Федеральное государственное автономное образовательное учреждение высшего образования «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)»

На правах рукописи

Окишев Борис Александрович

Публично-правовое регулирование в сфере использования цифровых технологий при обработке персональных данных

5.1.2. Публично-правовые (государственно-правовые) науки

ДИССЕРТАЦИЯ
на соискание учёной степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук, доцент
Добробаба Марина Борисовна

Москва – 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 3

ГЛАВА 1. Общая характеристика публично-правового регулирования в сфере использования цифровых технологий при обработке персональных данных 16

§ 1. Персональные данные: понятие и правовая природа 16

§ 2. Правовая природа использования цифровых технологий при обработке персональных данных 38

§ 3. Правовое обеспечение использования цифровых технологий при обработке персональных данных 53

ГЛАВА 2. Особенности публично-правового регулирования в сфере использования отдельных цифровых технологий при обработке персональных данных 80

§ 1. Особенности публично-правового регулирования в сфере использования искусственного интеллекта при обработке персональных данных 80

§ 2. Особенности публично-правового регулирования в сфере использования технологий распределённого реестра при обработке персональных данных 95

§ 3. Особенности публично-правового регулирования в сфере использования облачных технологий при обработке персональных данных 101

ГЛАВА 3. Проблемы и перспективы развития системы публично-правового регулирования обработки персональных данных с использованием цифровых технологий 112

§ 1. Этико-правовые проблемы в сфере публично-правового регулирования обработки персональных данных с использованием цифровых технологий 112

§ 2. Проблемы публично-правового регулирования обработки персональных данных, составляющих врачебную тайну, при использовании цифровых технологий 124

§ 3. Проблемы и перспективы развития института административной ответственности в области нарушения требований законодательства о персональных данных 134

ЗАКЛЮЧЕНИЕ 151

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ 164

ПРИЛОЖЕНИЕ 196

ВВЕДЕНИЕ

Актуальность темы исследования. Современное развитие цифровых и иных информационных технологий, влекущее за собой всё более широкое применение мобильного интернета, искусственного интеллекта, блокчейн-технологий и облачных сервисов, сопровождается увеличением количества коммуникационных каналов, в связи с чем всё большее значение приобретает публично-правовое регулирование в сфере использования цифровых технологий при обработке персональных данных.

Стремительное развитие экономики данных, технологий цифровизации и глобализация рынков привели к облегчению сбора, обработки, систематизации и накопления персональных данных граждан. Сбор данных транснациональными компаниями о гражданах других стран, их предпочтениях, личных данных нарушает национальные интересы в системе обеспечения безопасности государств, что также является весомым аргументом в пользу актуальности научных исследований публично-правового регулирования в сфере использования цифровых технологий при обработке персональных данных.

Правовое регулирование новых цифровых технологий сбора, обработки данных, в том числе технологий искусственного интеллекта, квантовых вычислений и квантовых коммуникаций, является национальным интересом в области экономики данных и цифровой трансформации государства в соответствии с национальным проектом «Экономика данных и цифровая трансформация государства», утверждённым протоколом Президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 20 декабря 2024 года № 12-пр, и соответствует национальной цели, закреплённой в Указе Президента Российской Федерации от 7 мая 2024 года № 309 «О национальных целях развития Российской Федерации до 2030 года и на перспективу до 2036 года», что подчеркивает важность изучения и развития публично-правового регулирования в сфере использования цифровых технологий при обработке персональных данных.

Вследствие развития технологий обработки и анализа данных о потребителе и его предпочтениях сформировались специальные инструменты повышения продаж и управления выбором потребителя: «маркетинговые исследования», «контекстная реклама», «персональные рассылки», «спам», «таргетинг» и другие. Несмотря на определённые преимущества явного увеличения обмена информацией, набирают силу и обратные тенденции, свидетельствующие об угрозах нарушения ряда конституционных прав граждан, в том числе права на неприкосновенность частной жизни, личную и семейную тайну. Вышеперечисленные процессы способствуют росту инцидентов, связанных с неправомерным использованием персональных данных в противоправных целях. К массивам информации получают доступ не только уполномоченные государственные органы, но и широкий круг лиц, чьи интересы могут носить личный или коммерческий характер.

Недостаточность нормативно закреплённых мер и способов регулирования в области персональных данных порождает правонарушения в данной сфере. Ежегодно происходят масштабные утечки персональных данных в связи с тем, что законодательство о защите персональных данных отстаёт от современного уровня развития технологий. Проработка мер ответственности за незаконный оборот персональных данных и иные нарушения законодательства в области персональных данных реализуется в рамках поручения Президента Российской Федерации по итогам заседания Совета по развитию гражданского общества и правам человека, состоявшегося 7 декабря 2022 года[1]. Данные обстоятельства являются «двигателем» для формирования и активного развития публично-правового регулирования в сфере использования цифровых технологий при обработке персональных данных.

Таким образом, актуальность научного исследования вопросов публично-правового регулирования в сфере использования цифровых технологий при обработке персональных данных в настоящий момент довольно высока, и

[1] См.: Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека / утв. Президентом РФ 12.01.2023 № Пр-19.

значимость таких исследований будет только возрастать в условиях дальнейшего развития экономики данных и широкого внедрения различных цифровых технологий.

Степень разработанности темы исследования. Публично-правовое регулирование в сфере использования цифровых технологий при обработке персональных данных только становится предметом научных исследований.

Проблемам публично-правового регулирования в сфере использования цифровых технологий при обработке персональных данных посвящены отдельные работы таких исследователей, как: И.Л. Бачило, М.В. Бундин, Н.И. Джафарова, М.Б. Добробаба, Г.Г. Камалова, А.А. Лазаров, Э.И. Лескина, А.В. Минбалеев, В.Б. Наумов, Н.И. Петрыкина, А.И. Савельев, С.В. Соловкин, Э.В. Талапина и др.

Правоотношения, связанные с развитием правового регулирования процесса обработки персональных данных как элемента системы цифрового профилирования, стали предметом изучения В.В. Игумнова и С.Е. Чаннова.

Информационно-правовая проблематика, связанная с публично-правовым регулированием в сфере использования цифровых технологий при обработке персональных данных, привлекает научное внимание зарубежных учёных. Основными иностранными исследователями данной темы являются: Л. Байгрэйва, К. Беннета, К. Гринлифа, К. Миллард, Ч. Рааба, А. Уэстина и др.

При этом до настоящего времени в отечественной науке не прорабатывался вопрос, посвящённый исследованию публично-правового регулирования в сфере использования комплекса современных цифровых технологий при обработке персональных данных. Смежные научные исследования проводились преимущественно либо по поводу персональных данных вообще, либо по поводу специальных правовых средств, которые применяются в области цифровых технологий, безотносительно специфики их применения в процессе обработки персональных данных.

Объектом диссертационного исследования являются общественные отношения, возникающие в процессе использования цифровых технологий при обработке персональных данных.

Предметом диссертационного исследования является совокупность публично-правовых норм, регулирующих общественные отношения по поводу использования цифровых технологий при обработке персональных данных, а также правоприменительная практика и научная доктрина по исследуемой тематике.

Цель диссертационного исследования заключается в разработке и обосновании концептуальных теоретических основ публично-правового регулирования использования цифровых технологий при обработке персональных данных, а также в выработке подходов и предложений по совершенствованию российского законодательства в рассматриваемой сфере.

Для достижения цели определены задачи диссертационного исследования:

– раскрыть понятие и определить правовую природу персональных данных как объекта публично-правового регулирования;

– выявить специфику правовой природы использования цифровых технологий при обработке персональных данных;

– определить особенности правового обеспечения использования цифровых технологий при обработке персональных данных;

– установить особенности публично-правового регулирования в сфере использования искусственного интеллекта при обработке персональных данных;

– обосновать специфику публично-правового регулирования в сфере использования технологий распределённого реестра при обработке персональных данных;

– выявить особенности публично-правового регулирования в сфере использования облачных технологий при обработке персональных данных;

– раскрыть этико-правовые проблемы публично-правового регулирования обработки персональных данных с использованием цифровых технологий и предложить пути их решения;

– изучить проблемы публично-правового регулирования обработки специальной категории персональных данных – персональных данных, составляющих врачебную тайну, при использовании цифровых технологий;

– выявить проблемы и определить приоритетные направления развития института административной ответственности в области нарушения требований законодательства о персональных данных.

Выполнение этих задач позволит достичь цели исследования и сформировать полное и всестороннее представление о публично-правовом регулировании использования цифровых технологий при обработке персональных данных.

Теоретическая основа диссертационного исследования представляет собой совокупность трудов учёных в области теории государства и права, информационного права, а также других отраслевых юридических наук, в частности работы таких исследователей, как: Е.Н. Абанина, М.И. Абдулаев, О.Ю. Авдевнина, А.Б. Агапов, Р.В. Амелин, В.В. Архипов, С.С. Алексеев, Ю.М. Батурин, И.Л. Бачило, М.В. Бундин, А.Б. Венгеров, Г.А. Грищенко, Н.И. Джафарова, М.Б. Добробаба, М.О. Дьяконова, В.В. Игумнов, А.А Лазаров, А.А. Ефремов, М.А. Ефремова, М.С. Журавлева, В.М. Жуйков, С.С. Завриев, О.А. Зайцев, С.М. Зубарев, О.С. Иоффе, А.Г. Истратова, Г.Г. Камалова, С.А. Комаров, В.А. Копылов, Б.В. Кристальный, Н.В. Кроткова, Э.И. Лескина, А.А. Малюк, А.В. Мартынов, А.В. Минбалеев, В.Б. Наумов, Т.А. Полякова, Н.И. Петрыкина, А.В. Попова, И.М. Рассолов, А.И. Савельев Л.А. Сергиенко, С.В. Соловкин, Э.В. Талалпина, Л.К. Терещенко, Е.В. Холодная, С.Е. Чаннов, А.Ф. Черданцев, С.Г. Чубукова, В.М. Шафиров, Л.С. Явич и др.

Методологическая основа диссертации представляет собой совокупность используемых как общенаучных (анализ, синтез, аналогия, метод системного анализа), так и специальных методов познания. Комплексность применения различных методов обусловлена целью и задачами исследования, характером отношений, складывающихся в сфере публично-правового регулирования использования цифровых технологий при обработке персональных данных.

Использование общенаучных методов познания обеспечило возможность комплексного исследования отношений, составляющих объект диссертационного исследования, в их развитии, целостности и взаимосвязи с иными отношениями. Кроме того, применение метода системного анализа позволило полноценно

изучить отношения по обработке персональных данных как системные явления, пребывающие в стремительном динамическом развитии, с позиции как юридической науки, так и иных общественных и технических наук.

При осуществлении диссертационного исследования также были использованы специальные юридические методы познания, а именно: историко-правовой метод, формально-юридический метод, сравнительно-правовой метод и другие.

Сравнительно-правовой метод применялся в ходе сопоставления отечественного подхода к правовому регулированию отношений в области персональных данных, а также использования цифровых технологий в процессе обработки персональных данных с наиболее интересными зарубежными подходами в данной сфере, позволив достичь тем самым определённых научных результатов.

Историко-правовой метод обеспечил исследование правовых вопросов обработки персональных данных не только в рамках их современного состояния, но и с точки зрения их прошлого и прогнозируемого будущего.

Формально-юридический метод использовался при выработке определений, в том числе для определения понятия «персональные данные», а также в рамках анализа сложившейся системы способов обработки персональных данных для установления актуального правового содержания исследуемых правовых явлений. Его применение обеспечило изучение правовой природы рассматриваемых в работе отношений и разработку предложений по формированию и развитию моделей развития публично-правового регулирования отношений в сфере использования цифровых технологий в процессе обработки персональных данных.

Нормативную основу исследования составили международные, зарубежные и российские нормативные правовые акты, регулирующие отношения в сфере персональных данных, в том числе положения Конституции РФ, общепризнанные принципы и нормы международного права, международные договоры, федеральное законодательство, подзаконные акты, а также нормативные

правовые акты зарубежных государств и межгосударственных объединений, в частности США, ЕС, Китая и других.

Эмпирическая база исследования включает в себя материалы правоприменительной практики, материалы из официальных источников государственных органов и подведомственных им организаций, данные аналитических исследований, в том числе полученные из открытых источников.

Научная новизна исследования заключается в том, что впервые были выявлены и сформированы концептуальные теоретические основы публично-правового регулирования использования современных цифровых технологий при обработке персональных данных в условиях экономики данных и цифровой трансформации государства. В рамках исследования публично-правового регулирования использования цифровых технологий при обработке персональных данных сформулирована авторская позиция относительно ключевых правовых понятий в данной области, а также представлены основные направления по дальнейшему совершенствованию правового института персональных данных. Также были выявлены проблемы и определены перспективные направления развития публично-правового регулирования использования цифровых технологий при обработке персональных данных.

На защиту выносятся следующие основные положения, представляющие собой наиболее значимые и теоретически обоснованные результаты диссертационного исследования, в которых содержится новизна или элементы научной новизны:

1. Доказано, что распространение, предоставление и доступ к персональным данным должны рассматриваться не как составляющие передачи персональных данных, а в качестве самостоятельных действий в рамках обработки персональных данных. В связи с этим в целях повышения эффективности института обработки персональных данных, совершенствования законодательства о персональных данных и обеспечения прав субъектов персональных данных предложено скорректированное определение «обработка персональных данных», под которым следует понимать «любое действие (операцию) или совокупность действий

(операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, распространение, предоставление, доступ, обезличивание, блокирование, удаление и уничтожение персональных данных».

2. В целях обеспечения защиты прав субъектов персональных данных, с учётом расширения процессов цифровизации в современном государстве и обществе, предложена специальная информационно-правовая презумпция относимости данных к персональным данным физического лица: «Любую информацию следует относить к числу персональных данных, если субъект этой информации заявляет о том, что данная информация определяет или позволяет его определить (идентифицировать). Обязанность по доказыванию обстоятельств, свидетельствующих об обратном, возлагается на лицо, осуществляющее обработку персональных данных».

3. Выявлены и обоснованы правовые признаки, которым должны отвечать сведения, относящиеся к персональным данным, в качестве обязательных в процессе их отнесения к таковым:

– возможность определить конкретного субъекта по данным;

– возможность связать данные для соотношения информации и субъекта;

– возможность произвести умозаключение, что данные принадлежат конкретному субъекту;

– возможность обособления конкретных персональных данных друг от друга;

– персональные данные должны отвечать всем вышеуказанным признакам одновременно.

4. Обосновано, что введение полного запрета на обработку персональных данных с использованием искусственного интеллекта приведёт к фактическому блокированию любых разработок, связанных с развитием и внедрением искусственного интеллекта. Ввиду этого предлагается нормативное закрепление

обязанности получения специального согласия на обработку персональных данных при использовании искусственного интеллекта.

Доказано, что обезличивание персональных данных выступает методом снижения рисков нарушения прав субъектов персональных данных при обработке данных с использованием искусственного интеллекта, но само по себе не может обеспечивать абсолютные гарантии защиты прав субъектов персональных данных. Обезличенные данные содержат в себе цифровые следы, по которым с использованием технологий искусственного интеллекта возможно установить их соответствие тому или иному субъекту персональных данных.

5. В целях минимизации рисков, связанных с обеспечением контроля над кругом субъектов, которые могут получить доступ к персональным данным при использовании технологии блокчейн и иных схожих технологий, обоснована необходимость законодательного закрепления обязанности применения операторами персональных данных специальных мер, направленных на реализацию возможности эффективного уничтожения персональных данных в блокчейне (чтобы после удаления на одном устройстве данные становились неразборчивыми для идентификации любого, кто может получить доступ к данным по цепочке хранения), например с помощью шифрования и удаления ключей дешифрования.

6. Предложены правовые признаки, определяющие законность установки и универсального использования средств фотовидеофиксации гражданами в части недопустимости нарушения требований обработки персональных данных.

Для признания правомерности установки средств фотовидеофиксации (камер и других средств) необходимо соблюдение совокупности условий:

– средство фотовидеофиксации установлено для целей охраны имущества, жизни и здоровья;

– средство фотовидеофиксации установлено на личной территории;

– средство фотовидеофиксации не направлено на территорию и имущество другого лица как на главный объект съёмки;

– данные, полученные со средств фотовидеофиксации, не нарушают неприкосновенность частной жизни, личную и семейную тайну.

Соответствующие правовые признаки целесообразно закрепить в рамках приказа Роскомнадзора как уполномоченного органа в контексте обобщения практики осуществления государственного контроля (надзора) в области персональных данных.

7. Сформулированы предложения, направленные на закрепление специального правового регулирования функционирования публичных облаков, которые позволят установить публично-правовую основу регулирования деятельности владельцев публичных облаков, а также разграничить и нормативно закрепить формы публичных облаков.

Обосновано, что действующее нормативно-техническое регулирование применения публичных облаков не позволяет должным образом определить термин «публичное облако». В связи с этим предложено правовое определение понятия «публичное облако», в качестве которого следует понимать «услугу, позволяющую пользователю обеспечить обработку, хранение, управление и резервное копирование данных с помощью предоставления доступа к сервисам сервера, программному обеспечению и техническим средствам». Выявлено, что основными формами применения публичных облаков в публичных целях являются: программное обеспечение как услуга; платформа как услуга; инфраструктура как услуга; рабочее место как услуга.

8. Разработаны предложения по развитию модели административной ответственности за нарушения законодательства о персональных данных. Выявлена проблема частичного пересечения двух составов административных правонарушений (статьи 13.14 и 13.14.1 Кодекса Российской Федерации об административных правонарушениях), в связи с чем предложен вариант её устранения путём введения единой статьи 13.14 Кодекса Российской Федерации об административных правонарушениях в новой редакции, которая будет предусматривать два самостоятельных состава административного правонарушения.

В частности, обосновано, что административно наказуемыми станут все незаконные действия по получению и (или) распространению информации, доступ к которой ограничен федеральным законом, за исключением случаев, предусмотренных статьей 5.53, частями 1–2.1, 10–18 статьи 13.11, статьей 14.29, частью 5 статьи 15.19, частью 2 статьи 17.13 Кодекса Российской Федерации об административных правонарушениях, если эти действия не содержат признаков уголовно наказуемого деяния. Также предложен дополнительный квалифицирующий состав административного правонарушения, в рамках которого будет установлена административная ответственность за незаконные действия по получению и (или) распространению информации, доступ к которой ограничен федеральным законом, совершённые должностным лицом (лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 и статьей 17.13 Кодекса Российской Федерации об административных правонарушениях), за исключением случаев, если эти действия не содержат признаков уголовно наказуемого деяния.

Теоретическое значение данного исследования состоит в формировании комплексного представления о современном доктринальном, практическом и законодательном опыте и стратегиях развития в рамках проблемы публично-правового регулирования использования цифровых технологий при обработке персональных данных, на основе чего сформулированы определённые выводы и предложения, которые могут быть использованы в науке информационного права, а также в области профильных исследований правовой охраны и регулирования персональных данных.

Практическая значимость данного исследования заключается в том, что научное исследование проблем публично-правового регулирования использования цифровых технологий при обработке персональных данных может оказать влияние на оценку существующих положений и норм в сфере обработки персональных данных, что способно поменять действующую правоприменительную практику при применении разработок, предложений и рекомендаций, сформулированных в

рамках настоящего исследования и направленных на изменение существующего правового регулирования соответствующих аспектов. Предложения могут использоваться в правоприменительной практике государственных органов, в том числе Роскомнадзором и судами Российской Федерации.

Кроме того, исследование направлено на реализацию целей и задач в рамках Национального проекта «Экономика данных и цифровая трансформация государства», а также для цели реализации Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы.

Результаты исследования могут быть использованы в учебном процессе для подготовки и преподавания курсов публично-правовых дисциплин, касающихся актуальных проблем информационного права, и смежных дисциплин.

Степень достоверности результатов исследования. Основные выводы, представленные в диссертации, подтверждены с помощью научных методов познания, логично обоснованы с опорой на данные российских и зарубежных исследователей, конституционное и отраслевое законодательство, юридическую практику. Достоверность подтверждается использованием достаточного количества доктринальных источников, а также нормативных правовых актов и судебной практики. Кроме того, достоверность результатов подтверждается их апробацией.

Апробация результатов исследования. Ключевые результаты проведенного исследования отражены в 8 научных публикациях, из них 3 – в рецензируемых изданиях, включенных в Перечень ВАК при Минобрнауки России.

Выносимые на публичную защиту положения прошли апробацию на ряде международных и всероссийских научно-практических конференций, круглых столов и семинаров, в том числе на: V и VI Международной научно-практической конференции «Бачиловские чтения» в ИГП РАН (г. Москва, 2022 г.; 2023 г.); VI Всероссийской ежегодной научно-практической конференции «Информационная безопасность и дети» (г. Москва, 2022 г.); на I и II Международной научно-практической конференции «Цифровые технологии и право» в рамках Международного форума Kazan Digital Week (г. Казань,

2022 г.; 2023 г.); на II Международной научно-практической аспирантской конференции памяти В.Ф. Яковлева в ВШП ИГСУ (г. Москва, 2022 г.); на XII Московской юридической неделе I Международного форума «Киберправо и кибербезопасность» (г. Москва, 2022 г.); на VII Всероссийской ежегодной научно-практической конференции «Информационная безопасность и дети: формирование культуры информационной безопасности участников образовательных отношений» (г. Москва, 2023 г.); на X Московском юридическом форуме (МЮФ) по теме «Фундамент устойчивого развития» (г. Москва, 2023 г.); на XXIV Международной научно-практической конференции «Кутафинские чтения» Московского государственного юридического университета имени О.Е. Кутафина (МГЮА) и XXIV Международной научно-практической конференции юридического факультета Московского государственного университета имени М.В. Ломоносова (г. Москва, 2023 г.); на Ежегодной международной научно-практической конференции МГУ «Правовые основы информационного общества: цифровая экономика, информационная безопасность, искусственный интеллект» (г. Москва, 2023 г.); на VII Международной конференции «Актуальные проблемы информационного права» МГУ ВШГА (г. Москва, 2024 г.); на Международной научно-практической конференции «Современные правовые модели регулирования искусственного интеллекта» (г. Москва, 2024 г.); на XI Московском юридическом форуме «Формирование многополярного мира: вызовы и перспективы» (г. Москва, 2024 г.); на Международной научно-практической конференции СЮФ, International (г. Ереван, 2024 г.); на XX Международном фестивале «НАУКА 0+» юридического факультета Московского государственного университета имени М.В. Ломоносова (г. Москва, 2025 г.).

Структура диссертации обусловлена целью и задачами исследования и состоит из введения, трёх глав, включающих девять параграфов, а также заключения и библиографического списка источников и использованной литературы.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПУБЛИЧНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

§ 1. Персональные данные: понятие и правовая природа

Персональные данные при рассмотрении в качестве правовой категории являются сложным правовым явлением, по поводу которого применяются специальные нормы различной отраслевой принадлежности. Обращая своё внимание на само понятие данной правовой категории, можно в наиболее общем виде обобщить, что когда мы ведём речь о персональных данных, то подразумеваем что-то личное, индивидуальное, возможно уникальное. Такую характеристику мы можем привести, поскольку складывается устойчивое представление о том, что персональные данные относятся непосредственно к нам как персоне, к нашему лицу, внешнему облику, фамилии, имени и отчеству, а также к иным подобным данным. Термин «персональный» происходит от латинского слова persōna – личность, личный, присущий каждому отдельному индивидууму[2].

На данный момент в мире быстроразвивающихся технологий сложно не только с теоретико-правовой, но и с сугубо правоприменительной точки зрения определиться с достоверной точностью относительно вопроса о том, что и в какой ситуации будет являться персональными данными, а что нет.

Термин «персональные данные» тесно связан с понятиями «личная информация», «приватная информация», «конфиденциальная информация», «тайна».

Явление приватности до конца не концептуализировано. Как пишут Т.И. Пороховская, А.А. Малюк, О.Ю. Полянская и И.Ю. Алексеева, данное явление

---

[2] Словарь иностранных слов, вошедших в состав русского языка: Материалы для лексической разработки заимствованных слов в рус. лит. речи: С портр. и краткой биогр. А.Н. Чудинова / сост. под ред. А.Н. Чудинова. – 3-е изд., тщательно испр. и знач. доп. (более 5000 новых слов) преимущественно соц.-полит. терминами, вошедшими в жизнь в последние годы. – СПб., 1910. – С. 423.

касается тех сфер жизни человека, о которых обычно известно только самым близким людям и друзьям[3].

Исторически право на приватность стало зарождаться с опубликованной работой выдающихся американских юристов конца XIX века С. Уоррена и Л. Брандайса (судья Верховного Суда), а именно статьи «Право на приватность»[4], в которой учёные сформулировали, что право «быть оставленным в уединении» должно признаваться в качестве самостоятельной правовой категории[5]. В дальнейшем развитие данной области права получило благодаря принятию Европейской конвенции о защите прав человека и основных свобод, вступившей в силу в 1953 году.

В русском языке понятие «приватность» идентично выражению «неприкосновенность частной и личной жизни». В юридической литературе термины «частная жизнь» и «личная жизнь» рассматриваются как синонимы[6]. То есть частная и личная жизнь – это и есть приватность.

В Конституции Российской Федерации[7] право на приватность нормативно закреплено в статье 23, в соответствии с которой «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени… на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений».

---

[3] См.: Пороховская Т.И. Концепт приватности: нормативное содержание в сфере межличностных отношений // Учёные записки Крымского федерального университета имени В.И. Вернадского. Социология. Педагогика. Психология. – 2014. – № 1. – С. 7; Малюк А.А. Этика в сфере информационных технологий. / А.А. Малюк, О.Ю. Полянская, И.Ю. Алексеева. – М.: Горячая линия–Телеком, 2011. – С. 76.

[4] Уоррен С., Брендейс Л.Д. Право на приватность. [Электронный ресурс]. Режим доступа: http://rus.triz–guide.com/1662.html, свободный (дата обращения: 01.06.2025).

[5] Сербин Д.С. Право на приватность в концепции Сэмюэла Уоррена и Луиса Брандейса // Взаимодействие институтов власти и общества в сфере защиты прав человека: Материалы VIII международной научно-практической конференции аспирантов, преподавателей, практических работников. Саратов, 1–2 июля 2015 года. – Саратов: Саратовский источник, 2015. – С. 179.

[6] Зверева Е.А. Правовой режим информации в отношениях с участием субъектов предпринимательской деятельности: монография. – М.: Юстицинформ, 2008. – С. 43.

[7] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).

Исследуя соотношение понятий «частная жизнь» и «персональные данные», российские учёные (А.М. Лушников[8], И.Л. Бачило, Л.А. Сергиенко, Б.В. Кристальный, А.Г. Арешев[9]) отмечают, что «персональные данные» как более узкое понятие входят в состав понятия «частная жизнь».

И.Л. Бачило указывала, что персональными данными являются сведения о личности, включенные в информационную систему государственных, общественных и частных, корпоративных организаций по инициативе гражданина или в силу закона[10]. А.И. Бычков[11] и М.Б. Добробаба отмечают в своих исследованиях проблему правовой трансформации правопонимания персональных данных, понятие стало гораздо шире и абстрактнее, что не позволяет чётко дифференцировать информацию и безошибочно определить возможность отнесения ее к персональным данным[12]. Изучаемый в настоящей научной работе вопрос соотношения категорий «информация» и «данные» поднимает в своих трудах Э.И. Лескина[13], что отдельно подчеркивает актуальность проблематики и интерес научного сообщества к изучаемой теме.

При наличии тех или иных обстоятельств субъект персональных данных может ограничить их использование, и данная информация уже будет рассматриваться как конфиденциальная, то есть охватываемая режимом той или иной тайны (например, коммерческой, профессиональной, медицинской), что демонстрирует гибкость режима персональных данных[14].

Персональные данные являются одной из составляющих частной жизни и подчиняются правовому принципу приватности (неприкосновенность частной

---

[8] Лушников А.М. Защита персональных данных работника: сравнительно-правовой комментарий гл. 14 Трудового кодекса РФ // Трудовое право. – 2009. – № 9. – С. 97.

[9] Персональные данные в структуре информационных ресурсов. Основы правового регулирования / И.Л. Бачило, Л.А. Сергиенко, Б.А. Кристальный, А.Г. Арешев. – Минск: Беллітфонд, 2006. – С. 296.

[10] Бачило И.Л. Информационное право РФ: учеб. для вузов. 2-е изд. – М.: Юрайт, 2011. – С. 351.

[11] Бычков А.И. Категории персональных данных // СПС «КонсультантПлюс».

[12] Добробаба М.Б. Понятие персональных данных: проблема правовой определённости // Вестник Университета имени О.Е. Кутафина. – 2023. – № 2 (102). – С. 45–46.

[13] Лескина Э.И. Понятие и объект оборота данных // Законодательство. – 2025. – № 3. – С. 42–49.

[14] Минбалеев А.В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 2 (14). – С. 7.

жизни). Такой вывод следует из анализа отечественной и зарубежной литературы. Противоречия между понятиями «персональные данные», «частная жизнь» и «приватность» не возникает, они взаимодополняют друг друга, формируя вертикальную, иерархическую правовую систему принципов и норм, регулирующих обработку персональных данных.

Юридически термин «персональные данные» сформировался в XX в. Первый в мире закон о защите персональных данных был принят в 1970 г. в Германии, в земле Гессен [15] . Первым международным документом в области защиты персональных данных стала «Конвенция о защите физических лиц при автоматизированной обработке персональных данных», принятая в 1981 г. в Страсбурге.

В статье 2 Конвенции о защите физических лиц при автоматизированной обработке персональных данных 1981 г. (далее – Конвенция 1981 г.) [16] персональные данные определяются как информация, которая касается конкретного или могущего быть идентифицированным лица («субъекта данных»). Вместе с тем в статье 6 данной Конвенции перечислены особые категории персональных данных, которые могут быть подвергнуты автоматической обработке только при наличии надлежащих гарантий, предусмотренных национальным правом. Особую категорию составляют сведения, раскрывающие национальную принадлежность, политические взгляды, религиозные или иные убеждения, персональные данные о здоровье или сексуальной жизни, сведения о судимости.

---

[15] Талапина Э.В. Эволюция прав человека в цифровую эпоху // Труды Института государства и права РАН. – 2019. – № 3. – Т. 14. – С. 122–146; Талапина Э.В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права РАН. – 2018. – Т. 13. – № 5. – С. 117–150.

[16] «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» (Заключена в г. Страсбурге 28 января 1981 г.) // Официальный интернет-портал правовой информации. [Электронный ресурс]. Режим доступа: http://www.pravo.gov.ru, свободный (дата обращения: 01.06.2025).

Согласно определению, изложенному в Европейском законе о защите данных (далее – GDPR)[17], персональные данные определяются как любая информация, относящаяся к физическому лицу, называемому субъектом данных, позволяющая идентифицировать его. Эта информация может быть непосредственно связана с человеком, например его имя или местонахождение, или косвенно связана с ним через такие идентификаторы, как физические, генетические или социальные характеристики.

В этой связи следует особо отметить один из важнейших признаков правовой категории «персональные данные» в рамках единой правовой системы ЕС, а именно то, что ключевым квалифицирующим признаком для констатации факта наличия в данном конкретном случае персональных данных будет возможность осуществления с помощью этих сведений (которые как раз и составляют содержание персональных данных) функции по идентификации субъекта персональных данных. Вопросы понятия персональных данных в Европейском союзе также изучал А.Г. Мираев[18].

Для более точного определения относимости данных к персональной информации в статье 29 GDPR предусмотрены конкретные стандарты, которым должны отвечать персональные данные. К числу таких стандартов относятся: возможность определить человека по данным; связать данные с какой-то информацией в сети для соотношения информации и человека; возможность произвести умозаключение, что данные принадлежат конкретному человеку.

Согласно статье 4 Закона КНР о защите личной информации[19] персональной информацией являются все виды информации, записанные с помощью

---

[17] Общий регламент по защите данных от 27 апреля 2016 г., или GDPR (General Data Protection Regulation), или Регламент ЕС 2016/679. [Электронный ресурс]. Режим доступа: https://ogdpr.eu/ru/gdpr-2016-679, свободный (дата обращения: 01.06.2025).

