в системе конфиденциальной информации / Е.К. Волчинская // Информационное право. – М.: Юрист, 2005. – № 3. – С. 17–21.

156. Егоров, А. Правовые основы институтов тайны / А. Егоров // Закон. – 1998. – № 2. – С. 75.

157. Ефремов, А. Понятие и виды конфиденциальной информации / А. Ефремов. – (http://www.russianlaw.net/law/confidential_data/a90/). – Дата обращения 02.07.2017.

158. Ищейнов, В.Я. Персональные данные в законодательных и нормативных документах Российской Федерации и информационных системах / В.Я. Ищейнов // Делопроизводство. – 2006. – № 3. – С. 90.

159. Коровяковский, Д.Г. Российский и зарубежный опыт в области защиты персональных данных / Д.Г. Коровяковский // Национальные интересы: приоритеты и безопасность. – 2009. – № 5. – С. 49–50.

160. Кузнецов, П.У. Правовая методология информационных процессов и информационной безопасности: монография / П.У. Кузнецов // Право – Информация – Безопасность. – Екатеринбург: УрГЮА, 2001. – № 1. – С. 64–65.

161. Лопатин, В.Н. Концептуальные основы развития законодательства в сфере обеспечения информационной безопасности / В.Н. Лопатин //

Управление защитой информации. – 1999. – Минск. – Т. 3. – № 1. – С. 27–35.

162. Лопатин, В.Н. Модельный закон «О персональных данных» для государств-участников СНГ / В.Н. Лопатин, А.В. Федоров // Сб. мат-лов Междунар. науч.-практич. конф. 29 ноября 1998 г. «Новые технологии в практике правоохранительных органов». – СПб., 1998. – С. 61–73.

163. Матузов, Н.И. Правовые режимы: Вопросы теории и практики / Н.И. Матузов, А.В. Малько // Правоведение. – 1996. – № 1. – С. 16–29.

164. Морозов, А.В. Интернет и проблемы правовой информатизации / А.В. Морозов / Текст выступления. Парламентские слушания в Государственной Думе 17.12.1996. – 5 с.

165. Морозов, А.В. Основные концепции подбора и подготовки персонала в правовых компьютерных системах законораспространительной деятельности / А.В. Морозов, В.К. Морозов. // Сб.: Правовая информатика. – М.: Минюст. РФ, 1997. – № 2. – С. 7–14.

166. Наумов, В.Б. Особенности правового регулирования сети Интернет / В.Б. Наумов // Тезисы докладов Всерос. науч.-методич. конф. «Интернет и современное общество», 8–11 декабря 1998 г. – СПб.: СПб, гос. ун-т. – С. 51–53.

167. Наумов, В.Б. Проблемы реализации авторских прав в сети Интернет / В.Б. Наумов // Мир Медиа XXI. – Национ. ин-т прессы, 1999. – № 1. – С. 14–16.

168. Нестерова, С. Институт коммерческой тайны в законодательстве России / С. Нестерова, Н. Ткаченко // Экономика и жизнь. – 1994. – № 4. – С. 204.

169. Параскевов, А.В. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом / А.В. Параскевов, А.В. Левченко, Ю.А. Кухоль // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар, КубГУ, 2015. – № 110. – С. 866–894.

170. Петровский, С.В. Правовое регулирование оказания интернет-услуг / С.В. Петровский // Российская юстиция. – 2001. – №5. – С. 63–64.

171. Полякова, Т.А. Правовые аспекты обеспечения информационной безопасности в субъектах Российской Федерации / Т.А. Полякова // Бюллетень Минюста РФ. – М.: Спарк, 2001. – № 7. – С. 60–62.

172. Полякова, Т.А. Проблемы развития законодательства Российской Федерации в сфере информационной безопасности / Т.А. Полякова // Сб. Правовая информатика. – М.: НЦПИ, 1999. – №4. – С. 38–44.

173. Разина, Е. Свобода слова, или право на забвение / Е. Разина // Справочно-правовой портал «Гарант.ру». – (http://www.garant.ru/ia/opinion/author/razina/637159/). – Дата обращения 20.05.2017.

174. Савинцева, М. Правовая защита персональной информации граждан в России / М. Савинцева // Законодательство и практика масс-медиа. – 2006. – № 9 (сент.). – С. 12–13.

175. Серго, А.Г. Как защитить свои авторские права в Интернете / А.Г. Серго // PCWeek (Russian editoin). – 2001. – № 38. – С. 15.