[18] Мираев А.Г. Понятие персональных данных в Российской Федерации и Европейском союзе // Юридическая наука. – 2019. – № 5. Режим доступа: https://cyberleninka.ru/article/n/ponyatie-personalnyh-dannyh-v-rossiyskoy-federatsii-i-evropeyskom-soyuze, свободный (дата обращения: 07.11.2025).

[19] Personal Information Protection Law of the People’s Republic of China (PIPL) от 2021 года. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1716804666&tld=ru&lang=en&name=Personal-Information-

электронных или иных средств, относящейся к определённому или определяемому физическому лицу, за исключением информации после применения технологий анонимизации.

Определения синонимичны и в целом повторяют концептуальное определение Конвенции 1981 года.

Впервые понятие «персональные данные» как правовая категория российского законодательства было введено Федеральным законом от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации»[20] и с самого начала было отнесено к категории конфиденциальных данных. В Перечне сведений конфиденциального характера[21] в качестве конфиденциальных сведений также указаны персональные данные.

Исходя из правового определения, установленного основным законом Российской Федерации, регулирующим отношения, связанные с персональными данными, а именно Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ (далее – Федеральный закон № 152-ФЗ), персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных)[22].

В Федеральном законе № 152-ФЗ предусмотрены также «специальные категории персональных данных», к которым относятся сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, об интимной жизни (п. 1 ст. 10 Федерального закона № 152-ФЗ) и «биометрические» – сведения,

---

Protection-Law-of-the-Peoples-Republic-of-China.pdf&text=Personal+Information+Protection+Law+of+the+People's+Republic+of+China+%28PIPL%29+от+2021+года&url=https%3A//www.china-briefing.com/news/wp-content/uploads/2021/08/Personal-Information-Protection-Law-of-the-Peoples-Republic-of-China.pdf&lr=43&mime=pdf&l10n=ru&sign=15649ac8fa4b45020874e2c17035c280&keyno=0, свободный (дата обращения: 01.06.2025).

[20] Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» (утратил силу) // Собрание законодательства РФ. – 1995. – № 8. – Ст. 609.

[21] Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера» // Собрание законодательства РФ. – 1997. – № 10. – Ст. 1127.

[22] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.

характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность (п. 1 ст. 11 Федерального закона № 152-ФЗ) [23].

Вопрос о квалификации информации в качестве персональных данных стал зависеть от конкретных обстоятельств и возможных взаимосвязей между различного рода фрагментами информации[24].

То есть вся информация, которая как-либо может характеризовать личность, может быть отнесена к персональным данным, подпадать под действие и регулироваться в соответствии с нормами Федерального закона № 152-ФЗ. Анализ зарубежных законов и норм позволяет сделать вывод, что главным в определении категории «персональные данные» является то, что с их помощью можно понять, что они относятся к конкретному субъекту персональных данных, а также то, что эти данные обрабатываются любым способом, будь то электронный, на бумаге или любой иной.

Таким образом, по итогам сравнительно-правового исследования категории персональных данных в ЕС, Китае и России (лидерах публично-правового регулирования области обработки персональных данных) можно вполне обоснованно констатировать, что закреплённая в Федеральном законе № 152-ФЗ легальная дефиниция «персональные данные» по своему содержанию потенциально обладает расширительным толкованием и недостаточной точностью, что несколько затрудняет правоприменение в данной области для законопослушных субъектов и потенциально предоставляет недобросовестным обработчикам персональных данных возможность осуществлять противоправные действия.

Помимо этого, возникает проблема определения относимости той или иной информации к числу персональных данных в каждом конкретном случае. Для решения этих проблем предлагается воспользоваться опытом законотворчества

---

[23] Донских А.Г. Актуальные проблемы использования персональных данных в деятельности СМИ // Вестник НГУ. Серия: История, филология. – 2021. – № 6. Т. 20: Журналистика. – С. 150.
[24] Савельев А.И. Электронная коммерция в России и за рубежом: правовое регулирование: монография. – М.: Статут, 2016. – С. 34.

Европейского союза и учесть опыт Китая, выраженного в нормах Закона КНР о защите личной информации.

Предлагается авторское определение понятия «персональные данные» как любая информация о физическом лице (субъекте персональных данных), которая позволяет идентифицировать данное лицо (за исключением, если такая информация содержится в обезличенном виде), а также иная информация, напрямую названная таковой в законе.

Преимуществом такого подхода к определению понятия «персональные данные» будет уточнение ключевого признака данной правовой категории. Установленный в легальной дефиниции признак «относимости» информации к определённому или определяемому лицу будет заменён на признак «идентифицируемости». Реальная возможность идентифицировать определённое лицо в данном случае будет рассматриваться как обязательный элемент правовой связи между информацией о каком-либо лице и правовыми последствиями, вызванными тем, что данная информация будет квалифицироваться как персональные данные. Представленная позиция также поддерживается в работе С.В. Соловкина[25].

Иными словами, в качестве одного из элементов гипотезы для применения той или иной нормы в области законодательства о персональных данных будет не юридический факт «относимости информации к определённому лицу», а юридический состав в виде совокупности юридических фактов (данные должны отвечать всем указанным фактам одновременно):

– возможность определить конкретного субъекта по данным;

– возможность связать данные субъекта с какой-то информацией для соотношения информации и субъекта;

– возможность произвести умозаключение, что данные принадлежат конкретному субъекту;

---

[25] Соловкин С.В. Публично-правовое регулирование процессов автоматизированного сбора данных о человеке в условиях цифровой трансформации: дис. ... канд. юрид. наук. – М., 2024. – С. 55.

– возможность обособления конкретных персональных данных друг от друга (возможность выделить конкретного субъекта из состава массива персональных данных, поскольку для отдельного состава персональных данных могут быть отдельные требования к обработке).

Приведённая совокупность юридических признаков может рассматриваться также в качестве методики или стандартов для правовой квалификации какой-либо информации в качестве персональных данных. Такой подход определённым образом способствовал бы достижению целей развития науки информационного права и правового регулирования в области обработки персональных данных.

Помимо этого, автор считает возможным дополнительно к авторскому понятию категории «персональные данные» вывести презумпцию относимости информации о физическом лице к персональным данным. Так, любую информацию о физическом лице следует относить к числу персональных данных, если субъект этой информация определяет или позволяет его определить (идентифицировать). Обязанность по доказыванию обстоятельств, свидетельствующих об обратном, возлагается на лицо, осуществляющее обработку персональных данных.

Такие приёмы правового регулирования, как нормативное закрепление презумпций и специальных правил распределения бремени доказывания, являются эффективными правовыми средствами, позволяющими установить определённый баланс интересов между участниками правоотношений, а также баланс частных и публичных интересов в применяемой области.

В современном российском праве есть немало примеров успешного применения презумпций и специальных правил распределения бремени доказывания как взаимосвязанного комплекса правовых средств. К примеру, в области потребительского права устанавливается презумпция «некомпетентности» потребителя (презумпция отсутствия у потребителя специальных познаний о свойствах и характеристиках товара, работы или услуги) и специальное распределение бремени доказывания обстоятельств, свидетельствующих о причинах возникновения недостатков в течение гарантийного срока и срока годности. Потребитель обязан доказать лишь наличие недостатков, а обязанность

по доказыванию факта наличия обстоятельств, исключающих ответственность продавца или изготовителя, возлагается именно на самого продавца или изготовителя. В научных трудах в области потребительского права[26] применение такого взаимосвязанного комплекса правовых средств неоднократно подчёркивалось в качестве одной из важнейших правовых гарантий реального обеспечения защиты прав потребителей[27].

Аналогичный приём юридической техники был весьма эффективно использован в рамках корпоративного права: презумпция недобросовестности (недобросовестность или неразумность действий директора в определённых случаях предполагается) «соседствует» со специальным правилом распределения бремени доказывания. Бремя доказывания отсутствия нарушения обязанности директора действовать добросовестно и разумно возлагается на директора. Примечательно, что в данном случае, равно как и в случае с презумпциями в потребительском праве, соответствующие нормы были сформулированы в рамках праворазъяснительных актов Верховного Суда Российской Федерации [28] и Высшего арбитражного суда Российской Федерации [29]. Подобного же подхода Верховного Суда Российской Федерации следовало бы ожидать и в праворазъяснительных актах в области обобщения судебной практики по делам в отношении защиты персональных данных, но специальных актов судебной практики такого до настоящего момента Верховный Суд Российской Федерации не разработал.

Наиболее ярким примером применения такого юридического приёма является установленная в Конституции Российской Федерации и иных

---

[26] См.: Жуйков В.М., Завриев С.С. Проблемы реализации принципов гражданского судопроизводства в правоприменительной деятельности: монография. – М.: НОРМА, ИНФРА-М, 2024. – С. 277; Шайхеев Т.И. Правовые позиции судов по экономическим спорам в примерах из судебной практики // Арбитражные споры. – 2022. – № 3. – С. 103–162.

[27] Бочкарев А.Е. Распределение бремени доказывания в гражданском процессе по спорам о качестве медицинских услуг // Медицинское право. – 2017. – № 6. – С. 5–9.

[28] Постановление Пленума Верховного Суда РФ от 28.06.2012 № 17 «О рассмотрении судами гражданских дел по спорам о защите прав потребителей» // Солидарность. – 2013. – № 31.

[29] Постановление Пленума ВАС РФ от 30.07.2013 № 62 «О некоторых вопросах возмещения убытков лицами, входящими в состав органов юридического лица» // Российская газета. – 2012. – № 156.

законодательных актах презумпция невиновности. Являясь трёхсоставной правовой категорией, презумпция невиновности объединяет в себе три составляющие, в том числе и правило о специальном распределении бремени доказывания: лицо, привлекаемое к ответственности, не должно доказывать свою невиновность, а все неустранимые сомнения в виновности трактуются в пользу невиновности.

Общим признаком для обоснования необходимости всех вышеприведённых презумпций является охраняемая законом потребность защитить интересы слабой стороны правоотношений: потребитель – в законодательстве о защите прав потребителей; юридическое лицо – в корпоративных правоотношениях; обвиняемый – в правоотношениях по привлечению к уголовной ответственности.

Таким образом, применение в правоотношениях, связанных с правовым регулированием персональных данных, презумпции относимости информации о физическом лице к персональным данных, в совокупности со специальными правилами распределения бремени доказывания (перенесение бремени доказывания с субъекта персональных данных на оператора), позволит установить реальный правовой механизм обеспечения баланса интересов в общественных отношениях при обработке персональных данных. Предложенный в настоящем труде взаимосвязанный комплекс правовых средств, по существу, стал бы полноценной правовой гарантией защиты охраняемых законом общественных отношений в области персональных данных.

Для цели развития технологий исключением должны быть данные после применения технологий анонимизации, при условии выполнения всех разумных мер по недопущению персонализации данных путём надёжного шифрования и других способов защиты данных от деанонимизации. Соответствующие технологии и разумные меры по недопущению персонализации данных должны быть определены и рекомендованы Минцифры России для цели обеспечения должного уровня информационной безопасности.

Преимущества предложенного автором подхода понимания персональных данных будут проявляться в различных аспектах.

Во-первых, в этом случае возможно будет точно отделить ту информацию, которая составляет собой персональные данные, от иной информации.

Во-вторых, из числа персональных данных будет исключена информация, обрабатываемая на основе технологии обезличивания персональных данных. Существующая сейчас легальная дефиниция не позволяет однозначно сделать такой важный для науки и практики вывод. Это выведет реальные статистические исследования, скрининг уязвимостей IT-продуктов, cookie-файлы из категорий обработки и передачи персональных данных, но только при условии их анонимизации, шифрования и правового закрепления иных требований к разумным мерам по недопущению персонализации данных.

Кроме вышесказанного, важно отметить, что законодательство предусматривает разные категории данных и в зависимости от категории устанавливает определённый уровень внимания и охраны к данным [30]. Так, отечественное законодательство (Федеральный закон № 152-ФЗ и Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление № 1119)) [31] предусматривает четыре категории обрабатываемых персональных данных, это:

– общедоступные;

– биометрические;

– специальные;

– иные.

К общедоступным категориям персональных данных в соответствии с абз. 3 п. 5 Постановления № 1119, а также в силу ст. 8 Федерального закона № 152-ФЗ

---

[30] Право персональных данных: учебник / [Е.В. Холодная, Е.В. Дженакова, А.А. Селюк и др.]; под ред. А.В. Минбалеева; Московский государственный юридический университет имени О.Е. Кутафина (МГЮА). – Саратов: Амирит, 2023. Режим доступа: https://search.rsl.ru/ru/record/01012589426?ysclid=mhur61rhjq90503672, свободный (дата обращения: 11.11.2025).

[31] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства РФ. – 2012. – № 45. – Ст. 6257.

могут относиться определённые данные, на которые субъект персональных данных дал согласие на обработку и нахождение их в общедоступном источнике. К числу таких общедоступных источников относятся справочники и адресные книги.

В качестве примеров общедоступных персональных данных вышеуказанные нормы приводят следующие сведения: ФИО гражданина, сведения о месте и времени рождения, адрес проживания, контактные данные, информация о профессии и т. п. В судебной практике и разъяснениях Роскомнадзора к подобным данным могут относить ИНН, СНИЛС [32], номер мобильного телефона [33], электронную почту, IP-адрес пользователя сети «Интернет» [34], номер личного автомобиля и другие данные, которые косвенно или прямо относятся к субъекту персональных данных.

В соответствии со ст. 10 Федерального закона № 152-ФЗ и абз. 1 п. 5 Постановления № 1119 к специальным категориям персональных данных относятся сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни[35].

---

[32] Апелляционное определение Санкт-Петербургского городского суда от 03.02.2015 № 33–1644/2015 по делу № 2-3097/2014. [Электронный ресурс]. Режим доступа: https://sankt-peterburgsky--spb.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=39162742&delo_id=5&new=5&text_number=1, свободный (дата обращения: 01.06.2025).

[33] Решение Черемушкинского районного суда города Москвы от 18.06.2019 по делу № 12–973/2019. [Электронный ресурс]. Режим доступа: https://mos-gorsud.ru/rs/cheryomushkinskij/cases/docs/content/e7b8a497-09c7-4d1d-a7f9-5827f76d6a20, свободный (дата обращения: 01.06.2025); Определение Судебной коллегии по гражданским делам Верховного Суда РФ от 01.08.2017 № 78–КГ17–45. [Электронный ресурс]. Режим доступа: https://vsrf.ru/lk/practice/stor_pdf/1570148, свободный (дата обращения: 01.06.2025).

[34] Постановление Второго арбитражного апелляционного суда от 08.08.2019 № 02АП.5517/2019 по делу № А31–3955/2019. [Электронный ресурс]. Режим доступа: https://kad.arbitr.ru/Kad/PdfDocument/973f0e30-b841-4f1b-bc4e-d717e5ac05f0/033676ef-2a40-4da5-abe9-172a21f899b7/A31-3955-2019_20190808_Postanovlenie_apelljacionnoj_instancii.pdf, свободный (дата обращения: 01.06.2025).

[35] Постановление Конституционного суда РФ от 13.07.2022 № 31–П «По делу о проверке конституционности пунктов 11 и 12 части 1 статьи 79 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» в связи с жалобой гражданки Ф.». [Электронный ресурс]. Режим доступа: https://1jur.ru/?btx=9129238&utm_campaign=refer_law.ru_content_link_native_middle&utm_content

В соответствии со ст. 11 Федерального закона № 152-ФЗ и абз. 3 п. 5 Постановления № 1119 к биометрическим категориям персональных данных относятся сведения о физиологических и биологических особенностях человека, которые позволяют установить его личность, но не относятся к специальным категориям персональных данных. Например, ДНК [36] и отпечатки пальцев [37]; образцы голоса[38], данные, полученные посредством фото- и видеосъёмки[39].

В соответствии с абз. 4 п. 5 Постановления № 1119 выделяются иные категории персональных данных и являются данными, которые не относятся к общедоступным, специальным или биометрическим. Например, данные, полученные с помощью системы глобального позиционирования (GPS),

---

=art&utm_medium=refer&utm_source=law.ru&utm_term=21946#/document/96/351179800, свободный (дата обращения: 01.06.2025).

[36] Marper v. The United Kingdom, постановление от 04.12.2008, жалобы № 30562/04 и № 30566/04. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1716807514&tld=ru&lang=ru&name=ECHR_S_and_Marper_v_The_United_Kingdom_04_12_2008.pdf&text=2+S.+and+Marper+v.+The+United+Kingdom%2C+постановление+от+04.12.2008%2C+жалобы+№+30562/04+и+№+30566/04&url=https%3A//europeancourt.ru/uploads/ECHR_S_and_Marper_v_The_United_Kingdom_04_12_2008.pdf&lr=43&mime=pdf&l10n=ru&sign=bdc4cb0b583ecd92765baf9b340afd57&keyno=0, свободный (дата обращения: 01.06.2025).

[37] Leander v. Sweden, постановление от 27.03.1987, жалоба № 9248/81. § 48. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1716807357&tld=ru&lang=en&name=?library=ECHR&id=001-57519&filename=CASE%20OF%20LEANDER%20v.%20&text=Leander+v.+Sweden%2C+постановление+от+27.03.1987%2C+жалоба+№+9248/81.+§+48&url=https%3A//hudoc.echr.coe.int/app/conversion/docx/%3Flibrary%3DECHR%26id%3D001-57519%26filename%3DCASE%2520OF%2520LEANDER%2520v.%2520&lr=43&mime=docx&l10n=ru&sign=0d2bd274ed2f7f8d9b2a6507899e5c08&keyno=0, свободный (дата обращения: 01.06.2025).

[38] P.G. and J.H. v. The United Kingdom, постановление от 25.09.2001, жалоба № 44787/98. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1716807578&tld=ru&lang=en&name=?library=ECHR&id=002-5500&filename=002-5500.pdf&TID=ihgdqbxnfi&text=P.G.+and+J.H.+v.+The+United+Kingdom%2C+постановление+от+25.09.2001%2C+жалоба+№+44787/98&url=https%3A//hudoc.echr.coe.int/app/conversion/pdf/%3Flibrary%3DECHR%26id%3D002-5500%26filename%3D002-5500.pdf%26TID%3Dihgdqbxnfi&lr=43&mime=pdf&l10n=ru&sign=17e49dd7f8e46b8f4e74281c26cff789&keyno=0, свободный (дата обращения: 01.06.2025).

[39] Бембеева Б.С. Право на защиту персональных данных и различные категории персональных данных // Право в сфере Интернета: сб. статей / отв. ред. М.А. Рожкова. – М.: Статут, 2018. – С. 48–61; EDN VNLNWS. [Электронный ресурс]. Режим доступа: https://www.elibrary.ru/download/elibrary_36521757_34882333.pdf, свободный (дата обращения: 01.06.2025).

наблюдения за использованием Интернета, рабочих телефонов и электронной почты.

В юридической литературе обращается внимание на проблемы применения нормы Федерального закона № 152-ФЗ о специальных категориях персональных данных и необходимости расширения перечня специальных категорий[40].

С учётом развития права в сфере публичной защиты персональных данных интересным и спорным вопросом, который носит непосредственно научный и практический правоприменительный характер, является проблема отнесения сведений о наличии инвалидности к специальным категориям персональных данных.

Однозначного ответа на вопрос, относятся ли сведения о наличии инвалидности к специальным категориям персональных данных, в законе нет. Часть 1 ст. 10 Федерального закона № 152-ФЗ относит к специальным категориям персональных данных сведения, касающиеся состояния здоровья. При этом законодательно закреплено легальное определение только «здоровья» (п. 1 ч. 1 ст. 3 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 № 323-ФЗ (далее – Федеральный закон № 323-ФЗ)), но в законе не приведено термина «состояние здоровья».

Данный пробел прямого регулирования вопроса породил определённую практическую проблему; так, мнение по отнесению сведений об инвалидности к специальным категориям персональных данных у судов и Роскомнадзора разделилось. В связи с этим возникает определённый вопрос о том, относится ли разрешение данного вопроса к компетенции судов.

Согласно позиции Роскомнадзора от 02.04.2012 № 01111907234 в ответе на частное обращение, информация в листке нетрудоспособности, в том числе об установлении или изменении группы инвалидности, является сведениями о

---

[40] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика: монография. – М.: Статут, 2011. – С. 97.

состоянии здоровья субъекта персональных данных[41]. В частном ответе на запрос Роскомнадзор в октябре 2022 г. уточнил[42], что обработка справки об инвалидности по зрению подразумевает обработку специальных категорий персональных данных. Не требуется согласия на обработку персональных данных в связи с обработкой справки об инвалидности по зрению в целях реализации права такого инвалида на использование факсимильного воспроизведения собственноручной подписи. Основание обработки здесь представлено в виде ссылки на п. 2.3 ч. 2 ст. 10 Федерального закона № 152-ФЗ, а также на положения ст. 14.1 Федерального закона «О социальной защите инвалидов в Российской Федерации» от 24.11.1995 № 181-ФЗ (далее – Федеральный закон № 181-ФЗ).

Судебная практика в части разрешения споров по поводу отнесения информации о группе инвалидности к специальной категории персональных данных – немногочисленная. В вынесенных решениях суды к единой позиции не пришли. В ряде дел отмечается, что обработка данных об инвалидности подпадает под понятие обработки одной из специальных категорий персональных данных[43]. Суд указал, что нижестоящие суды обоснованно исходили из наличия в действиях предприятия нарушений требований ч. 1 ст. 10 Федерального закона № 152-ФЗ, поскольку в ходе проверки выявлено содержание данных об инвалидности в скриншотах с базы данных кадровой службы и в анкете кандидата, заполняемой при приёме на работу. При этом в других решениях суда утверждается, что инвалидность – это социальный статус. То есть к специальным категориям персональных данных данные об инвалидности не относятся[44].

---

[41] Ответ Роскомнадзора от 02.04.2012 № 01111907234. [Электронный ресурс]. Режим доступа: https://rppa.ru/_media/analitika/01shr-07432_02.04.2012.pdf, свободный (дата обращения: 01.06.2025).

[42] Справочная информация, размещённая в справочной системе «Интернет». [Электронный ресурс]. Режим доступа: https://t.me/privacyexpert/1100, свободный (дата обращения: 01.06.2025).

[43] Постановление Федерального арбитражного суда Московского округа от 01.12.2011 по делу № А40-129859/10-146-801. [Электронный ресурс]. Режим доступа: https://kad.arbitr.ru/Card/caeb1566-f034-4a31-806b-ca5c26301056, свободный (дата обращения: 01.06.2025).

[44] Постановление Пятнадцатого арбитражного апелляционного суда № 15АП-7769/2011 от 13.04.2011 по делу № А-32-2810/2011. [Электронный ресурс]. Режим доступа: https://kad.arbitr.ru/Card/3d6395b0-26ab-4a19-aff5-218daca534aa, свободный (дата обращения: 01.06.2025).

Так суд в решении по делу указал, что согласно ст. 1 Федерального закона № 181-ФЗ, инвалид – лицо, которое имеет нарушение здоровья со стойким расстройством функций организма, обусловленное заболеваниями, последствиями травм или дефектами, приводящее к ограничению жизнедеятельности и вызывающее необходимость его социальной защиты. Признание лица инвалидом осуществляется федеральным учреждением медико-социальной экспертизы.

Исходя из положений указанной статьи, следует вывод о том, что обработка данных о состоянии здоровья (степень расстройства функций организма, заболевания, дефекты и травмы) осуществляется учреждениями медико-социальной экспертизы. После присвоения группы инвалидности лицо получает статус, требующий его социальной защиты, с чем работают социальные учреждения, в том числе центры по трудоустройству. Таким образом, такую категорию персональных данных, как инвалидность, в соответствии с п. 2 ч. 2 ст. 10 Федерального закона № 152-ФЗ можно отнести к общедоступным.

На практике операторы персональных данных до сих пор принимают решение об отнесении данных об инвалидности к сведениям о состоянии здоровья в зависимости от сложившейся в компании риск-культуры. Обоснование данного поведения компаний достаточно понятное – компании идут по пути закрытия для них наибольших рисков.

Закономерным итогом отнесения сведений об инвалидности к персональным данным будет возможность применения специальных оснований для административной ответственности как по ст. 19.7 КоАП РФ[45], так и по одной из частей ст. 13.11 КоАП РФ.

В случае классификации сведений об инвалидности в качестве специальной категории персональных данных их обработка будет осуществляться в строго определённых случаях (ч. 2 ст. 10 Федерального закона № 152-ФЗ). Помимо этого, правовым следствием такого решения будет большее внимание Роскомнадзора к защите таких данных и, соответственно, повышение риска проверок

[45] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Собрание законодательства РФ. – 2002. – № 1 (ч. 1). – Ст. 1.

Роскомнадзором. Такой тезис обосновывается исходя из того, что обработка специальной категории персональных данных и (или) биометрических персональных данных относится к группе тяжести «А» в соответствии с Постановлением Правительства РФ от 29 июня 2021 г. № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных».

Поднимая проблему соотношения баланса между необходимостью свободного использования сведений, относящихся к персональным данным, и их правовой защищённостью, необходимо отметить, что для гражданско-правовых и трудовых отношений данные об инвалидности (без подробностей о характере заболевания и иных подробных данных) соотносятся со статусом гражданина, который необходим обработчику для учёта особенностей работы, рабочего места и характера самой работы.

Усложнение обработки таких данных ведёт к тому, что субъектам их обработки (например, работодателям) будет труднее взаимодействовать с более незащищённым слоем общества – с инвалидами. Если учитывать, что бытовая запись в опроснике анкеты работодателя об инвалидности является специальной категорией персональных данных, то степень сложности защиты её хранения и обработки кратно возрастает, это приводит к дополнительным издержкам и расходам для такого работодателя, к примеру в виде найма дополнительных сотрудников, установки специальных программ и систем и иных мероприятий, направленных на особую защиту таких персональных данных. А это, в свою очередь, является дополнительным фактором, снижающим потенциальную заинтересованность работодателя в найме работников с инвалидностью, особенно если таких работников в штате лишь несколько.

Таким образом, необходимо выработать такие подходы к понятию персональных данных, которые позволят разрешать вопросы об отнесении информации к той или иной категории, а также будут обеспечивать соблюдение баланса интересов защиты этих данных и необходимости их обработки, не допуская дополнительных оснований для дискриминации различных особых субъектов общества (например, людей с ограниченными возможностями).

Относительно последнего мы придерживаемся научно-практической позиции, что инвалидность – это социальный статус и к специальным категориям персональных данных данные о наличии инвалидности не должны относиться.

Личностная, собственническая философия взгляда на персональные данные превалирует в рамках наиболее развитых правовых систем, и такой подход вполне органично имплементирован в правовую систему Российской Федерации. Вполне общепризнано, что сохранность персональных данных субъекта – это конституционное право человека и гражданина, равно как и право личности распоряжаться своими персональными данными, предоставлять доступ к ним и определять, кому их можно передавать, а кому нет и когда их изменять или удалять. Государство же в данной философии права обязано обеспечивать надёжную охрану, защиту, контроль и надзор в данной области, а также иные всевозможные действия для гарантии прав человека, гражданина, личности в отношении персональных данных.

Кроме прочего, важно зафиксировать, что в отечественном законодательстве нет термина «приватность» не по причине необработанности законодательства, а по той причине, что этот термин является англицизмом и на русском языке звучит как «неприкосновенность частной и личной жизни». Иными словами, данный термин прямо отражён в ст. 23 Конституции РФ. Персональные же данные являются составляющей частью более широкого понятия «частная жизнь». Субъект персональных данных может ограничить их использование, и данная информация уже будет рассматриваться как конфиденциальная, охватываемая режимом той или иной тайны.

После проведённого детального исследования вопроса о понятии и признаках правовой категории «персональные данные» можно в наиболее общем виде описать правовую природу данного явления посредством использования подхода С.С. Алексеева [46]. Суть данного подхода заключается в раскрытии правовой

[46] Алексеев С.С. Общие дозволения и запреты в советском праве: монография. – М.: Юридическая литература, 1998. – С. 227.

природы через юридические характеристики самого явления, которые, в свою очередь, позволят выявить его структуру, место среди иных правовых явлений равного порядка и роль данного правового явления в системе права[47].

Соответственно, если охарактеризовать правовую природу такого правового явления, как персональные данные, то следует обратить внимание на то, что оно относится к такой крупной правовой категории, как «информация», и находится в одном ряду с иными специальными категориями охраняемой законом информации (коммерческая, государственная, банковская, нотариальная и иные тайны, секреты производства и иные).

Структурно правовую категорию «персональные данные» следует рассматривать в качестве комплексного правового явления, поскольку общественные отношения по поводу этого объекта испытывают на себе дифференцированное регуляторное воздействие правовых норм не только различных отраслей права, но и отраслей различной правовой принадлежности. Иными словами, общественные отношения по поводу персональных данных регулируются как нормами публичного, так и частного права, при этом всё же регулирование нормами публичного права имеет преобладающее значение в данной области.

Подводя итог нашим рассуждениям о понятии и правовой природе персональных данных, обозначим некоторые, наиболее значимые выводы:

1. Предлагается авторское определение правовой категории «персональные данные» как любой информации о физическом лице (субъекте персональных данных), которая позволяет идентифицировать данное лицо, за исключением если такая информация содержится в обезличенном виде, а также иной информации, напрямую названной таковой в законе.

2. В целях обеспечения защиты прав субъектов персональных данных, с учётом расширения процессов цифровизации в современном государстве и обществе, предложена специальная информационно-правовая презумпция

---

[47] Комиссарова Е.Г. Формально-логические аспекты понятия «правовая природа» // Вестник Пермского университета. Юридические науки. – 2012. – № 2 (16). – С. 22.

относимости данных к персональным данным физического лица: «Любую информацию следует относить к числу персональных данных, если субъект этой информации заявляет о том, что данная информация определяет или позволяет его определить (идентифицировать). Обязанность по доказыванию обстоятельств, свидетельствующих об обратном, возлагается на лицо, осуществляющее обработку персональных данных».

3. Для цели развития науки информационного права выявлены и обоснованы правовые признаки, которым должны отвечать сведения, относящиеся к персональным данным, в качестве обязательных в процессе их отнесения к таковым:

– возможность определить конкретного субъекта по данным;

– возможность связать данные для соотношения информации и субъекта;

– возможность произвести умозаключение, что данные принадлежат конкретному субъекту;

– возможность обособления конкретных персональных данных друг от друга;

– персональные данные должны отвечать всем вышеуказанным признакам одновременно.

Для цели развития технологий исключением должны быть данные после применения технологий анонимизации, при условии выполнения всех разумных мер по недопущению персонализации данных путём надёжного шифрования и других способов защиты данных от деанонимизации. Соответствующие технологии и разумные меры по недопущению персонализации данных должны быть определены и рекомендованы Минцифры Российской Федерации для цели обеспечения должного уровня информационной безопасности.

Преимущества предложенного автором подхода к пониманию персональных данных будут проявляться в различных аспектах.

Во-первых, в этом случае возможно будет точно отделить ту информацию, которая составляет собой персональные данные, от иной информации.

Во-вторых, из числа персональных данных будет исключена информация, обрабатываемая на основе технологии обезличивания персональных данных. Существующая сейчас легальная дефиниция не позволяет однозначно сделать такой важный для науки и практики вывод. Это позволит вывести реальные статистические исследования, скрининг уязвимостей IT-продуктов, cookie-файлы из категорий обработки и передачи персональных данных, но только при условии их анонимизации и шифрования.

4. С научно-практической точки зрения представляется целесообразным отнести данные о наличии инвалидности к числу общедоступных персональных данных. Наличие инвалидности – это социальный статус, и к специальным категориям персональных данных данные о наличии инвалидности не должны относиться. Данный подход позволит не допускать дополнительных оснований для дискриминации лиц с ограниченными возможностями. Для гражданско-правовых, трудовых и ряда иных правоотношений данные о наличии инвалидности (без указания о заболевании и иных данных, составляющих медицинскую тайну) необходимы для учёта различных льгот и иных мер поддержки, а также специальных требований к рабочему месту и характеру трудовой функции.

5. Правовая природа персональных данных характеризуется тем, что относится к такой крупной правовой категории, как «информация», и находится в одном ряду с иными специальными категориями охраняемой законом информации, а также тем, что структурно данный правовой институт объединяет не только нормы различных отраслей, но и отраслей как публично-правового, так и частноправового цикла.

6. Информация о социальном статусе, а также иная информация об относимости к специальным социальным категориям (например, об инвалидности) сама по себе не должна быть отнесена к специальным категориям персональных данных, особенно в случае, если такая информация требуется для предоставления дополнительных социальных и иных гарантий.

§ 2. Правовая природа использования цифровых технологий при обработке персональных данных

Обработка персональных данных (далее – ПДн) в сети «Интернет» в условиях глобального информационного общества и цифровизации все чаще связывается с активным использованием информационных и цифровых технологий[48]. Обработка ПДн с помощью современных цифровых технологий делает возможным быстрое обобщение, анализ информации, позволяет использовать информацию для принятия решений, снижать затраты, повышать продажи, сохранять конкурентное преимущество. ПДн в предпринимательском обороте рассматриваются не только с технической, но и с коммерческой точки зрения, выступая определённым аналогом активов[49].

Персональные данные человека могут быть выражены в виде его индивидуальных предпочтений, взглядов, особенностей личной жизни, работы, увлечений, медицинских данных и прочей информации, наличие которой порой является весьма важным фактором успешного осуществления предпринимательской деятельности в определённых секторах экономики. Внедрение сложных алгоритмов и программного обеспечения для преобразования массовых данных в ресурс для целей принятия бизнес-решений затрагивает, в частности, отдельных лиц и группы лиц, особенно в случаях профилирования или маркировки, и в конечном итоге вызывает много проблем с защитой данных[50].

По мнению Л.А. Сергиенко, в связи с постоянным ростом объёма информации ограниченного доступа (в том числе и персональных данных) необходимо принимать во внимание особую ответственность при решении

---

[48] Минбалеев А.В., Филоненкова В.А. Проблемы защиты персональных данных и цифрового профиля человека в сети «Интернет» в условиях пандемии // Вестник ЮУрГУ. Серия: Право. – 2020. – № 3. – Т. 20. – С. 90.

[49] Санникова Л.В., Харитонова Ю.С. Цифровые активы как объекты предпринимательского оборота // Право и экономика. – 2018. – № 4. – С. 31.

[50] Минбалеев А.В., Филоненкова В.А. Проблемы защиты персональных данных и цифрового профиля человека в сети «Интернет» в условиях пандемии // Вестник ЮУрГУ. Серия: Право. – 2020. – № 3. – Т. 20. – С. 91.

вопросов регулирования соответствующих отношений [51]. Угрозы в области обработки персональных данных рассматриваются в контексте возрастающих масштабов компьютерной преступности в соответствии с Доктриной информационной безопасности Российской Федерации [52]. Важно при этом отметить, что обработка ПДн должна служить человечеству[53].

Важным вопросом является определение правовой природы обработки ПДн. И.Л. Бачило отмечает, что Федеральный закон № 159-ФЗ выравнивает положение страны в мировом информационном пространстве и упорядочивает правила работы с такими данными [54]. Персональные данные традиционно включаются в сферу правового регулирования как объекты, над которыми совершаются определённые действия – обработка[55]. Слово «обработать» в соответствии с толковым словарём – подвергнуть выделке, отделке, изменениям, анализу, сделать готовым для чего-то[56].

Федеральный закон № 159-ФЗ выделяет ряд действий, в которых раскрываются методы обработки персональных данных, но перечень является открытым, что позволяет отнести к методам обработки любое действие с ПДн.

---

[51] Сергиенко Л.А. Правовая защита персональных данных. Цели и принципы правового регулирования // Проблемы информатизации. – 1995. – № 1. – С. 37.

[52] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. – 2016. – № 50. – Ст. 7074.

[53] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1716879740&tld=ru&lang=en&name=?uri=CELEX:32016R0679&text=Regulation+%28EU%29+2016/679+of+the+European+Parliament+and+of+the+Council+of+27+April+2016+on+the+protection+of+natural+persons+with+regard+to+the+processing+of+personal+data+and+on+the+free+movement+of+such+data%2C+and+repealing+Directive&url=https%3A//eur-lex.europa.eu/legal-content/EN/TXT/PDF/%3Furi%3DCELEX%3A32016R0679&lr=43&mime=pdf&l10n=ru&sign=190ab917a0b580c7bfbd6af871a8e397&keyno=0, свободный (дата обращения: 01.06.2025).

[54] Бачило И.Л. Важный шаг в регулировании информационных прав граждан: К принятию ФЗ «О персональных данных» // Законы России. – 2006. – № 11. – С. 101.

[55] Минбалеев А.В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 2 (14). – С. 7.

[56] Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка; Российская АН, Ин-т рус. яз., Российский фонд культуры. – 2-е изд., испр. и доп. – М.: Азъ, 1994. – С. 567.

Обработка же ПДн в соответствии с Федеральным законом № 159-ФЗ допускается только на основе определённых принципов: на законной и справедливой основе, ограничиваясь достижением конкретных, заранее определённых и законных целей в ограниченном целями объёме с соблюдением точности, достаточности и актуальности, только в течение ограниченного необходимостью срока.

Принципы обработки ПДн служат гарантией соблюдения Конституции Российской Федерации. Согласно ч. 1 ст. 23 Конституции РФ каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. В соответствии со ст. 24 Конституции РФ сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. В развитие названных конституционных положений принят Федеральный закон № 152-ФЗ[57]. В соответствии с п. 1 ст. 3 Федерального закона № 152-ФЗ ПДн являются составной частью информации. Правовая природа обработки персональных данных заключается в том, что данные о физических лицах имеют несколько иную правовую природу, чем любые другие данные, так как любой гражданин, независимо от своего статуса, во всех случаях обладает правоспособностью, правосубъектностью[58].

Из приведённого ниже анализа определений в международных и отечественных нормативных правовых актах, регулирующих правовую охрану ПДн, можно сделать вывод, что обработка подразумевает собой любое действие с ПДн. Но законодательно выделяются следующие, отдельно поименованные, методы обработки ПДн: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

---

[57] Разъяснения Прокуратуры Акбулакского района. [Электронный ресурс]. Режим доступа: https://xn--80aafb8bpdbc2g.xn--p1ai/2021/11/3308/, свободный (дата обращения: 01.06.2025).

[58] Кудашкин Я.В. Особенности правовой природы и классификации персональных данных в России // Право и государство: теория и практика. – 2018. – № 1 (157). – С. 128.

Помимо этого, научные исследования в области определения понятия «обработка» были представлены в трудах таких отечественных учёных-правоведов, как Е.И. Казакевич и Е.П. Губин[59].

Пункт 3 статьи 3 Федерального закона № 152-ФЗ определяет обработку персональных данных как «любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных».

Часть 2 статьи 4 Регламента по защите персональных данных Европейского союза [60] определяет термин «обработка» как «любую операцию или набор операций, которые выполняются над персональными данными или над наборами персональных данных, автоматическими или неавтоматическими средствами. Такие как сбор, запись, организация, структурирование, хранение, адаптация или изменение, просмотр, использование, раскрытие (путём передачи, распространения или иначе, делая их доступными), выравнивание или комбинирование, ограничение, удаление или уничтожение».

Закон о защите персональных данных Китайской Народной Республики не предусматривает специального определения обработки ПДн, но в ст. 4 отмечается,

---

[59] Казакевич Е.И., Губин Е.П. Защита прав и свобод человека при обработке персональных данных в период цифровой трансформации // Уральский журнал правовых исследований. – 2022. – № 4 (21). – С. 40.

[60] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1716881024&tld=ru&lang=en&name=?uri=CELEX:32016R0679&text=Regulation+%28EU%29+2016/679+of+the+European+Parliament+and+of+the+Council+of+27+April+2016+on+the+protection+of+natural+persons+with+regard+to+the+processing+of+personal+data+and+on+the+free+movement+of+such+data%2C+and+repealing+Directive&url=https%3A//eur-lex.europa.eu/legal-content/EN/TXT/PDF/%3Furi%3DCELEX%3A32016R0679&lr=43&mime=pdf&l10n=ru&sign=c89c218bcdcd86247ca75f0c1bd5459e&keyno=0, свободный (дата обращения: 01.06.2025).

что обработка ПДн «включает сбор, хранение, использование, обработку, передачу, предоставление, раскрытие, удаление и т.д.»[61].

Регламент по защите персональных данных Европейского союза выделяет схожий перечень действий, но не идентичный. Так, если провести сравнительный анализ, то концептуально Федеральный закон № 152-ФЗ выделяет больший список определённых способов обработки, например: накопление, уточнение, извлечение. Регламент по защите персональных данных Европейского союза содержит понятия просмотр, выравнивание, комбинирование и ограничение, которых не содержит Федеральный закон № 152-ФЗ, а также имеет иное понимание некоторых способов (раскрытие и передача).

Под передачей ПДн в соответствии со ст. 3 Федерального закона № 152-ФЗ понимается распространение данных, предоставление ПДн и доступ к персональным данным. Однозначного определения «передачи» применительно к ПДн в законе не содержится, но в тексте закона формулировка дана следующим образом: «…передачу (распространение, предоставление, доступ)…» [62].

Таким образом, распространение, предоставление и доступ к персональным данным должны рассматриваться не как проявления передачи персональных данных, а в качестве самостоятельных действий, составляющих обработку персональных данных. Но все понятия имеют разное содержание, смысл и регулирование. В настоящем научном исследовании проанализирован объём каждого термина и предложена новая систематизация способов, методов обработки персональных данных.

---

[61] Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1716881263&tld=ru&lang=en&name=Personal-Information-Protection-Law-of-the-Peoples-Republic-of-China.pdf&text=Personal+Information+Protection+Law+of+the+People's+Republic+of+China+–+Effective+Nov.+1%2C+2021&url=https%3A//www.china-briefing.com/news/wp-content/uploads/2021/08/Personal-Information-Protection-Law-of-the-Peoples-Republic-of-China.pdf&lr=43&mime=pdf&l10n=ru&sign=6be13b78006ef629a8b4304acc0f1a2a&keyno=0, свободный (дата обращения: 01.06.2025).

[62] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.

В Федеральном законе № 152-ФЗ термин «распространение персональных данных» означает передачу ПДн неограниченному кругу лиц. В соответствии с п. 9 Постановления Пленума Верховного Суда РФ от 24.02.2005 № 3 под «распространением» понимается «опубликование таких сведений в печати, трансляция по радио и телевидению, демонстрация в кинохроникальных программах и других средствах массовой информации, распространение в сети «Интернет», а также с использованием иных средств телекоммуникационной связи, изложение в служебных характеристиках, публичных выступлениях, заявлениях, адресованных должностным лицам, или сообщение в той или иной, в том числе устной, форме хотя бы одному лицу» [63].

Тогда как термин «предоставление персональных данных» означает передачу ПДн определённому, ограниченному кругу лиц.

В Федеральном законе № 152-ФЗ отсутствует термин «доступ», но из закона следует, что передача ПДн может быть реализована путём передачи доступа к ПДн двумя способами:

а) распространение доступа – неограниченному кругу лиц;

б) предоставление доступа – ограниченному кругу лиц.

Таким образом, термин «доступ» имеет созависимый смысл от других терминов. Логически данные определения имеют различный объём и непропорционально вмещают и описывают друг друга. Схема кругов Эйлера, на которой отображена действительная логическая связь понятия «передача персональных данных», размещена на схеме № 1 в Приложении[64].

Важно отметить, что закон предусматривает отдельное правовое регулирование, своего рода надстройку, к понятию «трансграничная передача персональных данных», под которой понимает: распространение, предоставление, доступ ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому

---

[63] Постановление Пленума Верховного Суда РФ от 24.02.2005 № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» // Бюллетень Верховного Суда РФ. – 2005. – № 4.

[64] См.: Схема №1. Приложение. С.207.

лицу в соответствии с подп. 11 п. 3 Федерального закона № 152-ФЗ. Иными словами, трансграничная передача персональных данных с правовой точки зрения является разновидностью передачи персональных данных, осложнённой наличием международно-правового аспекта.

Построение цепочки взаимосвязанных определений по текущей схеме [65] примечательно тем, что правовое регулирование, ответственность и меры защиты персональных данных при предоставлении и распространении также будут сильно различаться, о чём, в частности, мы более подробно будем вести речь в §3.3 настоящего исследования.

Кроме прочего, для каждого типа «передачи» ПДн требуется особый тип согласия на передачу ПДн. Например, требуется отдельное согласие на распространение ПДн тогда, когда для предоставления ПДн нужно указать конкретный перечень третьих лиц, кому будут предоставляться ПДн.

Обобщающее понятие «передача персональных данных» консолидирует разные по своей сути правовые понятия, влекущие впоследствии разную обработку ПДн для субъекта права, что вводит в заблуждение субъектов обработки ПДн. В законе не приведены самостоятельные определения каждого отдельного термина, что влечёт некоторую неоднозначность и сложность понимания логики терминологии.

Под «обработкой персональных данных» в соответствии с подп. 3 п. 3 Федерального закона № 152-ФЗ понимаются в том числе действия, включающие «…передачу (распространение, предоставление, доступ)…», то есть гражданин, выражая своё «согласие на обработку персональных данных», фактически считает возможным или нужным предоставление согласия на передачу своих данных в целом, а не в части только конкретного способа передачи. Таким образом, нарушается принцип свободно, своей волей и в своём интересе давать согласие на обработку ПДн. Согласие в этом случае можно расценить как вынужденное и

[65] См.: Схема № 1 Приложения. С. 207.

притворное, порождающее, в свою очередь, соответствующие правовые последствия признания такой сделки ничтожной.

В целом понятия «предоставление» и «передача» являются синонимами в русском языке. Так, в соответствии со словарем русских синонимов:

Передача – «…распространение, пиктография, транш, радирование, предоставление…»;

Предоставление – «…выдача, обеспечение; вручение, франчайзинг, разрешение, передача, уделение, доставление, позволение, оказание, доставка, снабжение…»[66].

Можно резюмировать вышесказанное тем, что распространение, предоставление и доступ к персональным данным должны рассматриваться не как проявления передачи персональных данных, а в качестве самостоятельных действий, составляющих обработку персональных данных. В связи с этим в целях повышения эффективности института обработки персональных данных и обеспечения прав субъектов персональных данных предложено скорректированное определение «обработки персональных данных», под которым следует понимать «любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, распространение, предоставление, доступ, обезличивание, блокирование, удаление и уничтожение персональных данных».

Самостоятельного и полного определения понятию «передача персональных данных» законодатель в тексте закона прямо не дает, кроме как расшифровку, в рамках определения иного термина «обработка» в п. 3 ст. 3 Федерального закона № 152-ФЗ, путём заключения в объём термина «передача» трёх других, которые и составляют, по логике законодателя, общий термин «передача».

---

[66] Словарь русских синонимов. [Электронный ресурс]. Режим доступа: https://sinonim.org/, свободный (дата обращения: 01.06.2025).

Каждый термин: «предоставление», «распространение», «доступ» – является самостоятельной правовой категорией, влекущей необходимость применения различных средств правового регулирования. Соответственно, смешивание вышеуказанных правовых категорий может привести к определённым неблагоприятным последствиям. Проблемы отсутствия чёткого определения правовых категорий «предоставление» и «распространение» и, как следствие, нерешаемость проблем соотношения вышеуказанных категорий затрагиваются в трудах А.В. Минбалеева и К.А. Зюбанова[67].

Во-первых, введение субъекта персональных данных в заблуждение относительно объёма предоставляемых правомочий операторов по обработке персональных данных в рамках согласия на обработку ПДн. Такое положение нарушает цели и принципы Федерального закона № 152-ФЗ.

Во-вторых, повышаются правовые риски и на стороне добросовестных обработчиков ПДн, которые не в полной мере осознают различие данных правовых категорий (распространение, предоставление и доступ).

В-третьих, правовая неопределённость предоставляет потенциальную возможность недобросовестным операторам персональных данных злоупотреблять своим положением или совершать противоправные деяния, используя пробел в праве.

Выходом из сложившейся ситуации, по нашему видению, является введение чётких определений в ст. 3 Федерального закона № 152-ФЗ, определяющих понятийный аппарат законодательства в области ПДн. Необходимость обязательного законодательного закрепления правовых дефиниций, которые определяют те или иные действия по обработке ПДн, отмечает и видный учёный в области информационного права А.В. Минбалеев, указывая на то, что такой подход широко распространён за рубежом и основывается на чётком разграничении действий по обработке ПДн и создании специальных норм в отношении каждого

---

[67] Зюбанов К.А. Распространение сведений о гражданине, распространение персональных данных. [Электронный ресурс]. Режим доступа: https://pravo.hse.ru/digitalperson/dissemination, свободный (дата обращения: 01.06.2025).

из них [68]. Введение отдельного понятия для таких правовых категорий, как «передача персональных данных» и «доступ к персональным данным», позволит исправить недостатки правовой техники.

По нашему мнению, следует упростить схему понимания определения «обработки персональных данных» [69], исключив самостоятельную категорию «передача персональных данных», группирующую иные самостоятельные понятия как не соответствующее общей логике и терминологии, выдержанной в законе[70].

Представляется возможным изложить определение обработки персональных, данных в ст. 3 Федерального закона № 152-ФЗ, следующим образом: «обработка персональных данных – это любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, распространение, предоставление, доступ, обезличивание, блокирование, удаление и уничтожение персональных данных».

Таким образом, с научной точки зрения, автор выделяет, помимо прочих, ранее имеющих самостоятельный статус, такие самостоятельные категории в области обработки персональных данных, как «распространение», «доступ», «предоставление».

Обработку ПДн можно разделить по способу осуществления действий в отношении ПДн. Техническая обработка персональных данных – это обработка не механическим или ручным способом, а автоматизированным способом. Обработка, которая осуществляется путём действий автоматики, компьютеров, называется автоматизированной обработкой ПДн. Все остальные способы обработки не имеют особого термина и определяются как обработка неавтоматическими средствами.

---

[68] Минбалеев А.В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 2 (14). – С. 7.
[69] См.: Схема № 1. Приложения. С. 207.
[70] См.: Схема № 2. Приложения. С. 207.

Является важным разработка адекватного понятийного аппарата, поскольку во многом существующий понятийный аппарат сложился и ориентирован на бумажный документооборот, который не актуален в условиях цифровой экономики[71].

Законодательство и регулирующие органы рассматривают автоматизированный процесс обработки как совершение любых действий с личными данными, связанных с применением вычислительной техники. В науке и практике на данный момент не возникает споров о подобного рода классификации, что демонстрирует удачно сложившийся подход. Таким образом, систему способов обработки ПДн можно представить следующим образом:

Способы обработки ПДн:

а) автоматизированный;

б) без использования средств автоматизации (неавтоматическими средствами).

Обработка различных категорий ПДн имеет широкую индивидуальную специфику и накладывает определённые технические и правовые обязательства по обработке ПДн. В соответствии с пп. 2.5, 2.6 и 2.7 Методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения (приложение к Приказу Роскомнадзора от 30.05.2017 № 94)[72], а также в соответствии с положениями Федерального закона № 152-ФЗ выделяются особенности обработки ПДн в зависимости от обрабатываемой категории ПДн:

а) обработка общедоступных ПДн (п. 1 ст. 3 Федерального закона № 152- ФЗ);

---

[71] Цифровая экономика: актуальные направления правового регулирования: научно-практ. пособие / под ред. И.И. Кучерова, С.А. Синицына. – М.: Норма: ИЗиСП, 2022. – С. 253.

[72] Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30 мая 2017 г. № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения». [Электронный ресурс]. Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71652212/?ysclid=lwchijkaii571205726, свободный (дата обращения: 01.06.2025).

б) обработка биометрических ПДн (ст. 11 Федерального закона № 152-ФЗ). Правовая специфика обработки биометрических данных заключается в том, что такая обработка возможна только с письменного согласия субъекта данных, за исключением случаев, предусмотренных законом;

в) обработка специальных ПДн (ч. 1 ст. 10 Федерального закона № 152-ФЗ). Отличие обработки специальных ПДн от иных видов заключается в том, что обработка такой категории персональных данных возможна только в случаях, предусмотренных законом, но, помимо этого, такая обработка должна быть прекращена, если устранены причины, вызвавшие необходимость подобной обработки;

г) обработка иных ПДн. Некоторые отечественные правоведы, например Я.В. Кудашкин[73], выделяют обработку категории особых ПДн, которая, по нашему представлению, имеет то же значение, что и категория «иные».

Серьёзной проблемой являются вопросы правового регулирования обработки ПДн с помощью современных технологий. В период повсеместного распространения цифровых технологий и цифровой экономики изменяются многие сферы жизни общества.

В современном обществе право, функционируя как социальный регулятор, играет значительную роль в поддержке социального развития[74]. Как отмечает Е.И. Казакевич, в новой среде общественные и экономические отношения претерпевают изменения, в том числе благодаря постоянному сбору и использованию больших объёмов цифровых данных, а также принятию на их основе инновационных технологических, организационных и других решений.

---

[73] Кудашкин Я.В. Особенности правовой природы и классификации персональных данных в России // Право и государство: теория и практика. – 2018. – № 1 (157). – С. 129.

[74] Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам (протокол от 04.06.2019 № 7)). [Электронный ресурс]. Режим доступа: https://digital.gov.ru, свободный (дата обращения: 01.06.2025).

Главная сложность в обработке персональных данных при развитии цифровых технологий – это ограничение прав и свобод человека[75].

Но в исследованиях отмечается и обратная проблема – негативные последствия от усиления контроля в области защиты ПДн на состояние конкуренции на рынке, а также на развитие инноваций[76]. Перечень не является исчерпывающим, имеет специфику оборота и обработки ПДн с учётом особенностей каждой отдельной технологии.

К наиболее проблемным, с точки зрения применимости классических средств правового регулирования, технологиям, с помощью которых обрабатываются данные и, в частности, ПДн, относятся:

а) технологии искусственного интеллекта;

б) технологии распределённого реестра;

в) облачные технологии.

Таким образом, правовая природа обработки ПДн заключается в особом подходе к их использованию, который не должен нарушать права человека на неприкосновенность частной жизни, личную и семейную тайну[77]. Такой подход подразумевает, что обработка персональных данных должна осуществляться на законной основе, ограничиваться достижением конкретных, заранее определённых и законных целей, обеспечивая точность, достаточность и актуальность персональных данных по отношению к целям их обработки. Неправомерная обработка данных может служить основанием возникновения различных форм дискриминации человека и гражданина, нарушать основные конституционные права, в своих исследованиях отмечает А.А. Лазаров[78]. Изучаемые в настоящей

---

[75] Казакевич Е.И., Губин Е.П. Защита прав и свобод человека при обработке персональных данных в период цифровой трансформации // Уральский журнал правовых исследований. – 2022. – № 4 (21). – С. 41.

[76] Доклад «Consumer Data Rights and Competition – Background note». [Электронный ресурс]. Режим доступа: https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf, свободный (дата обращения 01.06.2025).

[77] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.

[78] Лазаров А.А. Информационно-правовое регулирование социального кредитования (скоринга): дис. … канд. юрид. наук. – М., 2023. – С. 12.

работе проблемы защиты конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации поднимает в своём диссертационном исследовании А.А. Федосин[79].

Законодательное закрепление определений методов обработки данных и создание специальных норм в отношении каждого из них позволят более эффективно осуществлять правовое регулирование обработки ПДн. Развитый понятийный аппарат даст возможность яснее понимать методы обработки ПДн при даче согласия гражданами для цели соблюдения своих конституционных прав и основных принципов обработки, установленных Федеральным законом № 152-ФЗ. Первоочередным действием, по нашему мнению, является введение отдельного понятия для термина «передача персональных данных», отдельного термина «доступ к персональным данным».

Подводя итог нашим рассуждениям о правовой природе обработки персональных данных с использованием цифровых технологий, можно отдельно подчеркнуть определённые и наиболее интересные выводы:

1. Каждый термин: «предоставление», «распространение», «доступ» – является самостоятельной правовой категорией, влекущей необходимость применения различных средств правового регулирования. Соответственно, смешивание вышеуказанных правовых категорий может привести к определённым неблагоприятным последствиям.

2. Необходимо закрепить специальную терминологическую базу методов обработки ПДн для достижения наибольшей эффективности правового регулирования и защиты конституционных прав гражданина и соблюдения принципов обработки ПДн.

Наиболее удачным, по нашему мнению, вариантом в таком случае будет выбор пути упрощения правопонимания категории «обработка персональных

---

[79] Федосин А.А. Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации: автореф. дис. … канд. юрид. наук. – Саранск, 2009. – 27 с.

данных» посредством исключения отдельной составной части данной категории в виде «передачи персональных данных».

Результатом такого решения будет несколько иное формулирование понятия категории «обработка персональных данных», которое будет пониматься как «любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, распространение, предоставление, доступ, обезличивание, блокирование, удаление и уничтожение персональных данных».

3. Для целей развития информационного права предлагается закрепить систему классификации персональных данных:

1. Классификация ПДн в зависимости от способов обработки ПДн:

а) автоматизированный;

б) без использования средств автоматизации (неавтоматическими средствами).

2. Классификация ПДн в зависимости от обрабатываемой категории ПДн:

а) общедоступные ПДн (п. 1 ст. 3 Федерального закона № 152-ФЗ);

б) биометрические ПДн (ст. 11 Федерального закона № 152-ФЗ). Правовая специфика обработки биометрических данных заключается в том, что такая обработка возможна только с письменного согласия субъекта данных, за исключением случаев, предусмотренных законом;

в) специальные ПДн (ч. 1 ст. 10 Федерального закона № 152-ФЗ). Отличие обработки специальных ПДн от иных видов заключается в том, что обработка такой категории персональных данных возможна только в случаях, предусмотренных законом, но, помимо этого, такая обработка должна быть прекращена, если устранены причины, вызвавшие необходимость подобной обработки;

г) иные ПДн (или особые).

§ 3. Правовое обеспечение использования цифровых технологий при обработке персональных данных

Переходя к раскрытию правового обеспечения использования цифровых технологий при обработке персональных данных, отметим, что в научном труде прежде всего формулируется и обосновывается авторская позиция относительно двуединого подхода к исследованию данного правового явления.

Суть авторского подхода научного исследования правового регулирования обработки персональных данных с использованием цифровых технологий заключается в том, что при исследовании внимание будет обращено преимущественно на такие правовые средства, посредством которых осуществляется или может осуществляться правовая охрана прав и законных интересов в области персональных данных. Преимущество такого подхода заключается в том, что будут исследованы те аспекты и средства правового регулирования, которые наполнены реальным юридическим содержанием и изучение которых представляет как сугубо научный интерес, так и позволяет удовлетворять конкретные потребности юридической практики. Тем самым реализуется практико-ориентированный подход в публично-правовых науках.

Возвращаясь к исследованию публично-правового регулирования обработки персональных данных в сфере использования цифровых технологий, следует указать на то, что данный сегмент правового регулирования является важной основой соблюдения гражданских прав и свобод человека.

В связи со значимостью защиты национальных интересов публично-правовое регулирование в области ПДн осуществляется не только на уровне государства, но и на уровне межгосударственных отношений. Правовое регулирование соответствующих отношений на межгосударственном уровне обеспечивается международными договорами, соглашениями, декларациями. На государственном уровне правовая защита ПДн регулируется государственными и

ведомственными актами[80]. Международные сообщества и государства стремятся к цели создать среду, в которой будут соблюдаться правовые минимумы, обеспечивая глобальную, экстерриториальную защиту прав своих граждан.

Интенсивное развитие информационных технологий (искусственный интеллект, облачные технологии, обработка больших данных, блокчейн, Интернет и иные инновационные решения), создаёт риски несанкционированного доступа и неправомерного использования персональных данных граждан. Современные правоотношения в сфере обеспечения безопасности персональных данных при применении цифровых технологий регулируются нормами российского и международного законодательства ввиду трансграничной обработки ПДн.

Согласно статье 15 Конституции Российской Федерации, общепризнанные принципы и нормы международного права, а также международные договоры Российской Федерации являются составной частью её правовой системы; при расхождении правил приоритет имеют положения международного договора.

К основным национальным интересам в информационной сфере относится защита информационных ресурсов от несанкционированного доступа, утечек, обеспечение безопасности информационных и телекоммуникационных систем, что подчеркивалось в Доктрине информационной безопасности Российской Федерации[81], Стратегии национальной безопасности Российской Федерации [82] и отводилось особое место в докладе Президента Российской Федерации на заседании Совета Безопасности РФ 20 мая 2022 г. «О повышении устойчивости и

---

[80] Организационно-правовые основы защиты персональных данных: учеб. пособие / подготов. А.В. Гортинским. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1716999221&tld=ru&lang=ru&name=621.pdf&text=Организационно-правовые+основы+защиты+персональных+данных»+–+учебное+пособие%2C+подготовленное+А.+В.+Гортинским&url=http%3A//elibrary.sgu.ru/uch_lit/621.pdf&lr=43&mime=pdf&l10n=ru&sign=2832c9ed0ec3f296b88544a3601d6483&keyno=0, свободный (дата обращения: 01.06.2025).

[81] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. – 2016. – № 50. – Ст. 7074.

[82] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. – 2021. – № 27 (ч. II). – Ст. 5351.

безопасности функционирования информационной инфраструктуры государства»[83] и других стратегических национальных нормативных актах.

Анализируя развитие правового регулирования в области персональных данных, выявляются некоторые наиболее важные стадии развития данного правового института. При этом стадии развития не предусматривают строгих хронометрических границ, а характеризуются в первую очередь уровнем правового регулирования и набором применяемых правовых средств. Исходя из вышеуказанного подхода к стадиям развития правового регулирования в области персональных данных, можно сформулировать некоторые наиболее важные из них:

I. Стадия концептуального развития принципов неотъемлемости информационных прав и свобод человека.

Ключевыми событиями этой стадии стали:

1890 – публикации статьи The right to privacy, в которой Луис Брандейс и Сэмюэль Уоррен сформулировали понятие «privacy» в контексте права остаться наедине с собой.

1948 – принятие «Всеобщей декларации прав человека».

1950 – принятие Европейской Конвенции.

1966 – принятие «Международного пакта о гражданских и политических правах» (вступил в силу с 1976 г.).

Вышеназванные события номинировали такие принципы, как защита от произвольного вмешательства в личную и семейную жизнь, и провозгласили

---

[83] Доклад Президента Российской Федерации В.В. Путина 20 мая 2022 г. на заседании Совета Безопасности Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства». [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1716999516&tld=ru&lang=ru&name=988fe6c43f2b5e1e8142e33d505d.pdf&text=Доклад+Президента+Российской+Федерации+В.В.+Путина+20+мая+2022+г.+на+заседании+Совета+Безопасности+Российской+Федерации+«О+повышении+устойчивости+и+безопасности+функционирования+информационной+инфраструктуры+государства»&url=http%3A//uc-pps.ru/files/ckeditor/8f/ef/988fe6c43f2b5e1e8142e33d505d.pdf&lr=43&mime=pdf&l10n=ru&sign=c863d62cd3c68f98a91533e4dfbbc90d&keyno=0, свободный (дата обращения: 01.06.2025).

«тайну корреспонденции» в качестве одной из разновидностей личных прав человека.

Учёные Л.В. Исакова и К.Е. Статуева[84] отмечают, что развитие концепции о том, что информационные права и свободы человека являются неотъемлемыми правами человека, началось с принятия «Всеобщей декларации прав человека» (1948 г.), Европейской Конвенции 1950 г. и «Международного пакта о гражданских и политических правах» (1966 г., вступил в силу с 1976 г.), защищающих от произвольного вмешательства в личную и семейную жизнь и провозглашающих «тайну корреспонденции» в качестве одной из разновидностей личных прав человека. Данные принципы составляют основу правового регулирования персональных данных.

II. Стадия развития международно-правового регулирования обработки ПДн посредством закрепления правовых основ и принципов.

1980 – в рамках деятельности Организации экономического сотрудничества и развития (ОЭСР) были утверждены «Основные положения о защите неприкосновенности частной жизни и международных обменов персональными данными»[85]. Указанные положения закрепляют совокупность базовых принципов, обусловленных необходимостью обеспечения защиты прав и свобод граждан. Данные принципы призваны служить фундаментом для формирования законодательства в сфере регулирования персональных данных. Кроме того, положениями установлены регламентированные ограничения, направленные на предотвращение неконтролируемого трансграничного перемещения персональных данных. Нормы распространяли действие лишь на незначительное число стран.