176. Столяров, Н.В. Организация защиты государственной тайны в России / Н.В. Столяров. – (http://www.sec4all.net/gostaina-russ.html). – Дата обращения: 02.04.2017.

177. Терещенко, Л.К. О соблюдении баланса интересов при установлении мер защиты персональных данных / Л.К. Терещенко // Журнал российского права. – 2011. – № 5. – С. 5–12.

178. Терещенко, Л.К. Электронное правосудие и открытость информации / Л.К. Терещенко // Право и экономика. – 2011. – № 4. – С. 4–10.

179. Терещенко, Л.К. Открытость информации и «пиратство» в Интернете / Л.К. Терещенко // Журнал зарубежного законодательства и сравнительного правоведения. – 2011. – № 1 (26). – С. 70–74.

180. Тихомиров, Ю.А. Правовой режим информационных процессов: Национальное законодательство и международное сотрудничество / Ю.А. Тихомиров // НТИ. – 1993. – Сер. 1 – № 7. – С. 3–6.

181. Тоффлер, Э. «Третья волна» / Э. Тоффлер // США Экономика, политика, идеология. – 1982. – № 7. – С. 97–102.

182. Фатьянов, А.А. Тайна как социальное и правовое явление. Ее виды / А.А. Фатьянов // Государство и право. – 1998. – № 6. – С. 19–28.

183. Хабриева, Т.Я. Коррупция и правопорядок в фокусе современной юридической доктрины / Т.Я. Хабриева // Журнал зарубежного законодательства и сравнительного правоведения. –2016. – № 4 (59). – С. 5-13.

184. Хабриева, Т.Я. Коррупция и право: доктринальные подходы к постановке проблемы / Т.Я. Хабриева // Журнал российского права. – 2012. – № 6 (186). – С. 5-17.

185. Халиев, К.Р. Нормативная сила «директив» ЕС / К.Р. Халиев // Актуальные проблемы экономики и права. – Казань: Познание, 2008. – № 3 (7). – С. 163–166.

2.3. Литература на иностранных языках

186. Banisar, D. National Comprehensive Data Protection / D. Banisar // Privacy Laws and Bills 2016 (November 28, 2016). – (https://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416). – Дата обращения 02.05.2017.

187. Beigner, B. La protection de la vie privee / B. Beigner // Libertes et Droits fondamentaux. – Paris: Dalloz, 2003. – P. 172–173.

188. Beigner, B. Le droit de la personnalité / B. Beigner // Collection “Que sais-je?” – P.U.F., 1992. – n°2703.

189. Bibent, M. Le Droit du Traitement de l’Information / M. Bibent. – Paris: ADBS, Nathan, 2000.

190. Bloustein, E. Privacy as an Aspect of Human Dignity / E. Bloustein // New York University Law Review. – 1964. – No 39. – P. 971.

191. Braibant, G. Données personnelles et société de l’information / G. Braibant. – Paris, 2000.

192. Byrum, K. The European right to be forgotten: A challenge to the United States Constitution's First Amendment and to professional public relations ethics / K. Byrum // Public Relations Review. – 2017. – Vol. 43. – No. 1. – P. 102–111.

193. Cadoux, L. La Vie Privée: un Avenir sous Haute Surveillance / L. Cadoux // Liberté d'Expression et Nouvelles Technologies, IQ Collectif. – Paris, 1998.

194. Gavison, R. Privacy and the Limits of Law / R. Gavison // Yale Law Journal. – 1980. – No 89. – P. 421, 428.

195. Hustinx, P.J. Right to privacy and data protection: mission impossible? / P.J. Hustinx // European Data Protection Day, 28 January 2010. – (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa384). – Дата обращения: 02.04.2017.

196. Masuda, Y. The Information Society as Postindustrial Society / Y. Masuda. – Washington: World Future Soc., 1983.

197. Reidenberg, J.R. Privacy Protection and the Interdependence of Law Technology and Self-Regulation / J.R. Reidenberg // Variations sur le Droit de la Société de l'Information. – Bruxelles: Bruylant, 2001.

198. Warren, S.D. Right To Privacy / S.D. Warren, L.D. Brandeis // Harvard Law Review. – 1890. – No. 5 (10 december). – Vol. IV. – (http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm). – Дата обращения: 2.04.2017)

199. Westin, A.F. Privacy and Freedom / A.F. Westin. – New York: Atheneum, 1967.

2.4. Диссертации, авторефераты диссертаций

200. Абаев, Ф.А. Правовое регулирование отношений по защите персональных данных работника в трудовом праве: автореф. дис. ... канд. юрид. наук: 12.00.05 / Ф.А. Абаев. – М., 2014. – 26 с.