---

[84] Исакова Л.В., Статуева К.Е. Международно-правовое регулирование защиты персональных данных работников // Новый университет. Серия: Экономика и право. – 2015. – № 4 (50). – С. 20.

[85] Основные положения Организации по экономическому сотрудничеству и развитию (ОЭСР) о защите неприкосновенности частной жизни и международных обменов персональных данных, 1980. [Электронный ресурс]. Режим доступа: https://rppa.ru/npa/oesr_23.09.1980, свободный (дата обращения: 01.06.2025).

1981 – в соответствии с принятой «Конвенцией Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» [86] (далее — Конвенция) сформированы международные законодательные основы регулирования обработки ПДн. Закреплены ключевые принципы обработки ПДн: целевое использование, ограничение по срокам, неизбыточность, актуальность данных, регулирование трансграничной передачи, обеспечение защиты, гарантии прав субъекта данных. Указанные принципы образуют единую систему международных стандартов, направленных на обеспечение баланса между эффективным использованием персональных данных и защитой прав и свобод человека.

1990 – подписано «Руководство ООН относительно компьютерных файлов персональных данных»[87]. Данное руководство в ряде положений повторяет нормы Конвенции и нацелено преимущественно на государства развивающихся стран.

III. Стадия становления и развития национального законодательства зарубежных юрисдикций в сфере регулирования обработки ПДн.

1995: Директива о защите данных 95/46 /ЕС закрепила принципы защиты основных прав и свобод физических лиц, право на неприкосновенность частной жизни при обработке ПДн и свободное перемещение таких данных.

1997: Директива 97/66/ЕС[88] дополнила Директиву 95/46/Е, закрепила, что юридические, нормативные и технические требования защиты и сбалансированности объема обрабатываемых ПДн.

---

[86] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) // Собрание законодательства РФ. – 2014. – № 5. – Ст. 419.

[87] Руководство ООН относительно компьютерных файлов персональных данных (Принято Генеральной Ассамблеей ООН 14 декабря 1990 г.). [Электронный ресурс]. Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/computerized_data.shtml, свободный (дата обращения: 01.06.2025).

[88] Директива 97/66/ЕС Европейского парламента и Совета Европейского союза об использовании персональных данных и защите неприкосновенности частной жизни в сфере телекоммуникаций (Принята в Страсбурге 15.12.1997). [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1717000149&tld=ru&lang=ru&name=директива%2097-66.pdf&text=Директива+97/66/ЕС+Европейского+парламента+и+Совета+Европейского+союза+о+использовании+персональных+данных+и+защите+неприкосновенности+частной+жизни+в+сфере+телекоммуникаций.+Принята+в+Страсбурге&url=https%3A//www.tgl.net.ru/files/infosafety/

2016: Регламент № 2016/679[89] развил правовое регулирование в отношении права субъекта на личную жизнь в контексте обработки ПДн, приняты общие принципы обработки ПДн.

2018: Генеральный регламент о защите ПДн (GDPR). Принят подписанием Протокола № 223 о внесении изменений в Конвенцию[90]. Регламент стал эталоном правового регулирования обработки ПДн для ряда стран и закрепил регулирование защиты биометрических и генетических данных, данных обрабатываемых с помощью ИИ, закрепил требования защиты данных и обязанности операторов ПДн уведомлять об утечках данных.

В дальнейшем многие зарубежные наработки в области ПДн были взяты за основу при становлении отечественного публично-правового регулирования обработки ПДн.

IV. Стадия становления и развития публично-правового отечественного законодательства в сфере регулирования ПДн.

2001: Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных подписана Российской Федерацией.

%25D0%25B4%25D0%25B8%25D1%2580%25D0%25B5%25D0%25BA%25D1%2582%25D0%25B8%25D0%25B2%25D0%25B0%252097-66.pdf&lr=43&mime=pdf&l10n=ru&sign=be5015ff290ee9908205828ad04ba74a&keyno=0, свободный (дата обращения: 01.06.2025).

[89] Регламент № 2016/679 Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)» (Принят в г. Брюсселе 27.04.2016). [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1717000215&tld=ru&lang=ru&name=2016-679-27.pdf&text=Регламент+N+2016/679+Европейского+парламента+и+Совета+Европейского+Союза+«О+защите+физических+лиц+при+обработке+персональных&url=https%3A//www.ugmk-clinic.ru/media/uploads/2022/04/29/2016-679-27.pdf&lr=43&mime=pdf&l10n=ru&sign=90f5129b7d907293bbfa6e04c46d744b&keyno=0, свободный (дата обращения: 01.06.2025).

[90] Протокол о внесении изменений в Конвенцию о защите физических лиц при автоматизированной обработке персональных данных (CETS № 223) (Подписан в г. Страсбурге 10.10.2018) // Бюллетень Европейского суда по правам человека. Российское издание. – 2018. – № 12. – С. 12.

2005: Конвенция[91] ратифицирована Российской Федерацией.

2006: Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[92]. Приняты базовые понятия и определения, которые используются во всех нормативных правовых актах, касающихся защиты информации и ПДн.

2006: Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[93] имплементировал основные положения Конвенции, а также закон ввёл дополнительные требования и специальные принципы по обработке ПДн.

2011: Федеральный закон от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»[94]. Пересмотрены и изменены положения защиты ПДн.

2017: Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»[95]. Установлен запрет на первичную обработку ПДн за пределами Российской Федерации.

2022: Федеральный закон от 14 июля 2022 г. № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской

---

[91] Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» // Российская газета. – 2005. – № 288.

[92] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. – 2006. – № 165.

[93] Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.

[94] Федеральный закон от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» // Российская газета. – 2011. – № 162.

[95] Федеральный закон от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» // Российская газета. – 2014. – № 163.

деятельности»[96]. Существенным образом изменены требования к обработке ПДн для цели обеспечения защиты национальных интересов прав граждан. Именно с этого момента автор видит полноценное становление комплексного, самостоятельного и сильного национального регулирования отношений по обработке и защите ПДн в Российской Федерации.

С принятием вышеназванных законов сфера отношений, связанных с обработкой персональных данных в Российской Федерации, впервые обрела столь детальное правовое регулирование.

V. Стадия правовой трансформации в области правового регулирования обработки персональных данных в условиях развития цифровых технологий.

Нами отдельно выводится данная стадия, так как публично-правовое регулирование в сфере ПДн активно трансформируется под давлением современных технологий, которые требуют изменений в ранее сформированный механизм правового регулирования. Век технологий характеризуется быстрой изменчивостью, ввиду чего современное правовое регулирование зачастую не успевает за развитием технологий. В силу технологических изменений требуется проведение правовых экспериментов для цели формирования сбалансированной правовой основы в области перспективных решений.

Правовые эксперименты, которые проводятся в настоящее время, в скором будущем приведут к правовой трансформации многих правовых институтов, и в первую очередь института персональных данных.

Данная стадия отдельно выделяется нами также и в целях реализации прогностической функции правовой науки, чем, в частности, и обусловлен выбор темы научного исследования.

В результате совершенствования законодательства в сфере защиты ПДн был достигнут положительный результат в части должного и эффективного правового

---

[96] Федеральный закон от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности» // Собрание законодательства РФ. – 2022. – № 29 (ч. III). – Ст. 5233.

регулирования сферы обработки ПДн, но следует отметить проблему недостаточной ответственности за совершение преступлений с незаконным использованием ПДн. В Уголовном кодексе Российской Федерации[97] (далее – УК РФ) недостаточно проработан состав преступления, который бы непосредственно касался ПДн, что не способствует эффективному поддержанию законности, даже несмотря на новые статьи УК РФ.

Вопросы уголовно-правовой охраны персональных данных в своих исследованиях также поднимают А.Ю. Волкова [98], Е.В. Хохлова [99], М.А. Ефремовой [100], Д.Ю. Крюков и Ю.В. Мокрецов [101], что отдельно свидетельствует об актуальности подчеркиваемой проблемы.

В рамках ст. 274 УК РФ установлена уголовная ответственность лишь за нарушение правил обработки и (или) передачи охраняемой компьютерной информации, при условии, что такое нарушение повлекло за собой крупный ущерб, а равно уничтожение, блокирование, модификацию либо копирование.

Данный состав преступления относится к категории преступлений средней тяжести, но может относиться к тяжким – при наличии дополнительных квалифицирующих признаков (тяжкие последствия в виде длительной приостановки или нарушения работы предприятия, учреждения или организации, получения доступа к информации, составляющей охраняемую законом тайну, предоставления к ней доступа неограниченному кругу лиц, причинения по неосторожности смерти, тяжкого вреда здоровью хотя бы одному человеку[102]).

---

[97] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.

[98] Волкова А.Ю. Персональные данные как объект уголовно-правовой охраны // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3. – С. 138.

[99] Хохлова Е.В. Об охране персональных данных уголовным законом. [Электронный ресурс]. Режим доступа: https://elibrary.ru/thguiy (дата обращения: 11.11.2025).

[100] Ефремова М.А. Уголовно-правовая охрана информационной безопасности: дис. ... докт. юрид. наук. М., 2017. – С. 29.

[101] Крюков Д.Ю., Мокрецов Ю.В. Актуальные проблемы правового регулирования оборота и защиты персональных данных в России // Вестник института: преступление, наказание, исправление. – 2017. – № 2 (38). – С. 37.

[102] Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершённых с использованием электронных или информационно-

Поддерживая позиции ранее упомянутых отечественных правоведов, в свою очередь, считаем минимально необходимым установление уголовной ответственности в виде наиболее общего состава преступления, который будет заключаться в неправомерных действиях с персональными данными или иной охраняемой законом информацией при условии, если такие деяния повлекли тяжкие последствия.

При этом категорию «тяжкие последствия» в данном случае можно использовать путём бланкетной нормы на ранее цитируемый пункт 14 Постановления Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершённых с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».

При этом к числу «тяжких последствий» следовало бы добавить причинение крупного ущерба. Поскольку весьма вероятна такая ситуация, при которой могут отсутствовать тяжкие последствия, которые предусмотрены п. 14 Постановления Пленума Верховного Суда РФ от 15.12.2022 № 37 (тяжкие последствия в виде длительной приостановки или нарушения работы предприятия, учреждения или организации, получения доступа к информации, составляющей охраняемую законом тайну, предоставления к ней доступа неограниченному кругу лиц, причинения по неосторожности смерти, тяжкого вреда здоровью хотя бы одному человеку), а предлагаемый нами состав преступления сформулирован в виде материального, т.е. обязательным элементом объективной стороны такого преступления является наличие последствий.

Иными словами, в случае если оставить в неизменном виде тяжкие последствия в формулировке п. 14 Постановления Пленума Верховного Суда РФ от 15.12.2022 № 37 – будет отсутствовать состав преступления и, как следствие, не будет наступать уголовная ответственность. А это, в свою очередь, негативно

телекоммуникационных сетей, включая сеть «Интернет» // Бюллетень Верховного Суда РФ. – 2023. – № 3.

скажется на уровне уголовно-правовой охраны отношений в области персональных данных.

Помимо этого, в качестве дополнительных квалифицирующих признаков, устанавливающих более суровую меру уголовной ответственности, следовало бы рассматривать совершение преступления группой лиц по предварительному сговору, или организованной группой, или лицом с использованием своего служебного положения.

Вопрос о санкции за совершение предлагаемого нами состава преступления остаётся открытым, но по аналогии с соответствующими составами преступлений (по ст. 274 и 274.1 Уголовного кодекса РФ) предложенные нами составы преступления следовало бы относить к преступлениям средней тяжести, а при наличии вышеупомянутых дополнительных квалифицирующих признаков – к тяжким преступлениям.

Примечательно, что выдвинутое нами предложение уже было частично реализовано по результатам принятия поправок к Уголовному кодексу Российской Федерации [103] . Следует отдельно оговориться, что выдвинутое автором предложение об усилении уголовно-правовой охраны в области ПДн было сформулировано ранее появления законопроекта № 502113-8 [104] (по итогам рассмотрения которого и были приняты вышеназванные поправки в УК РФ) и не опиралось на положение данного законопроекта.

В рамках принятых поправок в УК РФ предусматривается нормативное закрепление нескольких новых оснований для уголовной ответственности по новой статье 272.1 Уголовного кодекса РФ. Однако данные изменения в уголовном

---

[103] Федеральный закон от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // Собрание законодательства РФ. – 2024. – № 49 (ч. IV). – Ст. 7412.

[104] Проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации» (в части установления ответственности за незаконные использование и передачу, сбор и хранение компьютерной информации, содержащей персональные данные) // Система обеспечения законодательной деятельности. [Электронный ресурс]. Режим доступа: https://sozd.duma.gov.ru/bill/502113–8, свободный (дата обращения: 19.12.2024).

законодательстве не лишают научной новизны наши предложения об усилении мер уголовно-правовой охраны по нескольким причинам.

Во-первых, уголовная ответственность по новой статье 272.1 УК РФ устанавливается лишь в случае неправомерных действий только с компьютерной информацией (содержащей персональные данные), а предлагаемые нами составы преступлений не имеют данного ограничения и могут быть применимы для уголовно-правовой охраны любой информации (содержащей персональные данные или иную охраняемую законом информацию), вне зависимости от её формы. Таким образом, ст. 272.1 УК РФ была бы специальной по отношению к предлагаемой автором общей статье УК РФ.

Во-вторых, предлагаемые автором составы преступлений носят наиболее общий характер также ввиду того, что основанием для уголовной ответственности будут любые неправомерные действия с персональными данными или иной охраняемой законом информацией, но при условии, что такое нарушение повлекло тяжкие последствия. Статья 272.1 УК РФ устанавливает уголовную ответственность только за незаконное использование, или передачу, или сбор, или хранение компьютерной информации (содержащей персональные данные), а также в отношении функционирования программного обеспечения, предназначенного для таких действий. При этом предлагаемая автором статья может быть применена и во всех остальных случаях.

Таким образом, нововведения в УК РФ никак не препятствуют выводу о научной новизне предлагаемых автором положений об усилении мер уголовно-правовой охраны в области ПДн, а наоборот, свидетельствуют о достоверности данных научных выводов, поскольку тем самым успешно выполняется прогностическая функция научного исследования. Иными словами, автором верно выявлена проблема (проблема недостаточности мер уголовно-правовой охраны в области ПДн), верно предложен юридический механизм решения данной проблемы (установление новых составов преступлений в области ПДн), а также верно определено, что предлагаемые меры уголовно-правовой охраны должны носить широкий характер (объективная сторона преступления должна быть представлена

наиболее широким образом, но с учётом уточнения в части наличия тяжких последствий).

Новые правила обработки персональных данных требуют от операторов заранее уведомлять Роскомнадзор о каждой трансграничной передаче ПДн. Это усложняет бизнес-процессы и влечёт дополнительные издержки на юристов, что порождает дополнительные финансовые издержки предпринимателей, а как следствие, на конечных пользователей.

Важно особо подчеркнуть и современные правовые проблемы регулирования обработки персональных данных при запуске цифровых профилей, связанные с неполным соответствием общих норм об обработке персональных данных служащих со специальными, касающимися конкретно служебной деятельности и противодействия коррупции, на которые особо обращают внимание в своих исследованиях С.Е. Чаннов[105] и И.И. Игумнов[106].

Таким образом, все вышеперечисленные проблемы свидетельствуют о том, что действующее законодательство нуждается в принятии редакционных поправок. Как справедливо отмечает И.А. Михайлова, российское законодательство, действующее в сфере охраны ПДн, уже включающее в себя обширный круг федеральных законов и нормативных правовых актов, в настоящее время находится в стадии становления[107].

В этой связи уместно привести некоторые программные документы, которые определяют вектор государственной политики в области публично-правовой охраны в области киберпространства, в том числе в области правоотношений по поводу ПДн.

24 декабря 2024 года Генеральной Ассамблеей ООН была принята резолюция 79/243, которой утверждена «Конвенция Организации Объединенных Наций против

---

[105] Чаннов С.Е. Некоторые вопросы анализа цифровых профилей государственных и муниципальных служащих в целях противодействия коррупции // Кадровик. – 2025. – № 6.
[106] Игумнов В.В. Публично-правовое регулирование цифрового профилирования в Российской Федерации. – М., 2024.
[107] Михайлова И.А. Персональные данные и их правовая охрана: некоторые проблемы теории и практики // Законы России: опыт, анализ, практика. – 2017. – № 10. – С. 17.

киберпреступности; укрепление международного сотрудничества в борьбе с определёнными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям» [108] (далее – «Конвенция ООН о киберпреступности»). Данный международно-правовой документ предусматривает порядок и формы международного сотрудничества в области обеспечения безопасности киберпространства и борьбы с киберпреступлениями. Конвенцией ООН о киберпреступности предлагается криминализовать некоторые деяния, совершаемые с помощью различной компьютерной техники и иных устройств.

В частности, в рамках реализации положений Конвенции ООН о киберпреступности планируется установить ответственность (уголовную или административную) за неправомерный доступ, перехват, воздействие, подлог, хищение, отмывание доходов, полученных преступным путём, а также за различные преступные действия сексуального характера. При этом квалифицирующим признаком для наступления публично-правовой ответственности во всех вышеперечисленных случаях будет способ совершения такого деяния – посредством различных неправомерных действий с помощью компьютерной техники и иных устройств или посредством различных неправомерных действий с электронными данными (в том числе с персональными данными).

Особый интерес в этой связи вызывает ст. 9 Конвенции ООН о киберпреступности, в рамках которой как раз предполагается, что каждое государство-участник этой Конвенции в качестве уголовного преступления установит следующий состав: «неправомерное повреждение, удаление, порча,

---

[108] Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определёнными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям. [Электронный ресурс]. Режим доступа: https://www.un.org/ru/documents/treaty/A-RES-79-243, свободный (дата обращения: 01.02.2025).

изменение или блокирование электронных данных» [109], если такие деяния совершены умышленно и с причинением серьёзного ущерба.

Иными словами, положения Конвенции ООН о киберпреступности полностью поддерживают выдвинутое автором положение о необходимости нормативного закрепления уголовной ответственности в виде наиболее общего состава преступления, который будет заключаться в неправомерных действиях с персональными данными или иной охраняемой законом информацией при условии, если такие деяния повлекли тяжкие последствия.

Информационная безопасность личности, в частности персональные данные, включает правовое регулирование не только международными актами и национальным законодательством, но и судебной практикой, как было особо отмечено в правовом исследовании А.А. Чеботаревой[110]. Однако следует заметить, что одних лишь законодательных изменений будет недостаточно для достижения целей эффективного функционирования правового института персональных данных. Наиболее успешно такая задача может быть решена при наличии таких факторов общественной жизни, как тесное взаимодействие государства, граждан и бизнеса; повышение уровня правовой культуры; а также наиболее полное информирование граждан при предоставлении своих ПДн о правовых последствиях совершения ими соответствующих действий в отношении персональных данных, о своих правомочиях в связи с предоставлением ПДн и порядке их реализации.

Возвращая фокус нашего исследования к анализу правового регулирования использования цифровых технологий при обработке персональных данных - обратим своё внимание на содержании и объёме двух парных правовых категорий: «охрана персональных данных» и «защита персональных данных».

---

[109] Там же.

[110] Чеботарева А.А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе. [Электронный ресурс]. Режим доступа: http://igpran.ru/prepare/a.persons/ChebotarevaAA/Chebotareva_avtoref.pdf (дата обращения: 11.11.2025).

Механизм правового регулирования – это взятая в единстве система правовых средств, при помощи которой обеспечивается результативное правовое воздействие на общественные отношения[111]. Некоторые учёные правоведы[112] в вопросе о данном понятии придерживаются более широкого подхода к толкованию, включая в объём правовой категории «правовое регулирование» правовые стимулы и ограничения, правовую культуру и уровень правосознания, нормы права и акты реализации норм права, а также элементы правоотношений.

При этом классический подход к определению понятия «правовое регулирование» в наиболее общем виде понимается как реализуемый на практике процесс воздействия правовых средств на конкретные общественные отношения[113].

Вопрос о безопасности обрабатываемых ПДн является приоритетным вопросом Российской Федерации, что следует из положений Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утверждённой Указом Президента Российской Федерации от 09.05.2017 № 20, а также национального проекта «Экономика данных и цифровая трансформация государства», утверждённого протоколом Президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 20 декабря 2024 года № 12-пр, регулирующих публично-правовые отношения в сфере персональных данных. Несмотря на значимость вопросов защиты и охраны прав человека, в научной литературе и законодательстве до сих пор не существует единого подхода к таким ключевым понятиям, как «правовая защита ПДн» и «правовая охрана ПДн». Эти термины широко применяются в общей теории права, конституционном праве и других юридических науках, но, на наш взгляд и взгляд ряда учёных[114], нуждаются в дальнейшей разработке.

---

[111] Алексеев С.С. Общая теория права: учебник. – 2-е изд., перераб. и доп. – М.: ТК Велби; Проспект, 2008. – С. 267.

[112] Абдулаев М.И. Теория государства и права: учеб. для выс. учеб. заведений. – М.: Магистр-Пресс, 2004. – С. 410.

[113] Комаров С.А. Общая теория государства и права: курс лекций. – М., 1996. – С. 9.

[114] Бобров К. О разграничении понятий «правовая охрана» и «правовая защита» человека // Закон и право. – 2008. – № 8. – С. 37.

Защита и охрана представляют собой важные аспекты функционирования государства и общества. Однако в законодательстве не проводится чёткое разграничение между этими понятиями, и их содержание может совпадать в определённых ситуациях, что может привести к затруднениям в правильном понимании и применении соответствующих норм и правил.

Отсутствие единой терминологии в области защиты и охраны также создаёт проблемы для учёных и исследователей, которые занимаются изучением этих вопросов. Им приходится использовать различные подходы и критерии для определения и анализа данных понятий, что может приводить к различным выводам и неверным интерпретациям.

Таким образом, отсутствие чёткого разграничения между защитой и охраной в законодательстве указывает на необходимость более глубокого изучения и систематизации соответствующих норм и правил. Это позволит повысить эффективность публично-правовой системы и обеспечить более надёжную охрану/защиту прав и интересов граждан и общества как в вопросах безопасности обработки ПДн, так и в целом.

Многие учёные (Н.С. Малейн[115], С.Н. Кожевников[116], Э.П. Гаврилов[117], А.П. Сергеев[118], А.В. Тарасова[119], В.М. Шарифов[120], О.С. Иоффе[121], Е.А.

[115] Малеин Н.С. Охрана прав личности советским законодательством. – М.: Проспект, 1985. – С. 18–19.
[116] Коженинков С.Н. Меры защиты в советском праве»: автореф. дис. … канд. юрид. наук. – Свердловск, 1968. – С. 4–5.
[117] Гаврилов Э.П. Комментарий к Закону «Об авторском праве и смежных правах». – М.: Былинина, 1996. – С. 217.
[118] Гражданское право / под ред. Ю.К. Толстого, А.П. Сергеева. – СПб., 1996.
[119] Тарасова В.А. Охрана прав граждан в пенсионном обеспечении. – М.: Практика, 1978. – С. 23 24.
[120] Шафиров В.М. Обеспечение права: человекоцентристский подход: монография / В.М. Шафиров. – Красноярск, 2005. – С. 130–135.
[121] Иоффе О.С. Гражданско-правовая охрана интересов личности / под ред. Б.Б. Черепахина. – М.: Юридическая литература, 1969. – С. 3–4.

Суханов[122], Н.И. Матузов[123], Н.С. Малеин[124]) придерживаются мнения и позиции, что термин «защита» по своему объёму меньше термина «охрана».

Охрана прав – это более широкое понятие, которое включает в себя все юридические нормы, связанные с определённым благом. Защита права подразумевает те законодательные меры, которые применяются в случае нарушения права. Если исходить из такой позиции, то следует сделать вывод о том, что концептуально неверно использовать термин «защита» самостоятельно, в отрыве от термина «охрана», в отношении обеспечения безопасности ПДн и правового обеспечения конституционных прав и гарантий человека и гражданина.

Другие же учёные (Л.С. Явич[125], А.Ф. Черданцев[126], З.В. Макарова[127], Л.О. Красавчикова[128]), наоборот, считают, что термин «защита» шире «охраны» и что термин «защита» более результативно раскрывает смысл и суть действий. Если придерживаться подобной позиции в отношении обработки ПДн, то, на наш взгляд, теряется сама роль слова и термина «охрана», выраженная в превентивности и постоянности воздействия определённых правовых средств на общественные отношения.

Кроме прочего, в правовой науке также поддерживается мнение о различии данных понятий по временному критерию: охрана осуществляется постоянно, а защита происходит только при нарушении охраняемых прав[129]. Встречается и

---

[122] Гражданское право: в 4 т. Т. 1: Общая часть: учеб. для студентов вузов, обучающихся по направлению 521400 «Юриспруденция» и по специальности 021100 «Юриспруденция» / отв. ред. Е.А. Суханов. – 3-е изд., перераб. и доп. – М.: Волтерс Клувер, 2006. – С. 175.

[123] Матузов Н.И. Правовая система и личность. – Саратов: Изд-во Сарат. ун-та, 1987. – С. 130– 131.

[124] Малеин Н.С. Охрана прав личности советским законодательством. – М.: Наука, 1985. – С. 18– 19.

[125] Явич Л.С. Общая теория права. – Л.: Изд-во Ленинград. ун-та, 1976. – С. 219.

[126] Черданцев А.Ф. Теория государства и права: учеб. для вузов. – М.: Юрайт-М, 1999. – С. 115.

[127] Макарова З.В. Защита в российском уголовном процессе: понятие, виды, предмет и пределы // Правоведение. – 2000. – № 3. – С. 219.

[128] Красавчикова Л.О. Личная жизнь граждан под охраной закона. – М.: Право, 1983. – С. 33.

[129] Матузов Н.И. Правовая система и личность. – Саратов: Сфера, 1987. – С. 130–131.

позиция учёных (Г.Н. Стоякин [130], Н.А. Боброва [131], И.В. Ростовщиков [132], Н.В. Витрук[133], С.С. Алексеев[134], А.В. Стремоухов[135]) о том, что термины «охрана и «защита» синонимичны и тождественны. Либо разграничение понятий нецелесообразно ввиду того, что термин «охрана» практически не применяется в законодательстве, является доктринальным и поэтому не может считаться юридически значимым[136].

А.С. Мордовец[137] и Жорина А.В.[138] высказывали свои позиции по данному вопросу о том, что понятия «охрана» и «защита» взаимосвязаны, взаимозависимы, но являются отдельными правовыми институтами, имеющими самостоятельное нормативное закрепление, субъектный состав и механизмы реализации.

К интересным и заслуживающим отдельного внимания исследованиям относятся труды К.О. Боброва [139]: автором выделяются четыре концепции понимания терминов среди учёных и возможность различия понимания данных категорий исходя из целей их применения.

Интересное исследование по употреблению похожих правовых терминов в США провела О.В. Журкина [140] и пришла к выводу, что термин «защита»

---

[130] Стоякин Г.Н. Понятие «защита гражданских прав» // Проблемы гражданско-правовой ответственности и защиты гражданских прав. – Свердловск: Госиздат, 1973. – С. 30–35.
[131] Боброва Н.А. Гарантии реализации государственно-правовых норм // Закон. – 1984. – С. 95.
[132] Ростовщиков И.В. Права личности в России: их защита и обеспечение органами внутренних дел // Правоведение. – 1997. – С. 77–92.
[133]Витрук Н.В. Законность: понятие, защита и обеспечение // Общая теория права: курс лекций / под ред. В.К. Бабаева. – Нижний Новгород: Асгард, 1993. – С. 528–529.
[134] Алексеев С.С. Общая теория права. Т. 1. – М., 1981.
[135] Стремоухов А.В. Право человека на защиту и формы его защиты в Российской Федерации // Ленинградский юридический журнал. – 2017. – № 1 (47). – С. 36.
[136] Шубина Т.Б. Теоретические проблемы защиты права: автореф. дис. … канд. юрид. наук. Самара. – 1997. – С. 17.
[137] Мордовец А.С. Социально-юридический механизм обеспечения прав человека и гражданина. – Саратов, 1996. – С. 88.
[138] Жорина А.В. Соотношение понятий «охрана» и «защита авторских прав». [Электронный ресурс]. Режим доступа: https://sibadvokat.ru/statiy/sootnoshenie-ponyatiy-ohrana-i-zashhita-avtorskih-prav?ysclid=lw29obb85r101925365, свободный (дата обращения: 01.06.2025).
[139] Бобров К. О разграничении понятий «правовая охрана» и «правовая защита» человека // Закон и право. – 2008. – № 8. – С. 36–38.
[140] Журкина О.В. Нормы международного права и их влияние на национальное законодательство в вопросе о соотношении понятий «защита» и «охрана» // Matters of Russian and International Law. [Электронный ресурс]. Режим доступа: http://www.publishing-vak.ru/file/archive-law-2013-9/6-zhurkina.pdf, свободный (дата обращения: 01.06.2025).

рассматривается как два составных элемента: часть и целое. Процессуальное понятие «защита» (defend) является частью общего понятия защиты как правовой категории (protection). В этой связи считает необходимым использовать только термин «защита» для цели приведения в соответствие с нормами международного права.

Признавая научную полезность и интересность иных позиций относительно вопроса о соотношении данных понятий, в рамках нашего исследования мы будем придерживаться мнения учёных о том, что эти понятия не тождественны: понятие «охрана прав» шире «защиты прав». Охрана прав проявляется непрерывно и постоянно, независимо от того, нарушено ли охраняемое право, включает превентивные меры, меры контроля, направленные на недопущение нарушения прав, создание условий беспрепятственного удовлетворения прав лиц. Защита применяется в том случае, если необходима реализация активных мер, направленных на восстановление нарушенных прав субъектов персональных данных.

Отсутствие единой терминологической правовой базы явным образом наблюдается в процессе анализа основных целей и задач нормативных правовых актов, регулирующих обеспечение безопасности как более широких общественных отношений, так и отношений, связанных с обработкой ПДн в частности.

Термин «защита ПДн» широко используется в основных законах, регулирующих обработку ПДн в Российской Федерации. В Федеральном законе № 152-ФЗ[141] термин «защита» встречается сто пятьдесят раз, тогда как термин «охрана» встречается всего два раза и только в рамках регулирования обработки ПДн в соответствии с Федеральным законом № 57-ФЗ «О государственной охране»[142].

---

[141] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.

[142] Федеральный закон от 27.05.1996 № 57-ФЗ «О государственной охране» // Собрание законодательства РФ. – 1996. – № 22. – Ст. 2594.

Семь раз термин «охрана» присутствует в Федеральном законе № 149-ФЗ[143] в контексте охраны результатов интеллектуальной деятельности и сведений, относящихся к тайне. Термин «защита» присутствует сорок пять раз. Таким образом, в специальных законах, регулирующих вопросы обработки ПДн, больший приоритет отдается термину «защита ПДн».

В Конституции Российской Федерации используются термины «защита» и «охрана» в практически одинаковой доле (двадцать раз употребляется правовая категория «охрана» и сорок три раза – «защита»).

Федеральный закон № 152-ФЗ в соответствии со ст. 2 определяет своей целью «обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну».

Федеральный закон № 3-ФЗ «О полиции»[144] в ст. 1 раскрывает назначение полиции: «…для защиты жизни, здоровья, прав и свобод … для противодействия преступности, охраны общественного порядка, собственности и для обеспечения общественной безопасности».

Кодекс Российской Федерации об административных правонарушениях[145] в соответствии с ст. 1.2 задачами выделяет: «…защиту личности, охрану прав и свобод человека и гражданина, охрану здоровья граждан, санитарно-эпидемиологического благополучия населения, защиту общественной нравственности, охрану окружающей среды, установленного порядка осуществления государственной власти, общественного порядка и общественной безопасности, собственности, защиту законных экономических интересов физических и юридических лиц, общества и государства от административных правонарушений, а также предупреждение административных правонарушений».

---

[143] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3448.

[144] Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» // Собрание законодательства РФ. – 2011. – № 7. – Ст. 900.

[145] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195- ФЗ // Собрание законодательства РФ. – 2002. – № 1 (ч. 1). – Ст. 1.

Уголовный кодекс РФ в соответствии с ст. 2 задачами определяет: «…охрану прав и свобод человека и гражданина, собственности, общественного порядка и общественной безопасности, окружающей среды, конституционного строя Российской Федерации от преступных посягательств, обеспечение мира и безопасности человечества, а также предупреждение преступлений».