201. Антопольский, А.А. Правовое регулирование информации ограниченного доступа в сфере государственного управления: автореф. дисс. … канд. юрид. наук / А.А. Антопольский. – М., 2004.

202. Белгородцева, Н.Г. Теоретико-правовые аспекты защиты персональных данных: автореф. дис. ... канд. юрид. наук: 12.00.01 / Н.Г. Белгородцева. – М., 2012. – 25 с.

203. Белгородцева, Н.Г. Теоретико-правовые аспекты защиты персональных данных: дис. ... канд. юрид. наук: 12.00.01 / Н.Г. Белгородцева. – М., 2012. – 201 с.

204. Бондарь, И.В. Тайна по российскому законодательству (проблемы теории и практики): автореф. дис. ... канд. юрид. наук: 12.00.01 / И.В. Бондарь. – Нижний Новгород, 2004. – 27 с.

205. Вельдер, И.А. Система правовой защиты персональных данных в Европейском союзе: автореф. дис. ... канд. юрид. наук: 12.00.10 / И.А. Вельдер. – Казань, 2006. – 28 с.

206. Вельдер, И.А. Система правовой защиты персональных данных в Европейском союзе: дис. ... канд. юрид. наук: 12.00.10 / И.А. Вельдер.. – Казань, 2006. – 165 с.

207. Волокитина, Е.С. Метод и алгоритмы гарантированного обезличивания и реидентификации субъекта персональных данных в автоматизированных информационных системах: автореф. дис. ... канд. техн. наук: 05.13.19 / Е.С. Волокитина. – СПб., 2013. – 24 с.

208. Головкин, Р.Б. Правовое и моральное регулирование частной жизни в современной России: дис. ... д-ра юрид. наук: 12.00.01 / Р.Б. Головкин. – Н. Новгород, 2005. – 516 с.

209. Дворецкий, А.В. Защита персональных данных работника по законодательству Российской Федерации: автореф. дис. ... канд. юрид. наук: 12.00.05 / А.В. Дворецкий. – Томск, 2005. – 25 с.

210. Исаков, В.Б. Проблемы теории юридических фактов: дис. ... д-ра юрид. наук: 12.00.01 / В.Б. Исаков. – Свердловск, 1985. – 392 с.

211. Кузнецов, П.У. Теоретические основания информационного права: дис. ... д-ра юрид. наук: 12.00.14 / П.У. Кузнецов. – Екатеринбург, 2005. – 410 с.

212. Кучеренко, А.В. Правовое регулирование персональных данных в Российской Федерации: автореф. дис. ... канд. юрид. наук: 12.00.14 / А.В. Кучеренко. – Челябинск, 2010. – 22 с.

213. Лебедева, Н.Н. Правовая культура личности и Интернет: Теоретический аспект: автореф. дис. ... канд. юрид. наук: 12.00.01 / Н.Н. Лебедева. – М., 2004. – 21 с.

214. Минбалеев, А.В. Система информации: теоретико-правовой анализ: автореф. дис. ... канд. юрид. наук: 12.00.14 / А.В. Минбалеев. – Челябинск, 2006. – 33 с.

215. Петрыкина, Н.И. Правовое регулирование оборота персональных данных в России и странах ЕС: сравнительно-правовое исследование: дис. ... канд. юрид. наук: 12.00.14 / Н.И. Петрыкина. – М., 2007. – 173 с.

216. Петрыкина, Н.И. Правовое регулирование оборота персональных данных в России и странах ЕС: сравнительно-правовое исследование: автореф. дис. ... канд. юрид. наук: 12.00.14 / Н.И. Петрыкина. – М., 2007. – 26 с.

217. Просветова, О.Б. Защита персональных данных: дис. … канд. юрид. наук: 05.13.19 / О.Б. Просветова. – Воронеж, 2005. – 193 с.

218. Телина, Ю.С. Конституционное право гражданина на неприкосновенность частной жизни, личную и семейную тайну при обработке персональных данных в России и зарубежных странах: автореф. дис. ... канд. юрид. наук: 12.00.02 / Ю.С. Телина. – М., 2016. – 33 с.

219. Терещенко, Л.К. Правовой режим информации: автореф. дис. ... д-ра юрид. наук: 12.00.14 / Л.К. Терещенко. – М., 2011. – 54 с.

220. Федосин, А.С. Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации: автореф. дис. ... канд. юрид. наук: 12.00.14 / А.С. Федосин. – Саранск, 2009. – 27 с.