При рассмотрении норм Гражданского кодекса РФ становится очевидным, что оба понятия (охрана и защита) используются без какой-либо системы, причём даже как равнозначные[146].

Законодательство не проводит чёткого различия между защитой и охраной во многих случаях, и содержание этих понятий совпадает. Нет единой терминологии. При таком подходе грань между терминами фактически отсутствует или, по мнению некоторых учёных, весьма тонко разграничиваема[147].

Для более ясного определения и проявления терминологического различия терминов необходимо обратиться к методу толкования, выраженному в исследовании значения слов, проанализировать грамматическую (языковую) сущность. Данный метод используется для цели понимания значения терминов «охрана» и «защита».

Смысловое значение слово «защищать» раскрывается следующим образом:

В соответствии с словарем Д.Н. Ушакова [148] обозначает: «оборонять, ограждать от враждебных, неприязненных действий, от неприятеля. … Предохранять от чего-н. вредного… Выступать на суде в качестве чьего-н. защитника. … Вступаться за кого-что-н., отстаивать кого-что…».

---

[146] Никитченко А.А. Теоретико-правовые аспекты соотношения понятий «охрана» и «защита» результатов интеллектуальной деятельности // Вестник ТОГУ. – 2012. – № 1 (24). – С. 268.

[147] Бобров К. О разграничении понятий «правовая охрана» и «правовая защита» человека // Закон и право. – 2008. – № 8. – С. 36–38.

[148] Толковый словарь русского языка: т. 1–4 / сост. Г.О. Винокур, Б.А. Ларин, С.И. Ожегов [и др.]; под ред. Д.Н. Ушакова. – М.: Гос. ин-т «Советская энциклопедия», 1935. – С. 522.

В соответствии с словарем В.И. Даля[149] обозначает: «защитить что, кого, оберегать, охранять, оборонять, отстаивать, заступаться, не давать в обиду; закрывать, загораживать охраняя, защищать себя; быть защищаемым».

В свою очередь, смысловое значение слово «охранять» раскрывается следующим образом:

В соответствии с словарем Д.Н. Ушакова[150] обозначает: «Оберегать, стеречь, защищать, принимая меры для безопасности, для сохранения…».

В соответствии с словарем В.И. Даля[151] обозначает: «охранить что, кого, стеречь, беречь, оберегать, сторожить, караулить; боронить, защищать, безопасить, крыть, отстаивать, заступать, застаивать, держать в целости, сохранно, спасать…».

Лексический анализ толкования слов показал, что в русском языке слова «охранять» и «защищать» крайне тождественны (Ю.В. Самович[152]) и в них нет яркого и принципиального различия, но кажется, что слово «охранять» включает в себя более широкое значение, чем слово «защищать». Слово «охранять» включает и вбирает в себя как защиту, так и меры для обеспечения безопасности, сохранения, предостережения, тогда как толкование слова «защита» ограничивается непосредственным отстаиванием интересов.

При осуществлении грамматического анализа к такому же выводу приходит и ряд таких учёных, как А.А. Никитченко[153], Н.В. Остапюк, Д.Н. Латыпов[154] и

---

[149] Толковый словарь русского языка. Современная версия / В.И. Даль. – М.: Эксмо, 2004. – С. 341.

[150] Толковый словарь русского языка: т. 1–4 / сост. Г.О. Винокур, Б.А. Ларин, С.И. Ожегов [и др.]; под ред. Д.Н. Ушакова. – М.: Гос. ин-т «Советская энциклопедия», 1935. – С. 652.

[151] Толковый словарь русского языка. Современная версия / В.И. Даль. – М.: Эксмо, 2004. – С. 487.

[152] Самович Ю.В. О понятии правовая защита // МИТС-Наука: международный научный вестник: сетевое электронное научное издание. – 2006. – № 1. – С. 32.

[153] Никитченко А.А. Теоретико-правовые аспекты соотношения понятий «охрана» и «защита» результатов интеллектуальной деятельности // Вестник ТОГУ. – 2012. – № 1 (24). – С. 268.

[154] Остапюк Н.В. Указ. соч. С. 11; Латыпов Д.Н. Соотношение охраны и защиты гражданских прав // Актуальные проблемы российского права. – 2009. – № 1. – С. 179.

Н.Н. Изотов[155]. Хотя иного вывода придерживается А.А. Волова[156], делая вывод из анализа толкования слов, что слово «защищать» шире, что ещё раз подчеркивает схожесть восприятия и противоречивость понятий.

Для решения вопроса о разделении и взаимосвязи понятий «правовая охрана» и «правовая защита» необходимо, чтобы законодатель закрепил определение и содержание этих понятий в соответствующих нормативных правовых актах, а также указал их взаимодействие в рамках конкретных отраслей права[157].

Мы считаем, что для целей законодательного развития, в том числе развития правового регулирования обработки ПДн, необходимо определить чёткую терминологическую базу, в том числе вывести и законодательно закрепить понятия «охрана» и «защита». А.П. Смирнов[158] также отмечает, что уяснение содержания понятий «охрана права» и «защита права» действительно важно для решения общетеоретической задачи определения понятия «юридические средства». Совокупность таких средств обеспечивает эффективную государственную, судебную и правовую защиту и охрану субъективных прав.

По нашему мнению, термины «защита ПДн» и «охрана ПДн» различаются и требуют разного определения. Более верным в отношении достижения цели в безопасной обработке ПДн и обеспечения конституционных прав граждан в отношении их личной (персональной) информации является закрепление разных понятий, где «охрана ПДн» шире, чем «защита ПДн».

Охрана прав происходит непрерывно и постоянно, независимо от того, было ли право нарушено. Она включает превентивные меры и контроль, направленные на предотвращение нарушений. Защита применяется, когда необходимы активные действия для восстановления нарушенных прав субъектов персональных данных.

---

[155] Изотов Н.Н. Взаимосвязь «защиты» и «охраны» интеллектуальной собственности // Юриспруденция. – 2005. – № 8. – С. 39.

[156] Волова А.А. Соотношение понятий «правовая охрана» и «правовая защита» // Молодой учёный. – 2023. – № 43 (490). – С. 187.

[157] Бобров К. О разграничении понятий «правовая охрана» и «правовая защита» человека // Закон и право. – 2008. – № 8. – С. 37.

[158] Смирнов А.П. Соотношение понятий «охрана прав» и «защита прав» // Вестн. Том. гос. ун-та. – 2010. – № 331. – С. 43.

Данное предложение касается не только правовых отношений, связанных с регулированием персональных данных, но и в целом всех отраслей права.

Последствием введения разных терминов является комплексный пересмотр правовых норм, принятие соответствующих поправок практически в каждый нормативный акт, в том числе принятие поправок в Конституцию РФ, что кажется маловероятным и утопическим, поскольку в соответствии со ст. 135 Конституции РФ положения глав 1, 2 и 9 не могут быть изменены иначе, чем путём принятия новой Конституции.

По вышеназванным причинам, с учётом уже принятых нормативных правовых актов, сложившегося синонимического понимания данных терминов на законодательном уровне, невозможности комплексной терминологической систематизации на данном этапе развития отечественного законодательства требуется, как меньшая из мер, закрепление синонимичности понятий, вывести это понятие и разрешить возможные споры и научную полемику по вопросу объёма и целей каждого из терминов.

Резюмируя наше исследование по поводу обеспечения правового регулирования в сфере использования цифровых технологий при обработке персональных данных, следует остановиться на определённых выводах и позициях:

1. Публично-правовое регулирование персональных данных, обрабатываемых с использованием цифровых технологий, осуществляется не только на уровне государства, но и на международном уровне, посредством применения различных международных договоров и иных международных актов.

В Российской Федерации публично-правовое регулирование персональных данных, обрабатываемых с использованием цифровых технологий, осуществляется нормами специального Федерального закона «О персональных данных», а также законодательством о безопасности критической информационной инфраструктуры и законодательством об информации и информационных технологиях.

2. Для цели развития науки информационного права автором сформулированы и представлены стадии становления публично-правового регулирования персональных данных:

1) стадия концептуального развития принципов неотъемлемости информационных прав и свобод человека;

2) стадия развития международно-правового регулирования обработки ПДн посредством закрепления правовых основ и принципов;

3) стадия становления и развития национального законодательства в зарубежных юрисдикциях в сфере регулирования обработки ПДн;

4) стадия становления и развития отечественного законодательства в сфере публично-правового регулирования ПДн;

5) стадия правовой трансформации в области правового регулирования обработки персональных данных в условиях развития цифровых технологий.

3. Обоснована недостаточность имеющихся средств уголовно-правовой защиты общественных отношений в области персональных данных, несмотря на введение ст. 272.1 в УК РФ. Ввиду чего предложено установить уголовную ответственность за совершение деяния, которое выражается в «неправомерных действиях с персональными данными или иной охраняемой законом информацией при условии, если такие деяния повлекли тяжкие последствия»

Тяжкие последствия в настоящем случае понимаются в смысле соответствующих положений Постановления Пленума Верховного Суда РФ от 15.12.2022 №37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».

Обоснованность данного предложения дополнительно заключается в реализации взятых на себя Российской Федерацией обязательств в рамках Конвенции ООН о киберпреступлениях.

Помимо этого, в качестве дополнительных квалифицирующих признаков, устанавливающих более суровую меру уголовной ответственности, следовало бы рассматривать совершение преступления группой лиц по предварительному сговору, или организованной группой, или лицом с использованием своего служебного положения.

Вопрос о санкции за совершение предлагаемого нами состава преступления остаётся открытым, но по аналогии с соответствующими составами преступлений (по ст. 274 и 274.1 Уголовного кодекса РФ) предложенные нами составы преступлений следовало бы относить к преступлениям средней тяжести, а при наличии вышеупомянутых дополнительных квалифицирующих признаков – к тяжким преступлениям.

4. С терминологической точки зрения соотношение понятий «охрана персональных данных» и «защита персональных данных» в научно-практических целях следует считать отличными по объёму: «охрана прав» шире «защиты прав». С доктринальных позиций отечественной правовой науки данное утверждение обосновывается тем, что охрана прав проявляется непрерывно и постоянно, независимо от того, нарушено ли охраняемое право, включает превентивные меры, меры контроля, направленные на недопущение нарушения прав, создание условий беспрепятственного удовлетворения прав лиц. Защита применяется в том случае, если необходима реализация активных мер, направленных на восстановление нарушенных прав субъектов персональных данных.

5. Законодательное решение вопроса о соотношении понятий «защита» и «охрана» (в том числе в рамках законодательства о персональных данных) со строгих терминологических позиций нецелесообразно и практически невозможно. Нецелесообразно это, поскольку такое решение повлечёт за собой необходимость внесения многочисленных точечных изменений в огромное число нормативных правовых актов. Но практически нереализуемо это решение потому, что аналогичная терминологическая проблема прослеживается в том числе и в тех главах Конституции РФ, которые не могут быть изменены иначе, чем путём принятия новой Конституции.

ГЛАВА 2. ОСОБЕННОСТИ ПУБЛИЧНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ОТДЕЛЬНЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

§ 1. Особенности публично-правового регулирования в сфере использования искусственного интеллекта при обработке персональных данных

Международные исследования влияния технологий искусственного интеллекта (далее – ИИ) на современные процессы бизнеса и общества [159] подчеркивают особую значимость технологий ИИ в развитии науки и техники. В исследованиях отмечается, что ИИ окажет влияние на все отрасли промышленности и общественной жизни, изменит сложившиеся процессы, анатомию работы сотрудников компаний, сократив время на те или иные задачи, расширив возможности отдельных работников и ускорив влияние технической автоматизации.

Данные тезисы не являются исчерпывающими, что отмечает особую важность своевременного и полноценного анализа влияния ИИ для цели выработки его чёткого, всестороннего и ясного правового регулирования[160]. Ещё в 2017 году издание The Economist опубликовало тезис [161], что в настоящее время самым важным ресурсом более не является нефть, а являются данные. Новый тезис является катализатором к необходимости пересмотреть и актуализировать законодательство в сфере регулирования данных, используемых в технологии ИИ.

---

[159] The economic potential of generative AI: The next productivity frontier. [Электронный ресурс]. Режим доступа: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#key-insights, свободный (дата обращения: 01.06.2025).

[160] Камалова Г.Г. Искусственный интеллект для развития бизнеса и охрана персональных данных: правовые проблемы обеспечения баланса интересов // Право и бизнес: правовое пространство для развития бизнеса в России: коллективная монография: в 4 т. – М.: Проспект, – 2020. – С. 122–130.

[161] Информационная аналитика в издании The Economist. [Электронный ресурс]. Режим доступа: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data, свободный (дата обращения: 01.06.2025).

Проблема правового регулирования персональных данных (далее – ПДн), обрабатываемых с использованием технологий ИИ, становится всё более актуальной в Российской Федерации, особенно в последние несколько лет. При этом главный вопрос – соблюдение баланса между публично-правовыми требованиями по регулированию отношений по поводу ПДн (в том числе охране, обработке) и необходимостью их использования для обучения систем ИИ для целей выполнения задачи повышения доступности и качества данных.

Правовые проблемы регулировании ИИ, а в частности и вопросов обработки ПДн с помощью ИИ, являются насущной проблемой и задачей для стран с развитой и развивающейся экономикой, которые применяют и развивают технологии ИИ. Почти в каждом таком государстве приняты законы, затрагивающие регулирование процессов обработки ПДн, идёт процесс выработки, изменения правового отношения к регулированию технологии ИИ и степени его государственного контроля. В рамках нашей работы прежде всего рассмотрены актуальные правовые инструменты, применимые по отношению к процессам, связанным с ПДн и ИИ в Российской Федерации.

24 апреля 2020 года был принят Федеральный закон № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных»[162] (далее – Федеральный закон № 123-ФЗ).

С принятием Федерального закона № 123-ФЗ стало возможным обрабатывать обезличенные ПДн без согласия субъекта ПДн (идентифицируемого гражданина) для целей повышения эффективности государственного или муниципального управления. Дополнительных пояснений в пояснительной записке, комментариях

[162] Федеральный закон № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // Собрание законодательства РФ. – 2020. – № 17. – Ст. 2701.

или законе не имеется. На территории Москвы и Московской области была предоставлена возможность проведения правового эксперимента, направленного на развитие и применение технологий ИИ. Эксперимент установлен сроком на пять лет, и его период скоро будет завершён.

Обезличивание и дальнейшая обработка допускаются в отношении любых категорий данных, в том числе особых категорий данных (например, медицинских данных, биометрии и прочего), что представляет особый риск для безопасности субъектов ПДн. Подобные послабления в отношении правового регулирования в процессе проведения экспериментов с ИИ являются крайне тревожными в части вероятных утечек данных. Слабая проработка вопросов правового регулирования отношений в данной области, в том числе требований к участникам эксперимента, даёт все основания сомневаться в проработанности подобных решений.

Обращает на себя внимание то, что закрытого перечня обезличивающих персональные данные организаций фактически нет, что допускает обезличивание ПДн всеми участниками эксперимента (включенными в соответствующий реестр) для целей дальнейшего обучения ИИ и совершенствования процессов.

По предположению, выдвинутому ещё в 2020 году А. Зайцевым и Л. Мингазовой[163], возможен один из следующих сценариев:

– обезличиванием данных будут заниматься органы государственной власти и органы местного самоуправления, используя положения Приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию ПДн»[164]. В последующем данные будут передаваться участнику

---

[163] Обзор Федерального закона о проведении в Москве эксперимента в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта. [Электронный ресурс]. Режим доступа: https://zakon.ru/blog/2020/06/10/obzor_federalnogo_zakona_o_provedenii_v_moskve_eksperimenta_v_celyah_sozdaniya_neobhodimyh_uslovij_d?ysclid=ltu6zlfbfy656981848, свободный (дата обращения: 01.06.2025).

[164] Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» // Российская газета. – 2013. – № 208.

экспериментального правового режима на основании соглашения с уполномоченным органом;

– обезличивание данных будут осуществлять сами участники экспериментального правового режима. Соглашение с уполномоченным органом будет содержать требования к процедурам обезличивания ПДн, получаемых участником эксперимента[165].

По истечении четырёх лет эксперимента предположения подтвердились, и, более того, подход стал гибридный. Обработку и обезличивание осуществляют как органы, так и участники эксперимента. Похожий подход реализован в конце 2023 года в Федеральном законе от 08.08.2024 № 233-ФЗ[166].

Сам мораторий вызвал большой резонанс и опасения использования и внедрения ИИ. На обработку личных данных для эксперимента по внедрению ИИ в Москве предлагалось ввести мораторий до 2025 года[167]. Направлялся соответствующий законопроект[168]. В пояснительной записке к законопроекту была поднята проблема отсутствия гарантий использования ИИ исключительно для обеспечения правопорядка и вопрос о том, что отечественные разработки могут содержать серьёзные технические ошибки, что вызовет непредсказуемые последствия для общества.

---

[165] Обзор Федерального закона о проведении в Москве эксперимента в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта. [Электронный ресурс]. Режим доступа: https://zakon.ru/blog/2020/06/10/obzor_federalnogo_zakona_o_provedenii_v_moskve_eksperimenta_v_celyah_sozdaniya_neobhodimyh_uslovij_d?ysclid=ltu6zlfbfy656981848, свободный (дата обращения: 01.06.2025).

[166] Проект федерального закона № 992331-7 «О внесении изменений в Федеральный закон «О персональных данных» (в части уточнения порядка обработки персональных данных). [Электронный ресурс]. Режим доступа: https://sozd.duma.gov.ru/bill/992331-7, свободный (дата обращения: 01.06.2025).

[167] Информация с сайта СПС «Гарант». [Электронный ресурс]. Режим доступа: https://www.garant.ru/news/1364613/, свободный (дата обращения: 01.06.2025).

[168] Проект федерального закона № 950900-7 «О внесении изменения в статью 8 Федерального закона «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве» и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных». [Электронный ресурс]. Режим доступа: https://sozd.duma.gov.ru/bill/950900-7?ysclid=ltu979in6z178864765, свободный (дата обращения: 01.06.2025).

По результатам рассмотрения законопроект был отклонён. В проекте заключения Комитетом Государственной Думы по экономической политике было отдано предпочтение формированию комплексной системы регулирования общественных отношений, возникающих в связи с развитием и использованием технологий ИИ. Отмечена высокая важность эксперимента и то, что для целей развития ИИ необходим определённый порядок обработки данных, специальное регулирование для обработки обезличенных ПДн, отсутствие которого не приведёт к положительным результатам цели эксперимента[169].

С мнением, выраженным в Заключении Комитета Государственной Думы, нельзя не согласиться. Ведь запрет на обработку обезличенных ПДн граждан для целей повышения эффективности государственного или муниципального управления привёл бы к невозможности, фактическому блокированию любых разработок, связанных с развитием и внедрением ИИ в цифровую среду государственного, муниципального управления. Рассмотрение законопроекта Государственной Думой как представителями субъектов, граждан Российской Федерации и его отклонение свидетельствует о готовности общества к правовым экспериментам в области использования ИИ, даже через внедрение исключений в области обработки ПДн граждан. С данной позицией соглашаются и научные представители, такие как И.В. Попова[170] и И.И. Литвин.

С мнением последнего можно также согласиться относительно того, что автоматизированная обработка больших данных, даже обезличенных (ПДн), даёт возможность ИИ более быстрому и эффективному обучению, тогда как ограничения сбора и анализа данных приведут к снижению скорости развития технологий ИИ. Действительно важно найти баланс частных и государственных

---

[169] Добробаба М.Б. Правовое обеспечение защиты персональных данных при использовании технологий искусственного интеллекта // Информационное право. – 2023. – № 3 (77). – С. 37.

[170] Попова А.В. К вопросу о регламентации и содержании системы правовых принципов взаимодействия человека с искусственным интеллектом, роботами и объектами робототехники // Правовое государство: теория и практика. – 2020. – № 4-1 (62). – С. 65.

интересов и выработать наиболее оптимальные решения правового регулирования ИИ[171].

В продолжение рассуждения и анализа актуальных правовых инструментов регулирования ПДн и ИИ нельзя не рассмотреть важный документ для понимания стратегии российского правового регулирования ПДн и ИИ, а именно Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» (далее – Распоряжение № 2129-р)[172].

Распоряжением № 2129-р были зафиксированы правовые цели на период до 2024 года; одной из проблем, описанных в документе, является соблюдение баланса между требованиями по защите ПДн и необходимостью их использования для обучения систем ИИ.

Распоряжение № 2129-р подчеркнуло правовые задачи, которые требуется разрешить:

- обеспечение благоприятных правовых условий для безопасного и ответственного доступа разработчиков систем ИИ и робототехники к данным;
- правовая режимность для доступа к данным, включая ПДн для работы ИИ.

Разработчики Распоряжения № 2129-р обозначили следующие шаги для реализации поставленных задач:

- расширить практику раскрытия данных, содержащихся в информационных ресурсах органов и организаций государственного сектора;
- для обработки обезличенных данных предусмотреть более свободный правовой режим;

---

[171] Литвин И.И. Особенности сбора, обработки и защиты персональных данных искусственным интеллектом // Вестник Уральского юридического института МВД России. – 2021. – № 4. – С. 35.
[172] Распоряжение Правительства РФ от 19.08.2020 № 2129 р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // Собрание законодательства РФ. – 2020. – № 35. – Ст. 5593.

- проработать вопрос целесообразности и возможности определения условий, при которых субъекты профессиональной тайны вправе привлекать для обработки соответствующих сведений сторонние организации (в том числе для раскрытия потенциала облачных технологий и технологий с использованием искусственного интеллекта);
- уточнить правила получения согласия на обработку ПДн для случаев, когда такая обработка осуществляется в сфере ИИ.

В науке информационного права и практике идет поиск решения выявленных проблем, но на данный момент комплексного и системного решения нет.

На настоящий момент стратегия развития ИИ регулируется национальным проектом «Экономика данных и цифровая трансформация государства», утверждённым протоколом Президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 20 декабря 2024 года № 12-пр, и соответствует национальной цели, закреплённой в Указе Президента Российской Федерации от 7 мая 2024 года № 309 «О национальных целях развития Российской Федерации до 2030 года и на перспективу до 2036 года».

Важным условием к минимизации рисков при обработке ПДН при использовании ИИ является применение методов анонимизации. Необходимость реализации мер по анонимизации ПДн при использовании ИИ в ФЗ № 152-ФЗ подчеркивается в Концепции комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики [173] , а также подкрепляется позицией учёных (И.И. Кучерова, С.А. Синицына)[174].

---

[173] Концепция комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики. [Электронный ресурс]. Режим доступа: https://%D0%9E%D1%82%D1%87%D0%B5%D1%82_%D0%98%D0%A2%D0%9E%D0%93_3_%D1%8D%D1%82%D0%B0%D0%BF%20(1).pdf/, свободный (дата обращения: 01.06.2025).

[174] Цифровая экономика: актуальные направления правового регулирования: науч.-практ. пособие / под ред. И.И. Кучерова, С.А. Синицына. – М.: Норма: ИЗиСП, 2022. – С. 268.

Так, поддерживается идея закрепления норм, аналогичных с требованиями к политике в отношении обработки персональных данных в Руководящих принципах СЕ по большим данным применительно к персональным данным:

– «самостоятельно проводить оценку риска повторной идентификации, учитывая временные затраты, необходимые усилия и ресурсы, исходя из характера данных, контекста их использования, доступных технологий для повторной идентификации и сопутствующих расходов.

– подтвердить достаточность принятых мер в отношении анонимных данных и обеспечить результативность процесса деидентификации.

– технические меры могут быть дополнены юридическими или договорными обязательствами, направленными на предотвращение возможной повторной идентификации субъектов данных.

– регулярно пересматривать оценку риска повторной идентификации с учётом развития технологий в области методов анонимизации»[175].

Помимо вышеуказанного, следует обратить внимание и на правовую специфику согласия на обработку обезличенных ПДн, обрабатываемых посредством использования ИИ-технологий.

Задача построения системы правил получения согласия на обработку ПДн для целей использования и обучения ИИ была нормативно закреплена Приказом Росфинмониторинга от 18.04.2023 № 84, в котором было установлено, что не требуются согласия для обработки ПДн, если таковые получены в результате обезличивания персональных данных и используются для обработки их технологией ИИ.

В целом подход, при котором нет необходимости в согласии на обработку ПДн при обезличенной обработке посредством ИИ (с учётом переходного, экспериментального периода, установленного до 2025 года), представляется вполне логичным и удобным. Но, рассматривая вопрос с научной точки зрения,

---

[175] Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. [Электронный ресурс]. Режим доступа: https:// https://rm.coe.int/16806ebe7a#_blank, свободный (дата обращения: 01.06.2025).

возникают сомнения относительно соблюдения конституционных прав и законных интересов субъектов персональных данных. Иными словами, является ли такой подход полноценным правовым подходом, обеспечивающим прозрачность обработки, распространения, передачи данных граждан? Обеспечивает ли данный подход права граждан на ограничение распространения и обработки данных?

В настоящий момент, основываясь на анализе соответствующей нормативно-правовой базы, следует сделать вывод о том, что обезличенные персональные данные обрабатываются без согласия. Такое решение, на наш взгляд, с учётом современного уровня технологий представляется временным и не отвечающим целям Федерального закона № 152-ФЗ [176], так как на сегодняшний день не существует метода, который мог бы полностью обезличить данные с сохранением ценности таких данных[177].

Выдвинутое нами мнение о том, что необходимо отдельное, специальное согласие субъекта ПДн при обработке данных с использованием ИИ, поддерживают и видные учёные в сфере информационного права и технологий, в том числе А.В. Минбалеев, В.А. Филоненкова и А.А. Лазаров[178], отмечая, что большой объём обрабатываемой и генерируемой на её основе информации и данных должен быть контролируемым с чётко определённым ответственным лицом за обработку этих данных[179]. Текущий уровень развития информационных технологий при сборе нескольких наборов данных (в том числе обезличенных) и при последующей математической обработке потенциально может привести к тому, что такого рода данные будут позволять идентифицировать субъекта персональных данных.

---

[176] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.

[177] Матвеева Т. Выступление на Петербургском Международном юридическом форуме. Информация с сайта СПС «Гарант». [Электронный ресурс]. Режим доступа: https://www.garant.ru/news/1464529/?ysclid=ltx7wq8o8o183188278/, свободный (дата обращения: 01.06.2025).

[178] Лазаров А.А. Информационно-правовое регулирование социального кредитования (скоринга): дис. … канд. юрид. наук. – М., 2023. – 226 с.

[179] Минбалеев А.В., Филоненкова В.А. Проблемы защиты персональных данных и цифрового профиля человека в сети «Интернет» в условиях пандемии // Вестник Южно-Уральского государственного университета. Серия: Право. – 2020. – Т. 20. – № 3. – С. 89–94.

Таким образом, обезличивание персональных данных выступает методом снижения рисков нарушения прав субъектов персональных данных при обработке данных с использованием искусственного интеллекта, но само по себе не может обеспечивать абсолютные гарантии полной защиты прав субъектов персональных данных. Обезличенные данные содержат в себе цифровые следы, по которым с использованием технологий искусственного интеллекта возможно установить их соответствие тому или иному субъекту персональных данных. Обезличивание информации технически не даёт гарантию того, что эти данные невозможно будет восстановить и произвести идентификацию с субъектом персональных данных. Некоторые разработчики методов машинного обучения признают, что простые методы анонимизации данных могут быть связаны с риском раскрытия персональных данных[180].

Из этого следует, что права и законные интересы граждан, чьи данные обрабатываются для целей обучения ИИ, могут быть нарушены в связи с тем, что данные могут быть раскрыты неопределённому кругу лиц без согласия и ведома, поскольку субъект персональных данных будет лишён возможности получить информацию о факте обработки персональных данных посредством ИИ.

После правового анализа вопроса о согласии на обработку обезличенных ПДн, обрабатываемых посредством использования ИИ-технологий, для всестороннего и комплексного научного анализа следует обратить внимание на требования по обезличиванию ПДн для целей их обработки ИИ ввиду особой уязвимости в случае утечки ПДн граждан по результатам использования ИИ при обработке ПДн.

Активно разрабатываются методы унификации для искусственного интеллекта, отдельное внимание Минцифры России уделено процедуре

[180] Статья Бена Лорика о методах анонимизации данных. [Электронный ресурс]. Режим доступа: https://www.wipo.int/tech_trends/ru/artificial_intelligence/ask_the_experts/techtrends_ai_lorica.html, свободный (дата обращения: 01.06.2025).

обезличивания, методикам и средствам, чтобы никаким образом невозможно было установить исходные данные и нанести ущерб конкретному гражданину[181].

Законопроект № 992331-7[182] о внесении изменений в Федеральный закон № 152-ФЗ был предложен и рассмотрен Государственной Думой в конце 2023 года, по итогу был принят Федеральный закон от 08.08.2024 № 233-ФЗ[183].

Результатом принятого закона является внедрение особого порядка обработки ПДн, полученных в результате обезличивания ПДн, при формировании состава персональных данных и предоставлении доступа к ним. Ограничена обработка специальных категорий данных и введена обязанность передавать результат обезличенных данных в специальную государственную систему. Сформированы требования и круг пользователей государственной информационной системы уполномоченного органа в сфере регулирования информационных технологий. Данный нормативный правовой акт имеет большую значимость в части изменения фактических процессов обработки персональных данных и ИИ, существенно изменился подход и требования к процессу обработки.

Но, по нашему мнению, подобные правки в законодательство о персональных данных являются временным решением и не позволяют обеспечить должного результата по реализации целей, поставленных Распоряжением № 2129- р и Федеральным законом № 152-ФЗ. Подобные решения приводят лишь к усложнению процедурной стороны обработки персональных данных, не позволяя решить сущностные проблемы. Комплексным же решением всех вышеуказанных

---

[181] Шитов А. Интервью на круглом столе конференции OS DAY 23.06.2023. Информация с сайта РИА Новости. [Электронный ресурс]. Режим доступа: https://ria.ru/20230628/zakon-1880810358.html, свободный (дата обращения: 01.06.2025).

[182] Проект Федерального закона № 992331-7 «О внесении изменений в Федеральный закон «О персональных данных» (в части уточнения порядка обработки персональных данных). [Электронный ресурс]. Режим доступа: https://sozd.duma.gov.ru/bill/992331-7, свободный (дата обращения: 01.06.2025)

[183] Федеральный закон от 08.08.2024 № 233-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202408080031, свободный (дата обращения: 01.06.2025).

проблемных аспектов, по нашему мнению, было бы создание новой области правового регулирования – регулирование ИИ-технологий и, в частности, персональных данных, обрабатываемых с помощью технологии ИИ.

Следовало ожидать попытку сформулировать комплексное решение проблемы обработки ПДн с помощью технологии ИИ в конце 2024 года, в виде отчёта по реализации Распоряжения № 2129-р по окончании действия экспериментального режима, установленного Федеральным законом № 123-ФЗ, но на настоящий момент, до сих пор, законодательно вопрос не урегулирован. Как результат проведённого эксперимента ожидается принятие комплексного федерального закона, регулирующего ИИ и вносящего соответствующие правки в другие нормативные правовые акты в части регулирования процессов, связанных с обработкой обезличенных ПДн с помощью технологии ИИ.

Предположения о том, что требуется комплексное решение проблемы обработки ПДн, полученных в результате обезличивания персональных данных для ИИ, находит своё отражение в информации о создании правового регулирования ИИ, а именно полноценного закона об искусственном интеллекте. Так, в июле 2023 года заместитель главы Минцифры России Александр Шойтов заявил, что «нужно регулировать эту сферу, и мы этим занимаемся, соответствующее регулирование готовится. Одно из направлений – это обезличивание данных. Речь идёт о том, чтобы поэтапно в пилотных проектах, наращивая технологии, переходить к общему регулированию, расширять, масштабировать правильные решения... Сначала должен быть полноценный закон об искусственном интеллекте, у нас такого закона пока нет». Данная позиция подтверждает доводы о том, что частные, не комплексные законопроекты, направленные на правовое регулирование точечных процессов обработки ПДн с использованием ИИ, не могут быть решением глобальной задачи по унификации и регламентации всего правового процесса ИИ в Российской Федерации или даже ЕАЭС.

Проблемы правовой охраны персональных данных, обрабатываемых с использованием технологий искусственного интеллекта, весьма актуальны не

только для отечественного законодателя, но и во многих зарубежных правопорядках, ввиду чего для цели развития науки и права следует обратить внимание на наиболее успешный зарубежный опыт в данной области. Необходимо отметить, что процесс разработки законодательства в части правовой регламентации работы ИИ и смежных процессов идёт по всему миру. Так, в Европейском союзе отмечается активное обсуждение, разработка и внедрение правового регулирования области обработки ПДн, обрабатываемых ИИ, что несомненно подтверждает доводы об общемировой тенденции к регулированию данных и ИИ.

Помимо GDPR, в 2019 году, в рамках рекомендаций Европейского союза, был выработан документ T-PD (2019)01 «Руководство по защите персональных данных при использовании искусственного интеллекта» (Guidelines on artificial intelligence and data protection)[184]. Рекомендации описывают стратегии правового урегулирования сферы ПДн при обработке данных ИИ, а именно общие и частные требования к процессам и политикам обработки ПДн, которые должны учитывать разработчики.

С 2021 года в Европейском союзе рассматривался законопроект о регулировании ИИ[185]. Закон был принят в конце 2023 года и должен был вступить в силу не раньше 2025 года, на настоящий момент не вступил. Важно отметить, что персональные данные в соответствии с принятым законом могут обрабатываться с учётом категорийности высокого риска. Это свидетельствует о подходе, при котором стоит предпринимать особые меры для охраны ПДн в условиях обработки ИИ. В целом анализ и имплементация выработанных решений в законе

[184] Конвенция о защите физических лиц в связи с автоматической обработкой персональных данных (ETS № 108). [Электронный ресурс]. Режим доступа: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108, свободный (дата обращения: 01.06.2025).

[185] Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. [Электронный ресурс]. Режим доступа: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021PC0206, свободный (дата обращения: 01.06.2025).

рекомендуются к анализу для целей комплексного регулирования ИИ в Российской Федерации и помощи в ответах на поставленные проблемы.

Подводя промежуточные итоги исследованию в области публично-правового регулирования в сфере использования цифровых технологий при обработке персональных данных, а в частности – публично-правовому регулированию в сфере использования ИИ при обработке персональных данных, можно постулировать некоторые наиболее важные выводы:

1. Главной проблемой публично-правового регулирования обработки персональных данных с использованием технологий искусственного интеллекта остаётся соблюдение баланса между требованиями по защите персональных данных и необходимостью их использования для обучения систем искусственного интеллекта для цели выполнения задачи повышения доступности и качества данных.

Введение полного запрета на обработку персональных данных с использованием искусственного интеллекта приведёт к фактическому блокированию любых разработок, связанных с развитием и внедрением искусственного интеллекта. Ввиду этого предлагается нормативное закрепление обязанности получения специального согласия на обработку персональных данных при использовании искусственного интеллекта.

2. Обезличивание персональных данных выступает методом снижения рисков нарушения прав субъектов персональных данных при обработке данных с использованием искусственного интеллекта, но само по себе не может обеспечивать абсолютные гарантии защиты прав субъектов персональных данных. Обезличенные данные содержат в себе цифровые следы, по которым с использованием технологий искусственного интеллекта возможно установить их соответствие тому или иному субъекту персональных данных. Ввиду чего требуется наличие отдельного согласия на обработку персональных данных при обработке ПДн с использованием ИИ. Таким образом, развитие публично-правового регулирования обработки персональных данных при использовании и обучении ИИ не будет препятствовать минимизации рисков раскрытия

персональных данных неопределённому кругу лиц без согласия и ведома субъекта. Такое согласие представляется обязательным, по крайней мере до завершения процесса эксперимента и выработки полноценного правого и технического регулирования.

3. Выявлена проблема публично-правового регулирования обработки персональных данных с использованием технологий искусственного интеллекта, которая заключается в необходимости разработки и принятия цельного, единого источника правового регулирования ИИ, в частности при регулировании процессов обработки ПДн с использованием технологии ИИ. Отдельные Федеральные законы не обеспечивают комплексный нормативно-правовой подход к регулированию данной области, а направлены на правовое регулирование лишь точечных процессов обработки ПДн с использованием ИИ.

Предложено решение в виде принятия комплексного федерального закона, регулирующего ИИ, в том числе в части регулирования процессов, связанных с обработкой обезличенных ПДн с помощью технологии ИИ.

§ 2. Особенности публично-правового регулирования в сфере использования технологий распределённого реестра при обработке персональных данных

Технология распределённого реестра (блокчейн-технология) является одной из наиболее передовых цифровых технологий и находится в стадии активной адаптации и масштабирования применительно к различным сферам и областям деятельности. Технология блокчейн может использовать персональные данные при обработке общего массива информации при распределении в разобщённые реестры хранения и обработки данных. Это, в свою очередь, вызывает научный и практический интерес в изучении возможностей публично-правового регулирования обработки ПДн при использовании технологии. В современных условиях цифровизации различных публично-правовых и коммерческих процессов, процедур необходимо уделить отдельное внимание публично-правовому регулированию стремительно развивающейся технологии блокчейн, в связи с чем следует рассмотреть проблемы регулирования обработки персональных данных при использовании данной технологии.

Блокчейн – это распределённая база данных, которая содержит информацию обо всех транзакциях, проведённых участниками системы. Информация хранится в виде цепочки блоков[186]. Ключевая утилита блокчейна – это децентрализованное и защищённое от несанкционированного доступа хранилище данных, которое может выступать в качестве единого неопровержимого источника истины без необходимости более надёжного централизованного посредника. Это позволило применять такие варианты использования этой технологии, как верификация данных, хранение и передача цифровых активов, верификация документов, отслеживание цепочки поставок.

Важно отметить несколько принципиальных моментов для цели понимания правовой специфики обработки персональных данных при использовании блокчейн-технологии. Использование блокчейн-технологии отличается

[186] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic cash system. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 08.07.2025).

следующими ключевыми аспектами: данные хранятся децентрализованным образом, копии баз данных размещаются на нескольких узлах сети, которые часто существуют в различных юрисдикциях. Добавление новых данных в цепочках должно быть проверено и принято большинством узлов сети, то есть достигнут определённый консенсус между узлами сети (участниками построенной архитектуры блокчейн-процесса). Только после достижения консенсуса о добавлении новой информации в сеть данные будут перекопированы и сохранены в блоках цепи. Таким образом, сохранённые данные защищены от несанкционированных действий.

Блокчейн предназначен для того, чтобы быть средой для добавления информации, это означает, что записи, которые были зафиксированы на цепочках/узлах не могут быть отредактированы или удалены. Такое положение, в свою очередь, предоставляет большую устойчивость блокчейн-технологии к несанкционированному доступу, несанкционированному добавлению информации или удалению информации, а также неизменяемость транзакционности сделки, что является ключевым преимуществом для ряда отношений.

Вышеуказанная специфика технологии создает более высокую степень доверия к данным в цепочке блокчейна. При обработке персональных данных посредством блокчейна возникает ряд правовых проблем: проблема удаления информации из блокчейна, а также проблема доступа к информации, которая относится к числу персональных данных.

Такие данные, как имя, адрес, контактный номер и другие, составляют часть метаданных транзакции по цепочке и относятся в соответствии с законом к персональным данным. При этом такие персональные данные хранятся вне сети в открытом виде и доступны по ссылкам для всех участников блокчейн-цепи. Без обеспечения контроля доступа такие данные эквивалентны размещению в сети открытого текста.

Для цели соответствия требованиям публичного нормативно-правового регулирования в области персональных данных необходимо соблюсти одно из ключевых требований, а именно чтобы обработчик персональных данных

установил контроль над кругом лиц, имеющих доступ к персональным данным. Однако при использовании технологии блокчейн это может быть затруднено, так как персональные данные фиксируются по цепочке хранения, доступ к этой цепочке зависит от архитектуры хранения данных, которая должна соответствовать требованиям законодательства об обработке персональных данных.

Главная проблема заключается в том, что в блокчейне практически невозможно контролировать доступ к персональным данным, так как любой участник сети блокчейн (известный или анонимный) может быть оператором узла и/или участвовать в цепочке передачи данных по сети.

Представляется возможным предусмотреть определённые правовые меры для решения заявленных проблем по обработке персональных данных в системе блокчейн, прежде всего, установить обязанность применения технических решений, таких как шифрование для предотвращения несанкционированного раскрытия персональных данных. Возможным решением вопроса будет являться градирование данных и установление разных требований к их обработке или вовсе запрет на обработку. Э.И. Лескина отмечает в своих исследованиях интересный подход к регулированию «правовых режимов данных», связанный с установлением «правового режима персональных данных» для цели соблюдения баланса между правом на информацию и принципом неприкосновенности частной жизни человека, защитой конфиденциальности и содействием внедрению инноваций[187].

Наряду с этим, средством по организации и защите персональных данных в блокчейне является установление обязанности по ограничению срока хранения данных в цепи, то есть настройка системы блокчейн. Таким образом, при возведении определённых программ, процессов, сайтов на базе технологии блокчейн необходимо технически сделать среду, чтобы была возможность ограничивать срок хранения на других устройствах.

---

[187] Лескина Э.И. Доктринальные аспекты правовых режимов данных в условиях развития технологий больших данных // Журнал российского права. – 2024. – Т. 28. – № 7. – С. 122–136. [Электронный ресурс]. Режим доступа: https://jrp.jes.su/s1605-65900000622-5-1-ru-230/, свободный (дата обращения: 11.11.2025).

Как правило, если оператор, обработчик осуществил обработку персональных данных и нет никакой дальнейшей законной цели для обработки, хранения, передачи или каких-либо иных законных требований о хранении данных или иного обращения персональных данных, то оператор, обработчик должен удалить такие персональные данные. Это можно сделать либо путём удаления всей информации, либо путём удаления личных идентификационных персональных данных, которые в дальнейшем ограничивают возможность по персональной идентификации субъекта.

Однако, поскольку данные, передаваемые по цепочке блоков, являются неизменяемыми и не могут быть стёрты или изменены, такое положение вызывает ряд технических проблем. Следовательно, для эффективной утилизации персональных данных, данные должны быть переданы по цепочке таким образом, чтобы после удаления на одном устройстве данные становились неидентифицируемыми для любого, кто может получить доступ к данным по цепочке хранения. Такие мероприятия возможно выполнить, например, с помощью шифрования или удаления ключей дешифрования.

Таким образом, возможно предусмотреть легальную возможность обработки персональных данных с использованием системы блокчейн в приложениях, на сайтах или в прочих ресурсах, которые используют блокчейн для своих процессов. Важно отметить, что многое зависит от того, какая схема блокчейна организована, от чего ставится в зависимость повышение или понижение определённых рисков доступа и несанкционированного доступа к размещённым персональным данным.

На данный момент важно использовать принципы шифрования, дешифрования и иные технические средства, механизмы по увеличению степени надёжности хранящихся персональных данных с учётом особенности системы блокчейн. Важно обратить внимание, что с увеличением растущих мощностей и степени обработки данных в целом в мире увеличение компьютерных мощностей, угроза взлома и доступа к информации, хранящейся в блокчейне, повышается.

В качестве определённого результата наших исследований в области выявления специфики правового регулирования в области персональных данных,

обрабатываемых с использованием технологий распределённого реестра, можно сделать следующие выводы:

1. В целях минимизации рисков, связанных с обеспечением контроля над кругом субъектов, которые могут получить доступ к персональным данным при использовании технологии блокчейн и иных схожих технологий, обоснована необходимость законодательного закрепления обязанности применения операторами персональных данных специальных мер, направленных на реализацию возможности эффективного уничтожения персональных данных в блокчейне (чтобы после удаления на одном устройстве данные становились неразборчивыми для идентификации любого, кто может получить доступ к данным по цепочке хранения), например с помощью шифрования и удаления ключей дешифрования или путём применения технологий управления доступом к данным и технологий доказательства нулевого разглашения.

2. Использование блокчейн-технологии отличается высокой степенью анонимизации, что обеспечивает высокий уровень соблюдения конституционных прав граждан при обработке персональных данных. Учитывая децентрализованное хранение данных, а также специальный порядок действий в отношении блокчейна, при котором сохранённые данные защищены от несанкционированных действий в том числе с использованием инструментов шифрования, использование блокчейн-технологии в большей степени способно гарантировать высокий уровень анонимизации персональных данных. Вышеуказанная специфика технологии распределённого реестра создаёт более высокую степень доверия к данным в цепочке блокчейна.

Установлено, что при обработке персональных данных посредством блокчейна возникает ряд правовых проблем: проблема удаления информации из блокчейна, а также проблема доступа к информации, которая относится к числу персональных данных.

3. Такие данные, как имя, адрес, контактный номер и другие, составляют часть метаданных транзакции по цепочке и являются персональными данными, которые хранятся вне сети, в открытом виде и доступны по ссылкам, которые

хранятся в блокчейне, для всех участников цепи. Без обеспечения контроля доступа такие данные эквивалентны размещению в сети открытого текста и считаются персональными данными.

4. Публично-правовое регулирование в сфере использования технологий распределённого реестра при обработке персональных данных осложнено тем, что затруднительно установить эффективный и точный механизм контроля над кругом лиц, которые могут получить доступ к персональным данным при использовании блокчейн-технологий.

В целях минимизации рисков, связанных с обеспечением контроля над кругом субъектов, которые могут получить доступ к персональным данным при использовании технологии блокчейн и иных схожих технологий, обоснована необходимость законодательного закрепления обязанности применения операторами персональных данных специальных мер, направленных на реализацию возможности эффективного уничтожения персональных данных в блокчейне (чтобы после удаления на одном устройстве данные становились неразборчивыми для идентификации любого, кто может получить доступ к данным по цепочке хранения), например с помощью шифрования и удаления ключей дешифрования.

Таким образом, закрепление требований к обязательному применению шифрования или обязательному удалению ключей дешифрования при обработке ПДн посредством использования технологии блокчейн, а также путём применения технологий управления доступом к данным и технологий доказательства нулевого разглашения является наиболее эффективным правовым механизмом достижения целей и принципов законодательства в области персональных данных.

§ 3. Особенности публично-правового регулирования в сфере использования облачных технологий при обработке персональных данных

Облачные технологии не являются чем-то новым в современном мире технологий. Сама технология появилась и приобрела своё настоящее название ещё в 2006 году, с тех пор развиваясь, и нашла реализацию во многих информационных сферах. Под облачным сервисом (публичным облаком), согласно разъяснениям Национального института стандартизации и технологий США, понимается информационная концепция, предусматривающая предоставление сетевого доступа к вычислительному ресурсу[188].

В настоящее время множество известных сервисов предоставляют доступ пользователям к облачным решениям (публичным облакам), которые не требуют установки программного обеспечения на непосредственно устройство пользователя, не занимают память и не требуют особых мощностей или серверов пользователя публичного облака для развёртывания информационной системы.

Средний уровень общей облачной зрелости российского бизнеса оценён в 35 % из возможных 100 %[189]. Телекоммуникационные, рекламные, товароучётные, CRM-системы имеют облачные решения, которые могут представлять из себя программное обеспечение, платформу или инфраструктуру для цели предоставления услуги. А.И. Савельев также отмечает, что безусловным преимуществом облачных решений является возможность сокращения расходов на

---

[188] Разъяснения Национального института стандартизации и технологий США. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1717182010&tld=ru&lang=ru&name=dk5pes2uk2wyu798vml6uc6jny1jizas.pdf&text=облачным+сервисом+%28публичным+облаком%29%2C+согласно+разъяснениям+Национального+института+стандартизации+и+технологий+США%2C&url=https%3A//ncsa.ru/upload/iblock/4eb/dk5pes2uk2wyu798vml6uc6jny1jizas.pdf&lr=43&mime=pdf&l10n=ru&sign=75a7f0a1e06e4f9bd164d9fc79252a8f&keyno=0, свободный (дата обращения: 01.06.2025).

[189] Исследование облачной зрелости российского бизнеса 2023 // Cloud и «Технологии доверия», 2022. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1717182167&tld=ru&lang=ru&name=tedo-cloud-event.pdf&text=Исследование+облачной+зрелости+российского+бизнеса+2023+//+Cloud+и+«Технологии+доверия»%2C+2022&url=https%3A//data.tedo.ru/technology/tedo-cloud-event.pdf&lr=43&mime=pdf&l10n=ru&sign=f971079df43aabe71075452fd7820e6f&keyno=0, свободный (дата обращения: 01.06.2025).

IT-структуру и повышения уровня обслуживания[190]. По оценкам компании Gartner Group, большая часть банковских транзакций по всему миру осуществляется посредством облачной инфраструктуры[191].

Вышеперечисленные обстоятельства подчеркивают необходимость публично-правового регулирования в сфере использования облачных технологий при обработке персональных данных.

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, утверждённая Указом Президента Российской Федерации от 09.05.2017 № 20[192], подчёркивает роль облачных услуг и их развития, отмечая рост подобных сервисов более чем на 40 % ежегодно. В качестве приоритетных технологий развития были указаны облачные технологии в Распоряжении Правительства России от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»[193].

На настоящий момент стратегия развития ИИ регулируется национальным проектом «Экономика данных и цифровая трансформация государства», утверждённым протоколом Президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 20 декабря 2024 года № 12-пр, и соответствует национальной цели, закреплённой в Указе Президента Российской Федерации от 7 мая 2024 года № 309 «О национальных целях развития Российской Федерации до 2030 года и на перспективу до 2036 года».

Использование облачных технологий при обработке персональных данных сопряжено с рядом правовых рисков, связанных с утечкой персональных данных.

---

[190] Канашевский В.А. Юридические проблемы использования российскими банками облачных услуг зарубежных провайдеров // Lex Russica (Русский закон). – 2019. – № 3 (148). – С. 110.

[191] Кораблев А.В. Идентификация информационных рисков использования облачных технологий в банковской деятельности: дис. … канд. экон. наук. – Самара, 2017. – С. 3.

[192] Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства РФ. – 2017. – № 20. – Ст. 2901.

[193] Распоряжение Правительства России от 28 июля 2017 года №1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» // Собрание законодательства РФ. 2017. – № 32. – Ст. 5138.

Более двух третей облачного рынка в России приходится на компании финансового сектора и сферы ритейла, с чем связано повышенное внимание к правовому регулированию данной области, что отмечается также и в ряде исследований[194]. Так, статистически общий рост утечек ПДн россиян вырос в 40 раз по сравнению с показателями 2021 года[195]. Кроме того, Роскомнадзор подтвердил утечки 600 млн записей о соотечественниках, которые были опубликованы в общем доступе. Суммарно более 140 утечек ПДн было зафиксировано за период с февраля по декабрь 2022 года[196].

В ряде научных исследований подчеркивается актуальность изучения вопросов публично-правового регулирования ПДн в облачных системах [197]. Отмечается, что положения документов стратегического планирования в полной мере отражают и перспективные потребности расширения использования информационных технологий в сфере публичного управления в Российской Федерации[198].

Публичные облака могут быть представлены в нескольких формах (сервисные модели):

– программное обеспечение как услуга (Software-as-a-Service / SaaS);

– платформа как услуга (Platform-as-a-Service / PaaS);

– инфраструктура как услуга (Infrastructure-as-a-Service / IaaS) или

---

[194] См.: Исследование облачной зрелости российского бизнеса 2023 // Cloud и «Технологии доверия», 2022. [Электронный ресурс]. Режим доступа: https:// cloud.ru/ru/research/oblachnyj-rynokrossii-2022, свободный (дата обращения: 01.06.2025); Отчет «Интернет в России в 2022–2023 годах: состояние, тенденции и перспективы развития». [Электронный ресурс]. Режим доступа: https://raec.ru/live/analytics/14235/, свободный (дата обращения: 01.06.2025).

[195] Статистика Роскомнадзора по утечкам данных. [Электронный ресурс] // РБК. 2024. 23 фев. Режим доступа: https://www.rbc.ru/rbcfreenews/65d7ef3d9a7947d8608dbbb3, свободный (дата обращения: 01.06.2025).

[196] Шумилин А.С. Метод обеспечения защиты персональных данных в медицинской облачной системе // Вопросы кибербезопасности. – 2023. – № 4 (56). – С. 53–64.

[197] См.: Бикбулатова Ю.С. Информационно-правовое регулирование отношений, формирующихся при использовании облачных вычислений (сервисно-ориентированных распределённых информационных систем): дис. ... канд. юрид. наук. – М., 2018. – С. 34–35; Викторова Н.Г., Шухов Ф.Г. Цифровая экономика: развитие облачных технологий в России и за рубежом. // Век качества. – 2019. – № 2. – С. 81–90.

[198] Жеребцов А.Н., Малышев Е.А. Применение цифровых технологий в процессе публичного управления миграционными процессами в Российской Федерации // Lex Russica (Русский закон). – 2023. – Т. 76. – № 12 (205). – С. 101–112.

– рабочее место как услуга (Desktop as a Service / DaaS).

Облачные решения бывают разными и могут представлять из себя различные услуги, в связи с чем встречаются такие, отчасти синонимичные, термины, как «облачные сервисы», «облачные информационные системы», «облачные технологии», «облачная инфраструктура», «облачные вычисления».

Все эти термины объединяет то, что обработка информации (вычисления) потребителя услуги происходит удалённо, в облачном пространстве поставщика данной услуги. Облачные сервисы (публичные облака) располагаются на серверах владельца данного сервиса и могут находиться территориально в любой точке мира.

Принятый ГОСТ Р ИСО/МЭК 27018–2020[199] (далее – ГОСТ 27018–2020), идентичный международному стандарту ИСО/МЭК 27018:2019[200], использует понятие «публичное облако» (public cloud) – предоставление услуг SaaS, PaaS, IaaS и/или DaaS для относительно неограниченного круга клиентов[201]. Более научным, по нашему мнению, было бы определить термин не через другие понятия, а через ёмкое словесное определение сути термина, например: публичное облако – это модель предоставления программного обеспечения, при оказании услуг по которой владелец сервиса предоставляет пользователю совокупность информационных технологий и технических средств, обеспечивающих обработку и (или) хранение данных пользователя.

---

[199] ГОСТ Р ИСО/МЭК 27018–2020. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки (утв. и введен в действие Приказом Росстандарта от 10.11.2020 № 1042-ст). – М.: Стандартинформ, 2020.

[200] ИСО/МЭК 27018:2019 «Информационные технологии. Методы обеспечения безопасности. Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки» (ISO/IEC 27018:2019 «Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors»). [Электронный ресурс] // ФГБУ «Институт стандартизации». Режим доступа: https://www.gostinfo.ru/catalog/Details/?id=6444427 (дата обращения: 01.06.2025).

[201] ISO/IEC 17826:2022(en), 3.45 [Электронный ресурс] // ИСО – Международная организация по стандартизации. Режим доступа: https://www.iso.org/ru/standard/83451.html (дата обращения: 01.06.2025).

Важно отметить, что в российских исследованиях [202] могут встречаться схожие понятия («публичные облака» и «частные облака»), но для обозначения принадлежности облачного сервиса государству (государственные инфраструктурные проекты) или частным компаниям. На наш взгляд, данные термины, для целей унификации и русификации понятий, возможно было бы определить через понятие «сервисы облачной обработки данных». Для цели единообразия в настоящей работе мы будем использовать понятие «публичное облако» в значении, приведенном в ГОСТ 27018–2020. Предложенная формулировка термина «сервисы облачной обработки данных» более точно позволяет понять суть технологии и не меняет смысл широкого многообразия применения технологии, ведь, как показано в работе выше, технология может размещаться не только публично (в понимании PasS), но и локально, ограничиваться и шифроваться (DaaS).

Важно также подчеркнуть различие оператора персональных данных с термином «провайдер хостинга», поскольку в соответствии с п. 18 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон № 149-ФЗ) под провайдером хостинга понимается лицо, осуществляющее деятельность по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет». Пунктом 3 ст. 2 Федерального закона № 149-ФЗ установлено понятие информационной системы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Размещение информационной системы пользователя на вычислительных мощностях владельца сервиса не предполагается. Таким образом, владельцы указанных сервисов не относятся к провайдерам хостинга[203].

---

[202] Отчет «Интернет в России в 2022–2023 годах: состояние, тенденции и перспективы развития». [Электронный ресурс]. Режим доступа: https://raec.ru/live/analytics/14235/ (дата обращения: 01.06.2025).

[203] Ответ Минцифры РФ по провайдерам хостинга от 10.10.2023 № П25–22415ОГ. [Электронный ресурс]. Режим доступа: https://t.me/privacyexpert/1393 (дата обращения: 01.06.2025).

Среди рисков использования публичных облаков выделяется безопасность ПДн, связывающая их с местом нахождения технических средств, осуществляющих техническую обработку данных, что подчеркивается в ряде научных исследований[204]. Уязвимость ПДн при размещении их в публичных облаках нередко приводит к утечкам ПДн ряда глобальных корпораций, медицинских организаций, а также ряда государственных органов, хранящих чувствительные и специальные категории данных[205].

Учёными выделяется проблема обработки ПДн на стороне поставщика публичного облака в вопросах безопасности данных внутри системы, особенно в отношении публичных облаков, находящихся за пределами Российской Федерации, так как не всегда можно полагаться на поставщика услуг, в том числе в связи с недостаточной проработанностью правового регулирования публичных облаков[206].

Риски обработки ПДн и их охраны можно было бы минимизировать посредством заключения договора, который позволил бы учитывать интересы обеих сторон путём распределения полномочий и ответственности таким образом, чтобы поставщик публичного облака нёс большую ответственность и выполнял большие меры по охране и защите ПДн как профессиональный участник соответствующей деятельности.

Однако поставщики публичных облаков, как показывает практика, не идут на это при заключении стандартных типовых соглашений, так как такие обязательства налагали бы серьезные правовые требования в части соблюдения

---

[204] См.: Eustice J.C. Flying into the cloud without falling: understanding the intersection between data privacy law and cloud computing solutions. [Электронный ресурс]. Режим доступа: https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-andcloud-computing (дата обращения: 01.06.2025); Викторова Н.Г., Шухов Ф.Г. Цифровая экономика: развитие облачных технологий в России и за рубежом. // Век качества. – 2019. – № 2. – С. 81–90.

[205] См.: Фаизова А.Г. Правовые риски защиты персональных данных лиц, использующих облачные сервисы, и пути их минимизации // Молодой учёный. – 2023. – № 27 (474). – С. 116; «Утечки информации из облака возросли в два раза». [Электронный ресурс]. Режим доступа: https://securenews.ru/utechci-informatsii-vozrosli/ (дата обращения: 01.06.2025);

[206] Бережной А. Облачные вычисления: новое или хорошо забытое старое? // Системный администратор, спецвыпуск «Облачные вычисления». – 2011. – Март. – С. 5.

требований по обработке ПДн. Большая часть публичных облаков работают по модели договора присоединения, без права внесения правок в такие договоры. Кристофер Миллар [207] и Д.М. Сатикова [208] отмечают, что на практике такие соглашения изменяются в одностороннем порядке и предоставляют провайдеру более широкие права, например на информацию о пользователе.

Автор отмечает в настоящем исследовании проблему, связанную с риском невыполнения требований об удалении ПДн, хранящихся на публичных облаках. Хранение и обработка данных компанией-исполнителем (обработчиком) на облачных серверах технически может быть неопределённое время, даже после удаления данных пользователем облачного сервиса, что нарушает требования ч. 7 ст. 21 Федерального закона № 152-ФЗ, а также положения Приказа Роскомнадзора № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных» (далее – Приказ Роскомнадзора № 179)[209].

Учёными выделяются правовые особенности трансграничной передачи данных и проблемы определения термина «адекватная защита». При передаче информации обработчику за границу Российской Федерации такая передача квалифицируется как трансграничная передача данных и регулируется в соответствии со ст. 12 Федерального закона № 152-ФЗ в особом порядке. Правовые

---

[207] Cloud computing Law, edited by Christopher Millard // Oxford University Press, 2013.

[208] Сатикова Д.М. Обработка персональных данных с использованием облачных сервисов // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. – 2018. – № 4. – С. 172.

[209] Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных». [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1717183243&tld=ru&lang=ru&name=Prikaz_Roskomnadzora_ot_28_10_2022_N_179_Ob_utverzhdenii_Tre.docx&text=Приказ+Федеральной+службы+по+надзору+в+сфере+связи%2C+информационных+технологий+и+массовых+коммуникаций+от+28+октября+2022+г.+№+179+«Об+утверждении+Требований+к+подтверждению+уничтожения+персональных+данных»&url=https%3A//77.rkn.gov.ru/docs/77/Prikaz_Roskomnadzora_ot_28_10_2022_N_179_Ob_utverzhdenii_Tre.docx&lr=43&mime=docx&l10n=ru&sign=01e59729c0ef3b77ca3d07f95dea0583&keyno=0, свободный (дата обращения: 01.06.2025).

вопросы трансграничной передачи персональных данных отдельно рассматривались А.И. Савельевым[210].

Нормами Федерального закона № 152-ФЗ не запрещается передача ПДн за пределы России и не запрещается передача обработки ПДн на аутсорсинг за границу[211]. Для передачи обработки ПДн стороннему сервису (обработчику) должно быть выполнено условие о согласии субъекта ПДн, которому принадлежат ПДн, что регулируется ч. 7 ст. 21 Федерального закона № 152-ФЗ, а также Приказом Роскомнадзора № 179.

В соответствии со ст. 12 Федерального закона № 152-ФЗ допускается трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных[212], а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных[213].

Легальной дефиниции термина «адекватная защита» в российском законодательстве нет, в связи с чем в настоящее время Правительством выработан подход, согласно которому страны, осуществляющие адекватную защиту, – это

---

[210] Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». – 2-е изд., перераб. и доп. – М.: Статут, 2021. – С. 264.

[211] Зоркольцев Р.Д. Персональные данные, получаемые через Интернет: практические вопросы. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1717183117&tld=ru&lang=ru&name=Zorkolcev.pdf&text=Зоркольцев+Р.Д.+Персональные+данные%2C+получаемые+через+Интернет%3A+практические+вопросы&url=http%3A//planeta51.ru/content/files/Zashita/Zorkolcev.pdf&lr=43&mime=pdf&l10n=ru&sign=b9bc79c3a832a11d3d51b3456ffca52f&keyno=0, свободный (дата обращения: 01.06.2025).

[212] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // Собрание законодательства РФ. – 2014. – № 5. – Ст. 419.

[213] Письмо Минкомсвязи РФ от 13.05.2009 № ДС–П11–2502. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1717183348&tld=ru&lang=ru&name=rkn-p.pdf&text=Письмо+Минкомсвязи+РФ+от+13.05.2009+N+ДС-П11-2502&url=https%3A//www.herzen.spb.ru/upload/files/ib/rkn-p.pdf&lr=43&mime=pdf&l10n=ru&sign=7fb70fafdb23c1830715316ae03894f0&keyno=0, свободный (дата обращения: 01.06.2025).

дружественные и нейтральные страны[214], а также страны, которые прямо не являются недружественными[215]. Актуальность продемонстрированной проблемы подчеркивается тем, что в ходе настоящего исследования Роскомнадзор утвердил перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных[216], тем самым установив корректный перечень стран, на которых не распространяются повышенные меры защиты ПДн. Но проблема отсутствия чёткого определения термина «адекватная защита» остаётся актуальной.

Условия о конфиденциальности, безопасности и контроле над данными – одни из ключевых проблем, которые сегодня возникают в ИТ-контрактах. Для необходимой правовой охраны ПДн, обрабатываемых с использованием облачных технологий, учитывая особое развитие сервисов публичных облаков в Российской Федерации, рост решений на рынке и переход к публичным облакам во всех сферах, в том числе государственных и частных, представляется необходимым поддержать мнение учёных о необходимости закрепить специальное правовое регулирование публичных облаков, которое подробно и системно регулировало бы отношения в области деятельности публичных облаков. Кроме прочего, следует уточнить терминологическую базу и закрепить правовые понятия в части определений «публичное облако» и «адекватная защита». Необходимо разграничить и закрепить нормативно виды публичных облаков и их особенности.