221. Шередин, Р.В. Методы и системы защиты информации, информационная безопасность: автореф. дис. ... канд. техн. наук: 05.13.19 / Р.В. Шередин. – М., 2011. – 18 с.

2.5. Справочная литература

222. Даль В. Толковый словарь / В. Даль. – М., 1955. – Т. 4. – С. 386.

223. Ефремова, Т.Ф. Новый словарь русского языка. Толково-словообразовательный / Т.Ф. Ефремова. – М.: Русский язык, 2000. – (http://www.efremova.info). – Дата обращения: 02.04.2017.

224. Новейший философский словарь. – Минск, 1998.

225. Ожегов, С.И. Словарь русского языка / С.И. Ожегов. – М.: Русский язык, 1984. – С. 683.

226. Словарь бизнес-терминов. Академик.ру. 2001. – (http://dic.academic.ru/dic.nsf/business/3172). – Дата обращения: 02.04.2017.

227. Современный словарь иностранных слов. – М., 1993.

228. Философский словарь / Под ред. И.Т. Фролова. – 5-е изд. – М.: Политиздат, 1986. – С. 172.

229. Ткач, М.И. Энциклопедический словарь / М.И. Ткач. – М.: Проспект, 2009.– (http://dic.academic.ru/contents.nsf/es/). – Дата обращения: 02.04.2017.

3. Судебная практика

230. Апелляционное определение Московского городского суда от 06.07.2012 по делу № 11-11648\12 // СПС «КонсультантПлюс».

231. Апелляционное определение Московского городского суда от 06.07.2012 по делу № 11-11648\12 // СПС «КонсультантПлюс».

232. Case of Gaskin v. The United Kingdom, Judgement of 07/07/1989. – § 89. – (http://hudoc.echr.coe.int/eng?i=001-57491). – Дата обращения 02.05.2017.

233. Case of Guillot v. France, Judgement of 24/10/1996. – (http://hudoc.echr.coe.int/eng?i=001-58069). – Дата обращения 02.05.2017.

234. Case of Roman Zakharov v. Russia, Judgement of 04/12/2015. – (http://hudoc.echr.coe.int/eng?i=001-159324). – Дата обращения 02.05.2017.

235. Case of S. and Marper v. The United Kingdom, Judgement of 04/12/2008. – § 67. – (http://hudoc.echr.coe.int/eng?i=001-90051). – Дата обращения 02.05.2017.

236. Case of Shimovolos v. Russia, Judgement of 21/06/2011. – (http://hudoc.echr.coe.int/eng?i=001-105217). – Дата обращения 02.05.2017.

237. Case of Stjerna v. Finland, Judgement of 25/11/1994. – (http://hudoc.echr.coe.int/eng?i=001-57912). – Дата обращения 02.05.2017.

238. Judgement of the Court (Grand Chamber) 13 May 2014. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. – (http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=EN). – Дата обращения 20.05.2017.

239. Reno v. Condon, 528 U.S. 141 (2000). – (https://supreme.justia.com/cases/federal/us/528/141/case.html.). – Дата обращения 20.05.2017.

240. Owasso Independent School District v. Falvo, 534 U.S. 426 (2001). – (https://supreme.justia.com/cases/federal/us/534/426/case.html). – Дата обращения 20.05.2017.

241. Reno v. Condon, 528 U.S. 141 (2000). – (https://supreme.justia.com/cases/federal/us/528/141/case.html.). – Дата обращения 20.05.2017.

4. Интернет-ресурсы:

242. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). – (https://rkn.gov.ru/). – Загл. с экрана.

243. Портал персональных данных уполномоченного органа по защите прав субъекта субъектов персональных данных – (http://pd.rkn.gov.ru/). – Загл. с экрана.

244. ФСТЭК России – Федеральная служба по техническому и экспортному контролю – (http://fstec.ru/). – Загл. с экрана.

245. EUR-Lex.europa.eu. – (http://eur-lex.europa.eu/). – Загл. с экрана.

246. CNIL (Commission Nationale de l'Informatique et des Libertés). – (https://www.cnil.fr/). – Загл. с экрана.

247. Европейская Конвенция о защите прав человека: право и практика. / – (http://echr.ru/). – Загл. с экрана.

248. European Court of Human Rights (ECHR). – (http://www.echr.coe.int /Pages/home.aspx?p=home). – Загл. с экрана.

249. OECD – Information security and Privacy/ – (http://www.oecd.org /sti/ieconomy/informationsecurityandprivacy.htm). – Загл. с экрана.

250. EPIC – Electronic Privacy Information Center. – (https://epic.org/). – Загл. с экрана.