---

[214] Распоряжение Правительства РФ от 20.09.2023 № 2530-р (ред. от 18.03.2024) «Об утверждении перечня иностранных государств, в которых зарегистрированы иностранные банки (иностранные кредитные организации), действующие от своего имени и за свой счет, и иностранные юридические лица, осуществляющие деятельность, аналогичную деятельности брокера, которые могут быть допущены к участию в организованных торгах иностранной валютой» // Собрание законодательства РФ. – 2023. – № 39. – Ст. 7089.

[215] Распоряжение Правительства РФ от 05.03.2022 № 430-р (ред. от 29.10.2022) «Об утверждении перечня иностранных государств и территорий, совершающих недружественные действия в отношении Российской Федерации, российских юридических и физических лиц» // Собрание законодательства РФ. – 2022. – № 11. – Ст. 1748.

[216] Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.08.2022 № 128 «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных» // Собрание законодательства РФ. – 2022. – № 16. – Ст. 967.

Подводя черту по поводу специфики публично-правового регулирования в области персональных данных, обрабатываемых с использованием облачных технологий, следует остановиться на некоторых итогах научного изыскания:

1. Доказана необходимость специального правового регулирования функционирования публичных облаков, которое подробно и системно позволило бы установить правовую основу деятельности владельцев публичных облаков, а также разграничить и закрепить нормативно виды публичных облаков и специфику их правового регулирования.

2. Раскрыто значение видов публичных облаков, которое автор считает необходимым закрепить нормативно в виде ГОСТ 27018–2020:

– программное обеспечение как услуга (Software-as-a-Service / SaaS);

– платформа как услуга (Platform-as-a-Service / PaaS);

– инфраструктура как услуга (Infrastructure-as-a-Service / IaaS) или

– рабочее место как услуга (Desktop as a Service / DaaS).

Подчеркнута проблема отсутствия чёткости терминологической базы в научных исследованиях и практике в отношении облачных технологий при наличии специального термина «публичное облако», принятого в значении: предоставление услуг SaaS, PaaS, IaaS и/или DaaS для относительно неограниченного круга клиентов.

Автором предложено изменить наименование термина «публичное облако» на более точную формулировку: «сервисы облачной обработки данных». Предложенная формулировка термина более точно позволяет понять суть технологии и не меняет смысл широкого многообразия применения технологии.

3. Обосновано, что действующее нормативно-техническое регулирование применения публичных облаков не позволяет должным образом определить термин «публичное облако». В связи с этим предложено правовое определение понятия «публичное облако», в качестве которого следует понимать «услугу, позволяющую пользователю обеспечить обработку, хранение, управление и резервное копирование данных с помощью предоставления доступа к сервисам сервера, программному обеспечению и техническим средствам». Выявлено, что

основными формами применения публичных облаков в публичных целях являются: программное обеспечение как услуга; платформа как услуга; инфраструктура как услуга; рабочее место как услуга.

4. Среди наиболее высоких рисков использования публичных облаков выделяется безопасность ПДн, поскольку это связано с местом нахождения технических средств, осуществляющих техническую обработку этих данных.

5. Показано, что большая часть публичных облаков работают по модели рамочного договора, или договора присоединения, без возможности внесения правок в текст таких соглашений. Риски обработки ПДн и их охраны можно было бы минимизировать путём включения нормативных требований о заключении договора, посредством которого поставщик публичного облака будет обязан нести большую ответственность и выполнять расширенные требования по охране и защите ПДн.

6. Выявлена проблема, связанная с риском невыполнения требований об удалении ПДн, хранящихся на публичных облаках. Хранение и обработка, уничтожение данных компанией-исполнителем (обработчиком) на облачных серверах технически может быть неопределённое время, даже после их удаления пользователем облачного сервиса. Решение такой проблемы исключительно правовыми средствами представляется малоэффективным, ввиду чего предложено установление административной ответственности за невыполнение требования субъекта персональных данных об их удалении.

ГЛАВА 3. ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМЫ ПУБЛИЧНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ

§ 1. Этико-правовые проблемы в сфере публично-правового регулирования обработки персональных данных с использованием цифровых технологий

Интенсивное развитие науки и техники, способствующее ускоренному переходу человечества из общества постиндустриального в общество цифровое, открывает неведомые ранее горизонты познания и возможности реализации ещё недавно казавшихся фантастическими технологических проектов. Сопутствующими элементами развития современного общества, посредством стремительного развития технологий, является машинная обработка персональных данных, искусственный интеллект, присвоение социального рейтинга граждан, криптовалюта, блокчейн и много других технологических и этико-уязвимых технических нововведений[217]. Именно вследствие информатизации и активного развития науки и технологий обществу требуется надёжное публично-правовое обеспечение новой информационно-технологической реальности, с тем чтобы человеческая культура не потерялась, не растворилась в цифровом, электронном, информационно-технологическом пространстве; человек должен всегда преобладать над высокими технологиями[218].

Тема исследования публично-правового регулирования в сфере использования цифровых технологий при обработке персональных данных в контексте цивилизационного развития общества актуализирует разрешение фундаментального философского вопроса о дихотомии «свобода и безопасность»

---

[217] Информационно-технологическое обеспечение юридической деятельности (LegalTech): учебник / А.В. Минбалеев, Т.А. Полякова, М.Б. Добробаба и др. – М.: Проспект, 2022. – С. 274.

[218] Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций: коллективная монография: в 2 т. / Е.Н. Абанина, О.Ю. Авдевнина, Р.В. Амелин и др. – Саратов: Саратов. гос. юрид. академия, 2020. – С. 162.

в том ключе, что принятие норм и предписаний, трансформирующих базовые, или по крайней мере привычные, этические нормы в привычных нам границах либо вовсе избавляющих от тех или иных этически важных норм, приведёт человечество к разложению моральных и нравственных границ, потере человечности, деградации общества и исчезновению нравственности. По мере научно-технического прогресса чрезвычайно важно уделять внимание проблемам воздействия новейших научных разработок на общество, в частности по вопросам этических проблем юридической науки и правоприменительной практики[219].

Для начала нам следует определить место и роль юридической этики в праве вообще, а потом перейти к соответствующей специфике в области персональных данных.

С развитием технологий развивается право, регулирующее технологии. Возникают сложные, ранее не встречающиеся этические проблемы в правоприменительной практике, требующие разрешения и в юридической науке, которые приводят к выработке определённого отношения и подхода на основании философских исследований в области этических проблем в праве. Место юридической этики в современной науке и высокая значимость данного понятия в праве в условиях развития цифрового общества обусловливают необходимость всестороннего её изучения.

По мнению академика В.С. Степина, идеи, поддерживающие правовую регуляцию, сегодня размываются. В этом состоит одно из проявлений кризиса культуры техногенной цивилизации. Актуальной проблемой является поиск новых решений и моделей социальной регуляции, предполагающих повышение роли внеправовых регуляторов, конструирование оригинальных механизмов их взаимодействия с правом[220].

---

[219] Право и иные регуляторы в развитии цифровых технологий: монография / А.В. Минбалеев, А.В. Мартынов, Г.Г. Камалова [и др.]; Ин-т гос-ва и права Российской академии наук. – М.; Саратов: Амирит, 2022. – С. 6.

[220] Хабриева Т.Я., Капустин А.Я., Габов А.В., Черногор Н.Н. Конфликт интересов: природа, предупреждение, социальное регулирование // Журнал зарубежного законодательства и сравнительного правоведения. – 2018. – № 3 (70). – С. 9.

Этические проблемы юридической науки находят своё отражение прежде всего в правоприменительной практике. Именно в судебной практике возможно видеть актуальные проблемы морали и нравственности и их соотношения с действующими нормами в праве.

В данной части работы обратимся к отечественному нормативному регулированию и судебной практике по спорам в отношении этических вопросов, в том числе по новым научно-техническим достижениям, проанализируем и покажем проблемы этики – нравственности и морали в предметах споров. Развитие науки и техники, особенно стремительное, ставит новые и серьёзные задачи перед правовой системой судов и законодательной системой в целом в вопросе выработки определённого отношения к новым задачам, связанным с этической составляющей, а также стратегии их решения.

Нравственность выступает во многих качествах. При этом ориентиры нравственности закреплены прежде всего путём нормативного закрепления принципов, целей и задач в тех или иных нормативных правовых актах. Отражение закрепления принципов нравственности можно найти в каждом Федеральном законе Российской Федерации. Позиция автора настоящего исследования о том, что нормы морали закреплены прежде всего в его нормах-принципах, схожа с позицией Е.А. Артамоновой[221].

На примере уголовного и уголовно-процессуального права Т.К. Рябинина показывает место норм этики и инкорпорацию в праве, в частности, по мнению автора, мораль в уголовном судопроизводстве следует рассматривать как элемент механизма уголовно-процессуального регулирования, а механизм в целом – как морально-правовую систему. Автор отмечает, что «большинство норм права, определяющих задачи, сущность, исходные положения уголовного процесса и

[221] Артамонова Е.А. О производстве следственных действий в свете требований статьи 9 УПК РФ // Нравственные начала в уголовном процессе: сб. статей по материалам Всероссийского круглого стола / под общ. ред. К.Б. Калиновского, Л.А. Зашляпина. – СПб., 2021. – С. 24.

отношения его участников, отражают нравственные начала, соответствуют принципам морали»[222].

Таким образом, данная позиция также подтверждает предыдущий довод, что уже в сами нормы заложены определённые моральные ценности, что нормы и так служат своей целью определять этический, моральный, нравственный путь при отношении к тому или иному деянию. Но на практике все этические проблемы не могут регулироваться лишь нормами права, они не дают ответ на все острые вопросы нравственности и морали в общественных отношениях, особенно касательно стремительно развивающихся научных и технических достижений, которые порождают новые споры и преступления.

Переходя к научному анализу этико-правовых проблем в сфере защиты персональных данных, разберём некоторые случаи из практики и обозначим некоторые возникающие спорные ситуации в ключе соблюдения или нарушения нравственных норм, выраженных в виде споров о морали и нравственности.

Как писалось ранее, особо острые споры, которые можно отнести к спорам по этическим вопросам, можно рассмотреть на примере отношений, ещё не сформировавшихся, ибо постоянно развиваются и являются новеллами в техническом и, следовательно, в правовом плане тоже.

Одним из таких явлений, которое неразрывно связано с личностью человека, а следовательно, порождает множество правовых вопросов, связанных с этикой использования, распространения, хранения, передачи и других действий, является вопрос публично-правового регулирования оборота персональных данных субъекта.

Именно от нормативного регулирования, от объёма и подходов регулирования персональных данных зависит то, насколько будет позволено третьим лицам иметь доступ и в каком объёме смогут распоряжаться третьи лица личными и неотъемлемыми от человека персональными данными, которые по своей природе являются неимоверно уязвимой составляющей нашей повседневной

---

[222] Рябинина Т.К. Нравственные начала уголовного процесса: учеб. пособие. – Курск, 2017. – С. 36.

жизни. Противоправные действия или же действия, превышающие необходимость сбора персональных данных, могут серьезно нарушать права человека, его близких, затрагивать иные интересы.

Проблема использования персональных данных разных категорий очень остро стоит с этической точки зрения, начиная от данных о покупках, интересах пользователя, предпочтениях, паспортных данных, данных о членах семьи, о гражданском статусе, а также более существенных и ценных, особенно для преступников, медицинских данных, данных лица человека (биометрических данных), данных о его отпечатках пальцев и т.д. Проблемы правового регулирования отношений по поводу генетической информации институтов персональных данных, личной тайны, врачебной тайны глубоко анализировались учёными И.М. Рассоловым, С.Г. Чубуковой, И.В. Микуровой[223].

Именно этический аспект нормативного регулирования отношений с персональными данными стоит наиболее остро, наравне с правовыми вопросами об эвтаназии, абортами, биоэтике и прочими вопросами. В данном случае нормы права подстраиваются и принимаются исключительно для целей соблюдения конституционного права человека на личную жизнь[224], но конкурируют и с другими конституционными правами. Роль же суда – определить наиболее весомые права и увидеть обстоятельства, при которых на основе собственного мнения и отношения, на основе этических соображений принять то или иное решение, занять сторону того или иного лица в споре.

Проблема этики по вопросам обработки персональных данных отражается прежде всего в бытовых спорах, например при установке камер видеонаблюдения в подъезде, ведь обработка камерой информации о перемещении и действиях

---

[223] Рассолов И.М., Чубукова С.Г., Микурова И.В. Анализ возможного применения к регулированию отношений по поводу генетической информации институтов персональных данных, личной тайны, врачебной тайны // Lex Russica. – 2020. – № 4 (161). [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/analiz-vozmozhnogo-primeneniya-k-regulirovaniyu-otnosheniy-po-povodu-geneticheskoy-informatsii-institutov-personalnyh-dannyh-lichnoy (дата обращения: 07.11.2025).

[224] См.: ст. 23 Конституции Российской Федерации (Принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). Доступ из СПС «КонсультантПлюс».

жильцов подъезда является нарушением конституционных прав жильцов на тайну личной жизни. С другой стороны, установка камеры – это право собственника имущества обеспечить свою безопасность и реализация конституционного права на безопасную среду. Подобные судебные споры не редкость, и вызваны они развитием технологий, повсеместной доступностью приобретения соответствующих технологических средств, уязвимостью технологий перед кибершпионажем и прочими современными проблемами, прямо или косвенно связанными с этической стороной данного вопроса.

Так, Первым кассационным судом общей юрисдикции было рассмотрено дело от 16.02.2022 № 88-5317/2022[225]. Ответчик являлся соседом по земельному участку с истцом. Ответчик сам, без согласия истца установил камеры видеонаблюдения на крыше своего дома и на углу своего дома, которые были направлены на участок истца и частично контролировали его двор. Истец настаивал, что установка ответчиком камеры видеонаблюдения нарушает его законные права на неприкосновенность частной жизни. Истец заявил судебное требование к ответчику снять камеры видеонаблюдения с дома, направленные на собственность истца.

Суд первой инстанции удовлетворил требования ответчика и в обоснование своего решения отметил, что без правового обоснования и законной цели видеоконтроль за чужой территорией, а именно частной территорией, где находится жилое помещение истца, незаконен, является вмешательством в жизнь и нарушает права на уважение частной жизни истца.

Суд апелляционной инстанции не согласился с такими выводами и посчитал, что ответчик реализует своё право на защиту имущества, а именно дома и земельного участка. В процессе реализации своих прав ответчик имеет право

---

[225] Определение Первого кассационного суда общей юрисдикции от 16.02.2022 г. по делу № 2– 1106/2021. [Электронный ресурс]. Режим доступа: https://1kas.sudrf.ru/modules.php?name=sud_delo&name_op=case&case_id=32222732&case_uid=19c91455-73b0-4b0b-81e8-377383e9907d&delo_id=2800001&case_type=0&new=2800001&srv_num=1, свободный (дата обращения: 01.06.2025).

установить на принадлежащей ему территории и имуществе камеры видеонаблюдения.

Вывод из решения суда: истец должен доказать нарушение своих прав на неприкосновенность частной жизни, а также доказать, что ответчик использует данные с камер незаконно, распространяет информацию, составляющую личную, семейную тайну, вмешивается в жизнь истца. Предоставление фотографий с камер видеонаблюдения не доказывает, само по себе, противоправность видеосъёмки. Законом не запрещена установка камер для целей защиты своего имущества. И сама по себе установка камер на территории ответчика, хоть они и направлены на территорию и имущество истца, не посягает на личную жизнь истца. Если имущество установлено на личной территории, то это само по себе не посягает на личную жизнь другой стороны.

Анализируя вышепредставленную информацию, Первым кассационным судом общей юрисдикции не было установлено недобросовестности при осуществлении принадлежащих прав собственника имущества, поскольку установка на крыше и стене принадлежащего ответчику жилого дома видеокамер произведена в целях его личной безопасности и сохранности принадлежащего ему имущества, что не является нарушением прав на неприкосновенность частной жизни, личную и семейную тайну. Руководствуясь ст. 23, 24 Конституции Российской Федерации, ст. 152.1, 152.2, 209 Гражданского кодекса Российской Федерации (далее – ГК РФ)[226], положениями Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) «О персональных данных»[227] (далее – Закон о персональных данных), суд апелляционной инстанции пришел к правильному, по мнению автора, выводу о необходимости отказа в иске (о демонтаже камеры)[228].

---

[226] Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Собрание законодательства РФ. – 1994. – № 32. – Ст. 3301.

[227] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.

[228] Определение Первого кассационного суда общей юрисдикции от 16.02.2022 г. по делу № 2– 1106/2021. [Электронный ресурс]. Режим доступа: https://1kas.sudrf.ru/modules.php?name=sud_delo&name_op=case&case_id=32222732&case_uid=19c91455-73b0-4b0b-81e8-

То есть в данном случае суд встал на защиту интересов безопасности ответчика, мотивируя это правом собственности на объект, на который было установлено правомерно средство наблюдения. Этический факт того, что камера направлена на чужой участок, что с помощью этой камеры ответчик может собирать круглосуточно данные и даже использовать их в противоправных или аморальных целях, судом не учтён, а точнее этот аспект суд посчитал не столь важным (необоснованным). Суд встал на сторону ответчика, ставя в приоритет нормы права о собственности выше, чем нормы о сборе информации (персональные данные) человека, на участок которого направлена камера тоже, в том числе в части защиты этических аспектов личных правоотношений.

Но есть иные взгляды судов при разрешении подобных ситуаций, и, возможно даже наоборот, чрезмерно жёсткие. Так, из материалов дела № 2- 598/2021, рассматриваемого в Первом кассационном суде общей юрисдикции от 16.12.2021[229], следует, что был поднят вопрос об обязывании демонтировать видеокамеру.

Истец являлся собственником половины дома и прилежащего земельного участка, на котором располагался весь дом. Во второй половине дома проживал ответчик, установивший две камеры видеонаблюдения, что стало предметом судебного спора. Камеры записывали изображение земельного участка истца, но были установлены на половине ответчика.

Суд первой инстанции отказал истцу в требованиях. Апелляция же отменила решение первой инстанции и обязала ответчика демонтировать камеры.

Дело дошло до кассационного рассмотрения. Ответчик ссылался на то, что камеры установлены для сохранности личного имущества и личной безопасности. Ответчик указал, что получал согласие истца на обработку данных по поводу записи и передачи изображения снимаемого видеокамерами контента.

377383e9907d&delo_id=2800001&case_type=0&new=2800001&srv_num=1, свободный (дата обращения: 01.06.2025).

[229] Определение Первого кассационного суда общей юрисдикции от 16.12.2021 № 88–28204/2021 по делу № 2–598/2021. [Электронный ресурс]. Режим доступа: https://1kas.sudrf.ru/modules.php?name=docum_sud&id=37, свободный (дата обращения: 01.06.2025).

Кассационный суд встал на сторону истца и не внял доводам ответчика. В итоговом судебном акте указано, что «сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), относятся к сведениям конфиденциального характера, доступ к которым ограничен»[230].

Суд указал, что «камеры направлены по большей части на собственность истца, а не ответчика, а именно домовладение и земельный участок. Камеры снимают истца и членов его семьи. Камеры идентифицируют лицо на достаточном расстоянии. Все вышеперечисленные доводы суд привёл для цели указать, что законные интересы ответчика на защиту своего имущества в этом случае менее важны и не могут нарушать законные права истца на частную жизнь»[231].

Иными словами, когда одно лицо осуществляет контроль за определённой территорией другого лица путём видеонаблюдения, установленного на территории данного лица и не требующего согласия от истца (и реализует тем самым своё право на безопасность, что следует из материалов дела, поскольку основанием к установке камеры послужили спорные действия ответчика по отношению к собственности истца), суд посчитал, что этические нормы, выраженные в виде недопущения излишнего и несогласованного контроля за личностью истца на его же участке, являются ничуть не меньшим обоснованием к отказу ответчику в его праве, утверждая, что желание «защищать своё имущество не может оправдывать нарушение законных прав истца».

Тем самым в судебной практике мы встречаем множество примеров того, как суд использует нормы права с опорой на этические нормы, на отношение морали и нравственности на складывающиеся общественные отношения. Именно сквозь призму этики суд избирает главенство тех или иных норм, аргументируя в одних и тех же практически случаях свою позицию по-разному.

---

[230] Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» // Собрание законодательства РФ. – 1997. – № 10. – Ст. 1127.

[231] Определение Первого кассационного суда общей юрисдикции от 16.12.2021 № 88–28204/2021 по делу № 2–598/2021. [Электронный ресурс]. Режим доступа: https://1kas.sudrf.ru/modules.php?name=docum_sud&id=37, свободный (дата обращения: 01.06.2025).

Автором предлагается набор правил, определяющих законность установки видеокамер, используя которые, возможно найти этико-правовой баланс при публично-правовом регулировании обработки ПДн между такими конституционными правами, как уважение частной жизни и защита имущества: камеры должны быть установлены для целей защиты своего имущества; не произошло нарушение прав на неприкосновенность частной жизни – данные с камер не используются незаконно (распространяется информация, составляющая личную, семейную тайну, происходит вмешательство в жизнь), при этом предоставление фотографий с камер видеонаблюдения не доказывает, само по себе, противоправность видеосъёмки; камеры установлены на личной территории; камеры не направлены на территорию и имущество истца как на главный объект съёмки (менее ±30 % объёма съёмки) и не посягают на личную, интимную жизнь иного лица.

Такого рода требования к установке средств фотовидеофиксации следует обратить не только по отношению к частным лицам, но и к различным организациям, в том числе государственным органам.

Соответствующие правила целесообразнее было бы закрепить не на уровне законодательства, а в рамках приказа Роскомнадзора как уполномоченного органа в контексте обобщения практики осуществления государственного контроля (надзора) в области персональных данных.

Именно факт выбора трактования правовых норм в одинаковых или схожих отношениях и условиях свидетельствует о высокой степени необходимости правового регулирования данных этических вопросов с позиции баланса частных интересов различных субъектов, а также баланса частных и публичных интересов.

Таким образом, результатом проделанного научного исследования могут послужить следующие выводы:

1. Анализ судебной практики показал, что встречается множество примеров того, как суд использует нормы права с опорой на этические нормы, на отношение морали и нравственности касательно складывающихся «под давлением развития науки и техники» общественных отношений. Именно сквозь призму этики суд в

делах связанных с обработкой персональных данных избирает главенство тех или иных норм, аргументируя в одних и тех же практически случаях свою позицию по-разному.

2. Показана актуальная проблема обработки персональных данных, связанная с этическими вопросами при использовании цифровых технологий. Продемонстрирована необходимость учёта этического аспекта при разрешении некоторых вопросов в области персональных данных, исходя из ситуационного правового регулирования в конкретном случае, в связи с чем необходимо выработать принципы и методы определения баланса между охраной частной собственности и права на тайну частной жизни.

3. Именно факт важности субъективной оценки судьёй обстоятельств в каждом конкретном случае, последующего выбора трактования правовых норм в одинаковых или схожих отношениях и условиях свидетельствует о высокой степени необходимости учёта этического аспекта при разрешении некоторых вопросов в области персональных данных, исходя из ситуационного правового регулирования в конкретном случае.

4. Автором предлагается система правил, определяющая законность установки средств фотовидеофиксации, используя которую, возможно найти этико-правовой баланс при публично-правовом регулировании обработки ПДн между такими конституционными правами, как уважение частной жизни и защита имущества.

Предложены правовые признаки, определяющие законность установки и универсального использования средств фотовидеофиксации гражданами в части недопустимости нарушения требований обработки персональных данных.

Для признания правомерности установки средств фотовидеофиксации (камер и других средств) необходимо соблюдение совокупности условий:

– средство фотовидеофиксации установлено для целей охраны имущества, жизни и здоровья;

– средство фотовидеофиксации установлено на личной территории;

– средство фотовидеофиксации не направлено на территорию и имущество другого лица как на главный объект съёмки*;*

– данные, полученные со средств фотовидеофиксации, не нарушают неприкосновенность частной жизни, личную и семейную тайну.

Соответствующие правовые признаки целесообразно закрепить в рамках приказа Роскомнадзора как уполномоченного органа в контексте обобщения практики осуществления государственного контроля (надзора) в области персональных данных.

§ 2. Проблемы публично-правового регулирования обработки персональных данных, составляющих врачебную тайну, при использовании цифровых технологий

Персональные данные, составляющие сведения о здоровье граждан, представляют собой медицинские данные. В соответствии с Федеральным законом «О персональных данных» [232] сведения о состоянии здоровья отнесены к персональным данным.

Сфера данных о здоровье гражданина охватывает широкий спектр информации. Сюда входит личная информация о гражданине (именуемая персональными данными), относящаяся к состоянию здоровья человека, а также медицинская информация (например, рецепт врача, направления, протоколы медицинских осмотров, лабораторные анализы и т.д.), административная и финансовая информация о здоровье (в частности, расписание приёмов к врачу, счета за медицинские услуги, медицинские справки для оформления больничных листов и т.д.).

Стоит обратить внимание, что напрямую информация о здоровье граждан является медицинской информацией (медицинскими данными, содержащимися в медицинских документах), в то время как административная и финансовая информация лишь косвенно затрагивает медицинские данные гражданина, выполняя «обслуживающие» функции. Данное разделение имеет практическое значение в части реализации охраны персональных данных граждан в сфере медицины, так как от того, какая именно информация закреплена и какими именно документами она подтверждается, зависит круг лиц, которым сведения, составляющие информацию о здоровье граждан, могут быть переданы. Например, отделу кадров работника, находящегося на больничном, медицинской организацией будет разглашена информация, составляющая персональные данные в сфере медицины, лишь косвенно затрагивающая вопросы здоровья работника, а

[232] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.

именно в виде листка нетрудоспособности, что по выделенной нами классификации относится к административной и финансовой информации.

Ввиду того, что медицинские данные считаются конфиденциальными данными, на них распространяется особый режим, и обрабатывать их могут только медицинские работники, связанные обязательством сохранения врачебной тайны. Кроме того, организация должна принять необходимые меры безопасности, чтобы медицинские данные были защищены и не подлежали несанкционированному разглашению.

В рамках темы медицинских данных граждан существует несколько неоднозначных вопросов: как коррелируют между собой правовые режимы персональных данных и врачебной тайны; кто несёт ответственность за сохранность персональных данных пациентов; можно ли разглашать сведения о персональных данных пациентов, составляющих медицинские данные, работодателю или отделу кадров; в случае смерти гражданина можно ли получить доступ к информации о состоянии здоровья умершего, содержащейся в медицинских документах, могут ли данные сведения быть разглашены третьи лицам.

Фактически к персональным данным можно отнести любую информацию, которая характеризует и прямо или косвенно позволяет определить физическое лицо. В случае если данные не позволяют идентифицировать физическое лицо, к персональным такие данные не относятся.

Интересным в контексте определения персональных данных через возможность идентификации лица представляется европейский подход, согласно которому обезличенные данные являются обратимыми. Данный подход основывается на том, что в случае, если обезличенные данные могут быть возвращены к такому состоянию, при котором они позволяют косвенно определить

лицо, информацию о котором эти данные содержат, то такие данные являются персональными[233].

В свою очередь, в понятие врачебной тайны законодатель включает любые сведения о факте обращения гражданина за медицинской помощью, о состоянии здоровья, диагнозе, а также иные сведения, полученные в ходе обследования и (или) лечения гражданина.

Обратимся к специальному законодательству в сфере охраны здоровья граждан. Так, ст. 79 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации»[234] установлена обязанность медицинской организации по соблюдению врачебной тайны, в том числе по соблюдению конфиденциальности персональных данных, используемых в медицинских информационных системах.

В данной норме законодатель фактически определил, что правовой режим персональных данных является частью правового режима врачебной тайны. При этом мы видим чёткое указание на то, что обработка и распространение персональных данных, касающихся здоровья граждан, выполняются посредством медицинских информационных систем.

Прежде всего отметим, что сфера персональных данных гораздо шире врачебной тайны, так как включает, помимо врачебной тайны, иные специальные режимы правовой охраны информации. Врачебная тайна по своему характеру является отдельным видом персональных данных, правовая охрана которого регламентирована специальным законодательством об основах охраны граждан.

В порядке закономерного развития информационного общества сфера персональных данных граждан в части медицинских данных была также затронута цифровизацией, в результате чего в целях наиболее эффективной оптимизации процесса обработки и распространения персональных данных граждан,

---

[233] Opinion 4/2007 on the Concept of Personal Data. WP 136, 20 June 2007. Article 29 Data Protection Working Party. P. 16–18. [Электронный ресурс]. Режим доступа: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, свободный (дата обращения: 01.06.2025).

[234] Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 23.07.2025) «Об основах охраны здоровья граждан в Российской Федерации» // Собрание законодательства РФ. – 2011. – № 48. – Ст. 6724; – 2021. – № 27 (ч. 1). – Ст. 5186.

касающихся их состояния здоровья, были разработаны медицинские информационные системы медицинских организаций. Требования к данным системам чётко регламентированы Приказом Минздрава России от 24.12.2018 № 911н[235].

С одной стороны, одним из плюсов развития медицинских информационных систем является возможность ведения электронных медицинских карт пациента. Данная мера позволяет без излишней бюрократизации процессов, оперативно передать сведения о состоянии здоровья пациента из одного медицинского учреждения в другое[236]. Ещё более легальным данное преимущество стало после внесения изменений в Закон о персональных данных в 2021 году, в результате которых разграничили моменты предоставления согласия гражданина на обработку персональных данных и согласия на распространение персональных данных, вследствие чего подписание соглашения на обработку персональных данных перестало быть автоматическим согласием также и на распространение персональных данных.

С другой стороны, медицинские информационные системы должны быть дополнительно обеспечены с точки зрения информационной безопасности в части технического обеспечения сохранности персональных данных граждан, касающихся их состояния здоровья. В связи с цифровизацией процесса обработки, хранения и распространения данных о состоянии здоровья граждан обострилась проблема, связанная с разглашением данных о состоянии здоровья третьим лицам, к которым такие сведения могут попасть как «по ошибке», так и преступным путём.

Главным актором (фактически менеджером), выполняющим административные функции по сбору персональных данных о состоянии здоровья

---

[235] Приказ Минздрава России от 24.12.2018 № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций» // Официальный интернет-портал правовой информации. [Электронный ресурс]. Режим доступа: http://www.pravo.gov.ru, свободный (дата обращения: 01.06.2025).

[236] Тимофеев И.В. Цифровая информатизация и информационная безопасность в современном здравоохранении: конституционно-правовой подход к проблеме // Конституционное и муниципальное право. – 2019. – № 12. – С. 25.

граждан, являются медицинские организации. При этом как при подписании договора на оказание медицинских услуг, так и при подписании отдельных самостоятельных соглашений на обработку персональных данных мало кто обращает внимание на то, доступ к каким именно персональным данным предоставляют граждане и правом на передачу каких именно данных они наделяют медицинские организации.

Подобная невнимательность и халатность со стороны самих субъектов персональных данных может привести к тому, что сведения о диагнозе или же о состоянии здоровья граждан могут попасть к третьим лицам, целью деятельности которых является извлечение прибыли, к примеру в результате оказания ритуальных услуг. Так, лица с «тяжёлыми» заболеваниями, которым назначено паллиативное лечение, становятся объектом повышенного внимания для организаций, специализирующихся на оказании ритуальных услуг населению.

В целом представляется необходимым провести комплекс мероприятий, направленных на повышение уровня эффективности обеспечения безопасности и сохранности персональных данных, полученных медицинскими организациями и обрабатываемых медицинскими информационными системами. Кроме того, важно обеспечить высокий уровень «цифровой гигиены» сотрудников медицинских организаций путём проведения обучения, что повысит уровень ответственности среди сотрудников медицинских учреждений к вопросам цифровой обработки персональных данных и о возможных мерах уголовной и гражданско-правовой ответственности, применяемых в случаях незаконного разглашения сведений, относящихся к персональным данным граждан о состоянии здоровья, и данных, составляющих врачебную тайну.

В трудах Э.В. Талапиной встречается следующий тезис: «В эпоху цифрового капитализма изменилось само понятие человеческого»[237]. В контексте поднятой проблемы данный тезис можно развить путём указания на то, что в процессе развития информационного общества не только меняется понятие человеческого,

[237] Талапина Э.В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права РАН. – 2018. – № 5. – С. 118.

но и поддается активному давлению всё «человечное», так как незаконное разглашение сведений, относящихся к персональным данным, зачастую приводит к моральным и нравственным страданиям не только для самого субъекта персональных данных, но иногда и для его родных и близких. Именно поэтому так распространены иски с требованиями о взыскании компенсации морального вреда за раскрытие персональных данных, и именно поэтому актуальна проблема обеспечения надлежащей защиты персональных данных[238].

Данные о здоровье граждан должны обрабатываться только медицинскими организациями. Отдел кадров работодателя должен получать лишь административные данные, необходимые для оформления больничного листа (к таким данным, например, относятся данные о количестве дней больничного листа и код болезни). Подобная мера позволит избежать дискриминации на местах и случаев незаконного увольнения в связи с возможными проблемами со здоровьем у сотрудников. В Евросоюзе подобная проблема встречается крайне редко, что позволяет говорить о высоком уровне охраны персональных данных, касающихся состояния здоровья сотрудников.

Кроме того, в период распространения новой коронавирусной инфекции COVID-19, а также вспышек данной инфекции в начале 2022 года выявилась проблема, связанная со своевременным получением больничного листа в медицинских организациях с целью его дальнейшего предъявления по месту требования (чаще по месту работы) и закрытием больничного.

В целях сохранения баланса интересов (в частности, для соблюдения баланса между запретом на разглашение медицинских данных третьим лицам и позитивной тенденцией по минимизации излишнего документооборота, создающего трудности в своевременном закрытии больничного) предлагается обеспечить возможность подключения компаний к работе медицинских информационных систем в части обеспечения оперативного документооборота, то есть предоставить возможность

---

[238] Бачило И.Л., Сергиенко Л.А., Кристальный Б.В., Арешев А.Г. Персональные данные в структуре информационных ресурсов. Основы правового регулирования. – Минск: Беллітфонд, – 2006. – С. 351.

медицинским учреждениям по каналам прямой связи направлять больничный лист сразу в компанию работника, без необходимости его личного присутствия в медицинском учреждении по запросу сотрудника.

Должно быть обеспечено надлежащее информирование пациентов (субъектов ПДн) сотрудниками медицинских учреждений о том, для цели какого объёма обработки и какие именно данные предоставляются медицинскому учреждению при подписании такого согласия.

Необходимость реализации данной меры обусловлена тем, что зачастую гражданам-пациентам предоставляют на подпись соглашение на обработку персональных данных (без надлежащего информирования о конкретном его содержании, без возможности внесения каких-либо изменений в текст этого соглашения и без возможности отказа от определённых видов обработки) либо включают данное условие в договор на оказание медицинских услуг, не разъясняя, на что именно они соглашаются, кому и в каком объёме могут быть переданы данные о состоянии здоровья. Такое положение абсолютно противоречит принципу прозрачности (открытости) информации, а также способствует введению в заблуждение посредством умалчивания и иного бездействия, не отвечающего требованиям добросовестности.

В связи с неоднозначной позицией судов, отдельного внимания заслуживает вопрос о том, могут ли родственники в случае смерти гражданина получить доступ к информации о состоянии здоровья умершего, содержащейся в медицинских документах.

Во-первых, сам факт получения третьими лицами информации о состоянии здоровья умершего причиняет моральный вред родственникам умершего, что не может даже ставиться под сомнение и требует особого внимания при разрешении подобной категории дел. Во-вторых, при решении вопроса о разглашении медицинских данных умершего лица необходимо учитывать причины обращения за разглашением такой информации.

Значимым судебным актом, разрешающим затронутые вопросы, является Постановление Конституционного Суда Российской Федерации от 13.01.2020

№ 1-П[239]. В данном постановлении прямо подчеркнуто, что Закон об основах охраны граждан в Российской Федерации не содержит положений, регламентирующих правовой режим доступа к информации о состоянии здоровья и медицинской документации после смерти пациента. Соответственно, отсутствует: регламентация круга лиц, объём информации, формы и сроки предоставления информации, касающейся здоровья умершего лица.

В действительности при разрешении данного вопроса необходимо учитывать баланс интересов пациентов, родственников, супругов и других лиц в вопросах получения доступа к медицинской информации пациента в случае его смерти. Так, если сведения о причине смерти и диагнозе пациента доступны заинтересованному лицу в силу закона, сохранение в тайне от него информации, касающейся медицинского вмешательства, в том числе о диагностике, лечении и назначенных препаратах, не может во всех случаях оправдываться необходимостью защиты врачебной тайны, особенно с учётом мотивов и целей обращения за такими сведениями.

В судебной практике[240, 241, 242] часто встречаются «отказные дела» по искам о взыскании компенсации морального вреда с медицинских организаций, в результате действий или бездействия сотрудников которых наступила смерть пациента. Безусловно, следует учитывать, что зачастую родственников умерших пациентов захватывают эмоции, провоцирующие на обращение в суд с подобными

---

[239] Постановление Конституционного Суда Российской Федерации от 13.01.2020 № 1–П «По делу о проверке конституционности частей 2 и 3 статьи 13, пункта 5 части 5 статьи 19 и части 1 статьи 20 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» в связи с жалобой гражданки Р.Д. Свечниковой» // Собрание законодательства РФ. – 2020. – № 3. – Ст. 275.

[240] Апелляционное определение Верховного суда Республики Татарстан от 17.08.2017 по делу № 33–13279/2017. [Электронный ресурс]. Режим доступа: https://vs.tat.sudrf.ru/modules.php?name=information&irid=9, свободный (дата обращения: 01.06.2025).

[241] Апелляционное определение Ленинградского Областного суда от 20.04.2016 № 33-2182/2016. [Электронный ресурс]. Режим доступа: https://oblsud.lo.sudrf.ru/modules.php?name=information, свободный (дата обращения: 01.06.2025).

[242] Кассационное определение Третьего кассационного суда общей юрисдикции от 31.07.2024 по делу № 88–17092/2024. [Электронный ресурс]. Режим доступа: http://3kas.sudrf.ru/, свободный (дата обращения: 01.06.2025).

исками, однако количество таких исков всё же заставляет задуматься о надлежащем исполнении обязанностей со стороны сотрудников медицинских учреждений. Подобные иски являются чаще отказными ввиду отсутствия надлежащей доказательственной базы, что обусловлено отказом в предоставлении медицинских документов, содержащих сведения о ходе и методике лечения, что также лишает заявителей возможности провести свою экспертизу на предмет соответствия действий сотрудников медицинских учреждений обстоятельствам происходящего и состоянию здоровья пациента.

Как указал Конституционный Суд Российской Федерации, при рассмотрении данной категории дел судам следует руководствоваться принципами соразмерности и справедливости принятия решения о необходимости ознакомить заинтересованное лицо со сведениями, относящимися к истории болезни умершего пациента, в той мере, в какой это необходимо для эффективной защиты прав заявителя и прав умершего.

Конституционный Суд Российской Федерации также подчеркнул, что, несмотря на несколько десятков принятых поправок в Закон об основах охраны здоровья, ни одна из них не была направлена на совершенствование нормативного регулирования доступа заинтересованных лиц к медицинской документации умершего пациента. В результате сложилось неоднозначное, нечёткое и противоречивое правовое регулирование вопроса о предоставлении доступа к медицинской документации, регламентирующей состояние здоровья, методику лечения умершего пациента, что не соответствует Конституции Российской Федерации.

Представляется необходимым установить следующие ключевые моменты в вопросе публично-правового регулирования в сфере использования цифровых технологий при обработке персональных данных, составляющих врачебную тайну:

1. Следует внести изменения в действующий Закон об основах охраны здоровья, дополнив его положениями о допустимости предоставления медицинских данных умерших пациентов супругам, родственникам и иным заинтересованным лицам по их запросу. При этом необходимо учитывать цели

такого запроса, чтобы минимизировать риск обнародования или использования полученных сведений в корыстных целях.

2. Выявлена проблема надлежащего информирования пациентов (субъектов ПДн) сотрудниками медицинских учреждений. Требуется установление законодательных требований по надлежащему информированию сотрудниками медицинских организаций субъектов персональных данных (а в данном случае одновременно и пациентов) о том, согласие на обработку каких конкретно персональных данных, касающихся состояния здоровья, они предоставляют медицинскому учреждению при подписании такого согласия.

3. Выявлена проблема соотношения норм о персональных данных с нормами законодательства в сфере охраны и социального обеспечения. В частности, была поставлена проблема об относимости данных о наличии инвалидности к числу общедоступных персональных данных.

4. Наличие инвалидности – это социальный статус, и данные о ней не должны относиться к специальным категориям персональных данных. Данный подход позволит не допускать дополнительных оснований для дискриминации лиц с ограниченными возможностями. Для гражданско-правовых, трудовых и ряда иных правоотношений данные о наличии инвалидности (без указания о диагнозе и иных данных, составляющих медицинскую тайну) необходимы для учёта различных льгот и иных мер поддержки, а также специальных требований к рабочему месту и характеру трудовой функции.

§ 3. Проблемы и перспективы развития института административной ответственности в области нарушения требований законодательства о персональных данных

Административная ответственность, являясь классическим институтом публичного права, посредством охранительных норм осуществляет юридическое обеспечение реализации и защиты закреплённых в нормах права субъективных прав и законных интересов конкретных участников правоотношений в области персональных данных.

Помимо этого, по верному замечанию Н.И. Джафаровой: «меры административной ответственности имеют важное назначение, заключающееся в государственном реагировании в отношении правонарушителя на всех стадиях реализации своего противоправного замысла, начиная с незаконного получения информации, относящейся к персональным данным». Поддерживает установление особых мер ответственности за нарушение прав субъекта, несоблюдение мер защиты информации, за их использование в не предусмотренных согласием или законом целях, объёмах и сроках В.В. Игумнов[243].

Переходя к научному исследованию в сфере развития института административной ответственности в области нарушения требований законодательства о персональных данных, следует изначально определиться с примерным перечнем составов административных правонарушений в области персональных данных.

Наряду с этим для достижения поставленной научной задачи нужно не просто перечислить конкретные составы административных правонарушений в области персональных данных, но и провести их определённую научную стратификацию на несколько групп, а также необходимо детально исследовать элементы составов административных правонарушений в области персональных данных с целью выявить наиболее юридически значимые из них.

---

[243] Игумнов В.В. Публично-правовое регулирование цифрового профилирования в Российской Федерации: автореф. дис. … канд. юрид. наук. – М., 2024.

На основе такого детального исследования существующего состояния института административной ответственности в области персональных данных уже можно в обратном хронологическом порядке проследить историю развития этого института публичного права, а также сформулировать некоторые выводы и проследить определённые закономерности развития нормотворчества в данной области.

Если задаться целью выявить составы административных правонарушений в области персональных данных, то можно прийти к ошибочному выводу о том, что их перечень исчерпывается теми составами административных правонарушений, административная ответственность за которые предусмотрена профильной статьёй 13.11 «Нарушение законодательства Российской Федерации о персональных данных» Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ).

Данные составы административных правонарушений следует сгруппировать, поскольку они носят профильный характер для обеспечения реализации и защиты субъективных прав и законных интересов конкретных участников правоотношений в области персональных данных. Помимо этого, дополнительным обоснованием целесообразности такого варианта группировки будет общая история возникновения и дальнейшего развития всех нижеперечисленных составов административных правонарушений.

В соответствии с п. 1 ст. 1 Федерального закона от 7 февраля 2017 года № 13-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» в ст. 13.11 КоАП РФ были внесены существенные изменения, в результате которых первоначальный вариант данной нормы полностью видоизменился:

– вместо одного общего для всего законодательства о персональных данных состава административного правонарушения (формой которого было нарушение порядка сбора, хранения, использования или распространения персональных данных) появились сразу семь новых составов административных

правонарушений, формой некоторых из них были несколько вариантов действий (бездействий);

– существенным образом изменились санкции в рамках данной статьи (ранее максимальный размер административного штрафа составлял лишь десять тысяч рублей для юридических лиц, а минимальной формой административного наказания вообще являлось предупреждение, но после соответствующих изменений административные штрафы возросли в несколько раз).

В «профильную» группу административных правонарушений в области персональных данных следует отнести следующие составы административных правонарушений:

1. Незаконная обработка персональных данных, осуществляемая вне допустимых законодательством о персональных данных случаев, а равно и несовместимая с целями сбора обработка персональных данных (пп. 1 и 1.1 ст. 13.11 КоАП РФ). Административная ответственность в этом случае может достигать 300 000 рублей, а за повторное – 500 000 рублей.

Суммы штрафов в данном случае и в последующем будут приведены в редакции Федерального закона от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях».

Данный состав административного правонарушения носит формальный характер, то есть для констатации факта его совершения не нужно наступление тех или иных последствий, достаточно совершения виновных действий.

Бездействие не может быть формой административно наказуемого деяния по данному основанию, поскольку «обработка персональных данных» во всех случаях имеет форму действия в соответствии с закреплённой в ст. 6 Федерального закона № 152-ФЗ нормой дефиниции о понятии «обработка персональных данных».

2. Второй состав административного правонарушения – пп. 2 и 2.1 ст. 13.11 КоАП РФ – также двусоставный по форме деяния:

– обработка ПДн без письменного согласия на обработку, если такое согласие обязательно;

– обработка ПДн при наличии письменного согласия на обработку персональных данных, если в таком письменном согласии отсутствуют сведения, которые являются обязательными в силу п. 4 ст. 9 Федерального закона № 152-ФЗ.

Наказание в данном случае может достигать 700 000 рублей за совершение данного административного правонарушения впервые и до 1,5 миллиона рублей – за повторное.

Если обратить своё внимание на развитие соответствующих норм пп. 1, 1.1, 2 и 2.1 КоАП РФ, то наиболее важные изменения произошли в 2021 году в связи с принятием соответствующих поправок, в соответствии с которыми были значительно увеличены суммы административных штрафов (относительно изменений 2017 года), а также в качестве самостоятельного появился состав административного правонарушения, который выражается в повторном совершении данного административного правонарушения и, соответственно, за совершение которого повторно установлен более высокий размер административного штрафа.

3. Третьим по счёту можно назвать целую серию составов административных правонарушений, обобщённых по нескольким общим признакам: специальный субъект административного правонарушения – оператор обработки персональных данных; административно наказуемое деяние – невыполнение специальных требований законодательства о персональных данных.

К числу данной подгруппы относятся административные правонарушения, административная ответственность за которые предусмотрена следующими пунктами ст. 13.11 КоАП РФ:

– пункт 3 ст. 13.11 КоАП РФ – неисполнение обязанности (предусмотренной ч. 2 ст. 18.1 Федерального закона № 152-ФЗ) по обеспечению доступа как к документу о политике оператора в области обработки персональных данных, так и к сведениям о применяемых оператором требованиях к защите персональных данных (максимальный размер административной ответственности – до шестидесяти тысяч рублей);

– пункт 4 ст. 13.11 КоАП РФ – неисполнение обязанности (предусмотренной ч. 4 ст. 14 Федерального закона № 152-ФЗ) по предоставлению субъекту персональных данных соответствующей информации (максимальный размер административной ответственности – до восьмидесяти тысяч рублей);

– пункты 5 и 5.1 ст. 13.11 КоАП РФ – неисполнение в соответствующий срок обязанности (предусмотренной ст. 21 Федерального закона № 152-ФЗ) по уточнению, уничтожению или блокировке имеющихся сведений, относящихся к персональным данным (максимальный размер административной ответственности – до девяноста тысяч рублей и до полумиллиона при повторном совершении).

В этом случае следует особо ответить, что данный состав административного правонарушения не является длящимся в силу прямого указания на обстоятельство «неисполнение в срок» в соответствии с абз. 3 п. 19 Постановления Пленума ВАС РФ от 27 января 2003 года № 2 «О некоторых вопросах, связанных с введением в действие Кодекса Российской Федерации об административных правонарушениях»;

– пункт 6 ст. 13.11 КоАП РФ – невыполнение оператором обязанности по обеспечению сохранности и неприкосновенности персональных данных, если таковое произошло без использования средств автоматизации и повлекло за собой совершение кем-либо неправомерных действий с полученными персональными данными.

В данном случае следует особо отметить, что этот состав административного правонарушения относится к числу материальных, то есть для наступления административной ответственности по этому основанию необходимо наличие определённых материальных последствий;

– пункт 7 ст. 13.11 КоАП РФ – невыполнение обязанности по обезличиванию персональных данных: специфика в данном случае будет заключаться в особом субъекте (должностное лицо государственного или муниципального органа), административное наказание – до двенадцати тысяч рублей;

– пункты 8 и 9 ст. 13.11 КоАП РФ – можно сформулировать как использование оператором баз данных, находящихся вне пределов Российской

Федерации (максимальный размер административной ответственности – до шести миллионов рублей и до восемнадцати миллионов при повторном совершении).

В данном случае (а также в п. 1.1 ст. 13.11 КоАП РФ и во всех последующих) следует особо отметить, что административная ответственность индивидуальных предпринимателей будет равна соответствующей ответственности для юридических лиц, что является особым исключением из общего правила ст. 2.4 КоАП РФ, в соответствии с которым индивидуальные предприниматели приравниваются к должностным лицам;

– отдельно следует указать новые составы административных правонарушений (пп. 10–18 ст. 13.11 КоАП РФ). Основанием для административной ответственности в этом случае будет либо невыполнение оператором обязанности по уведомлению о намерении обрабатывать ПДн, либо совершение любых действий, которые привели к утечке ПДн. Административные штрафы в этом случае варьируются в зависимости от количества идентификаторов и могут достигать 5 миллионов, а также 1–3 % от суммы выручки или размера собственных средств кредитной организации, но не более 500 миллионов рублей.

Спецификой в этом случае будет то, что ранее оборотные штрафы применялись только в отношении наиболее тяжких административных правонарушений за нарушение антимонопольного законодательства (по ст. 14.31, 14.34 и 14.43.1 КоАП РФ). Глобальные утечки ПДн теперь являются специальным составом административных правонарушений.

В части анализа динамики изменения всех вышеуказанных в данной подгруппе соответствующих норм можно упомянуть, что в 2021 году размеры административных штрафов по всем из них были существенным образом увеличены в соответствии с принятием Федерального закона от 24 февраля 2021 года № 19-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях». А рассмотренный нами последний пример был дополнительно включён в текст данной статьи в 2019 году в связи с принятием Федерального закона от 2 декабря 2019 года № 405-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».

Следующие из нижеперечисленных административных правонарушений можно сгруппировать по такому признаку, как наличие квалифицирующих признаков для привлечения к административной ответственности, по этим специальным составам административных правонарушений, а не по соответствующим общим основаниям.

Итак, к группе особых составов административных правонарушений с квалифицирующими признаками будут относиться административные правонарушения, административная ответственность за которые предусмотрена ст. 13.11.3 «Нарушение требований в области размещения биометрических персональных данных», 13.14 «Разглашение информации с ограниченным доступом», 13.14.1 «Незаконное получение информации с ограниченным доступом», а также 17.13 «Незаконное распространение сведений о защищаемых лицах». В данных нормах КоАП РФ содержатся следующие составы административных правонарушений:

– статья 13.11.3 КоАП РФ – размещение и обновление организациями биометрических персональных данных в нарушение требований ст. 4 Федерального закона № 152-ФЗ (квалифицирующим признаком в данном составе будет специальный объект административного правонарушения: общественные отношения в области размещения и обновления именно биометрических персональных данных, а субъектами ответственности будут не только юридические лица, но и должностные лица, административная ответственность для последних будет составлять до трёхсот тысяч рублей, а в отношении юридических лиц административная ответственность установлена до миллиона рублей). При этом отдельно следует заметить, что данный состав административных правонарушений был нормативно закреплён в КоАП РФ лишь в 2023 году в связи с принятием Федерального закона от 12 декабря 2023 года № 589-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»;

– статья 13.14 КоАП РФ – разглашение охраняемой законом информации, совершённое лицом, получившим доступ к ней в рамках выполнения

профессиональных обязанностей. Стоит отметить, что по данному составу квалифицирующими признаками будут одновременно и объект административного правонарушения (общественные отношения в области защиты охраняемой законом информации, к числу которой относятся не только персональные данные, но и банковская, медицинская, коммерческая и иная тайны), и субъект административного правонарушения (адвокаты, нотариусы, любые иные работники, и соответственно их работодатели, и иные субъекты профессиональной деятельности). Административная ответственность может достигать 200 тысяч рублей.

Обращает на себя внимание, что данный состав административного правонарушения является особым ещё и в силу того, что в качестве меры административного наказания предусматривает дисквалификацию. Если проследить динамику законотворческой работы в области совершенствования данной нормы, то можно в качестве наиболее существенных изменений выделить лишь изменения в 2021 году в рамках поправок в КоАП РФ, в соответствии с которыми были значительно увеличены размеры административных штрафов, а также в санкцию данной статьи была включена ещё одна вариативная мера административного наказания в виде дисквалификации;

– статья 13.14.1 КоАП РФ была введена также после принятия вышеуказанных поправок в КоАП РФ и по своему объекту идентична ранее рассмотренному примеру, но с объективной стороны выражается в незаконном получении охраняемой законом информации. Отличие обнаруживает себя и в отсутствии специального квалифицирующего признака субъекта данного административного правонарушения.

Иными словами, в данном случае будет безразлично, получило ли лицо незаконным способом информацию в силу служебного положения или по иным причинам. Идентичны и санкции обоих рассматриваемых составов административных правонарушений.

В связи с чем представляется разумным отказаться от разграничения двух вышеуказанных составов и объединить их в один общий, сформулировав новый состав следующим образом:

«Статья 13.14. КоАП РФ «Незаконные действия по получению и (или) распространению информации с ограниченным доступом»

1. Незаконные действия по получению и (или) распространению информации, доступ к которой ограничен федеральным законом, за исключением случаев, предусмотренных статьей 5.53, частями 1 и 2 статьи 13.11, статьей 14.29, частью 5 статьи 15.19, частью 2 статьи 17.13 настоящего Кодекса, если эти действия не содержат признаков уголовно наказуемого деяния –

влекут наложение административного штрафа на граждан в размере от пяти тысяч до десяти тысяч рублей; на должностных лиц – от сорока тысяч до пятидесяти тысяч рублей или дисквалификацию на срок до трёх лет; на юридических лиц – от ста тысяч до двухсот тысяч рублей.

2. Незаконные действия, совершённые лицом (получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 и статьей 17.13 настоящего Кодекса), по получению и (или) распространению информации, доступ к которой ограничен федеральным законом, за исключением случаев, если совершение таких действий не влечёт уголовную ответственность –

влекут наложение административного штрафа на граждан в размере от десяти тысяч до пятнадцати тысяч рублей; на должностных лиц – от ста тысяч до трёхсот тысяч рублей или дисквалификацию на срок до пяти лет; на юридических лиц – от трёхсот тысяч до семисот тысяч рублей».

Помимо очевидной цели систематизации законодательства об административной ответственности в части совершенствования соответствующих норм об ответственности за незаконные действия по получению и (или) распространению информации с ограниченным доступом, достигаются также и другие важные с точки зрения нормотворчества цели:

1. Разглашение охраняемой законом информации станет административно наказуемо и для иных лиц, получивших доступ к таким сведениям вне служебного положения. Заметим, что сейчас такие действия строго формально не являются административно наказуемыми по непонятным причинам.

2. Незаконные действия по получению и (или) распространению охраняемой законом информации обычным, не обладающим квалифицирующими признаками субъектом будет специальным составом административного правонарушения по отношению ко всем иным, перечисленным в п. 1 предлагаемого варианта. Это будет способствовать тому, что в этом случае будет допустимо привлекать к административной ответственности по иным составам административных правонарушений, административная ответственность за которые предусмотрена, как правило, в более крупном размере административных штрафов.

3. Административная ответственность за любые незаконные действия по получению или распространению охраняемой законом информации (если эти действия совершены лицом в силу своего служебного положения) будет закономерным образом существенно выше и тем самым приравняется к административной ответственности по ч. 2 ст. 13.11 КоАП РФ за обработку персональных данных без согласия субъекта персональных данных. Имеющийся теперь порядок довольно сложно объяснить и обосновать, так как сейчас такой специальный субъект может быть привлечён к меньшей административной ответственности за разглашение охраняемой законом информации, чем за незаконную обработку персональных данных.

4. В качестве последнего в данном перечне аргументов, но не по значимости, можно обозначить как некоторую неопределённость в части законодательной техники, а именно: в соответствии с п. 1 ст. 28.4 КоАП РФ дела об административных правонарушениях, административная ответственность за которые предусмотрена … ст. 13.14, … возбуждаются прокурором. Иными словами, по ст. 13.14.1 КоАП РФ прокурор по общему правилу не вправе возбуждать дела об административных правонарушениях, кроме случаев, если указанное деяние было выявлено в ходе осуществления прокурорского надзора.

Данное положение сложно считать в достаточной мере обоснованным, особенно с учётом идентичности санкций обеих статьей КоАП РФ;

– статья 17.13 КоАП РФ содержит два пункта и довольно большое число составов административных правонарушений, которые можно обобщённо наименовать как нарушение законодательства о государственной защите конфиденциальности сведений о защищаемых лицах и об их имуществе (в том числе о персональных данных этих лиц). Квалифицирующим признаком в данном случае будет субъект административного правонарушения, а именно наличие специального государственно-правового статуса у потенциального потерпевшего.

В качестве ещё одной группы составов административных правонарушений можно рассматривать административные правонарушения, связанные с лицензированием и лицензионным контролем в области обращения персональных данных. К числу таких административных правонарушений относятся составы, закреплённые в пп. 1 и 5 ст. 13.12 «Нарушение правил защиты информации», а также в п. 1 ст. 13.13 «Незаконная деятельность в области защиты информации» КоАП РФ.

Такой избирательный подход обоснован тем, что иные составы административных правонарушений, которые закреплены в других пунктах вышеуказанных статей, в качестве своего объекта административных правонарушений называют совершенно иные группы общественных отношений, а именно: общественные отношения в области охраны сведений, составляющих государственную тайну. Такие общественные отношения не относятся к предмету нашего исследования, и потому отдельное их изучение не вполне обосновано в рамках нашей работы.

В пп. 1 и 5 ст. 13.12 КоАП РФ закреплены довольно похожие по своей объективной стороне административные правонарушения, так как в обоих случаях с объективной стороны административно наказуемым будет нарушение условий лицензии на осуществление деятельности в области защиты информации (в том числе деятельности по разработке и производству средств защиты конфиденциальной информации, а также самой деятельности по технической

защите конфиденциальной информации). Данная деятельность подлежит лицензированию в соответствии с Постановлением Правительства РФ от 3 марта 2012 года № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации», а также Постановлением Правительства РФ от 3 февраля 2012 года № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

С правовой точки зрения отличия в двух вышеуказанных составах будут заключаться в факте наличия или отсутствия дополнительного квалифицирующего признака в виде грубого нарушения лицензионных требований. Понятие грубого нарушения лицензионных требований дано отдельно в каждом из вышеперечисленных Постановлений Правительства РФ о лицензировании соответствующих видов деятельности.

Помимо указанных правовых отличий, разумеется, будет разниться и мера административной ответственности: в случае грубого нарушения – административное приостановление деятельности.

Если проследить историю развития административной ответственности по данным конкретным пунктам ст. 13.12 КоАП РФ, то окажется, что они не претерпели существенных изменений, а лишь были немного ужесточены в 2013 году в рамках принятия соответствующих поправок в КоАП РФ, но размеры административных штрафов по ним существенно не были увеличены, в отличие от всех рассмотренных нами ранее примеров административных правонарушений в области персональных данных.

В пункте 1 ст. 13.13 КоАП РФ установлена административная ответственность за занятие видами деятельности в области защиты информации (в том числе в области персональных данных), без наличия лицензии на осуществление ранее упомянутых в предыдущем примере видов деятельности. Такой состав административных правонарушений является специальным не только по отношению к «профильным» составам административных правонарушений в области персональных данных, но и одновременно по отношению к общему составу административных правонарушений, закреплённому в ст. 14.1 КоАП РФ

«Осуществление предпринимательской деятельности без государственной регистрации или без специального разрешения (лицензии)».

В качестве специфики данного состава административного правонарушения можно выделить наличие в санкции конфискации средств защиты информации. Такой вид административного наказания может применяться в качестве дополнительного к административному штрафу.

Динамика развития норм об административной ответственности по п. 1 ст. 13.13 КоАП РФ весьма примечательна отсутствием последующих изменений и дополнений, которые свойственны развитию норм, регулирующих активно развивающиеся отношения в области ПДн. Данная норма почти в неизменном виде сохранилась с момента принятия КоАП РФ, за исключением изменения порядка исчисления административных штрафов в 2007 году, когда административные штрафы перестали исчисляться в минимальных размерах оплаты труда, а стали исчисляться в твёрдом денежном выражении.

Эффективность правовой охраны в области персональных данных зависит в немалой степени от эффективности и неизбежности ответственности за нарушения законодательства о персональных данных, в том числе в части административной ответственности.

Вопрос об административной ответственности для операторов ПДн стал актуальным в 2017 году, когда с 1 июля 2017 года вступил в силу Федеральный закон от 07.02.2017 № 13-ФЗ, который преобразовал специальную статью 13.11 КоАП РФ из одного состава правонарушения в восемь, в соответствии с которыми квалифицируются административные правонарушения в области персональных данных.

По данным Роскомнадзора, в 2020 году чаще всего привлекали к ответственности за правонарушения, предусмотренные ч. 1, 5 и 6 ст. 13.11 КоАП РФ, а именно за обработку персональных данных в случаях, не предусмотренных законодательством РФ, а также за невыполнение требования об уточнении, блокировании или уничтожении персональных данных и за утечку данных.

Действующая редакция ст. 13.11 КоАП РФ перечисляет лишь отдельные обязанности, за неисполнение которых оператор понесёт ответственность. Законодатель не пошёл по пути использования бланкетной нормы (которая бы отсылала к законодательству о персональных данных), а лишь перечислил определённый круг обязанностей операторов обработки персональных данных. Из поля внимания законодателя выпали весьма актуальные и частые нарушения.

Для цели развития административно-правового регулирования обработки ПДн в Российской Федерации и одновременно для борьбы с незаконным оборотом персональных данных можно позаимствовать правовой механизм, установленный в испанском законодательстве. Законом Испании предусмотрено, что в случае рекламной рассылки рекламодатель обязан в каждом письме или сообщении указывать не только источник получения персональных данных субъекта и его права, но и сведения о личности держателя, о лице, осуществляющем рассылку. Такой подход помог бы дополнительно разрешить существующую проблему в области рассылки рекламы, поскольку рекламораспространитель будет идентифицирован и тем самым распространение рекламы таким способом будет снабжено минимально необходимыми правовыми инструментами для достижения правопорядка в данной области.

Один из институтов, который будет способствовать совершенствованию механизма административной ответственности и позволит мотивировать операторов персональных данных не нарушать действующее законодательство, – это введение новых видов административных наказаний наравне с действующими штрафами. В качестве новых наказаний стоит предусмотреть дисквалификацию и административное приостановление деятельности, которые, по мнению ряда учёных, будут создавать стимулы для соблюдения действующего законодательства, поскольку ни один хозяйствующий субъект не заинтересован в приостановлении своей деятельности. Судебный порядок наложения таких наказаний позволит не допустить возможных злоупотреблений со стороны государственных органов, выражающихся в необоснованном нарушении прав хозяйствующих субъектов.

Стоит отметить потенциальные шаги, которые нужно сделать для повышения эффективности действующего законодательства в сфере персональных данных. Поскольку главная цель, которую преследуют большинство операторов, – это извлечение прибыли, то главный механизм, который будет влиять на действия операторов, – это меры ответственности, предусмотренные действующим законодательством и напрямую влияющие на прибыль организации.

Подводя промежуточный итог нашему исследованию в рамках данного параграфа, следует сформулировать некоторые наиболее интересные и значимые выводы и предложения относительно развития института административной ответственности в области нарушения требований законодательства о персональных данных.

1. Можно выделить некоторые наиболее важные этапы реформирования данного правового института:

– 2017 год – начало существенных видоизменений института административной ответственности в области нарушения требований законодательства о персональных данных. Изменения заключались во включении в КоАП РФ множества новых составов административных правонарушений в данной области;

– 2019–2021 годы – последующее увеличение составов административных правонарушений в данной области и некоторое ужесточение санкций уже имеющихся составов административных правонарушений;

– 2023 год – включение в КоАП РФ некоторых дополнительных специальных составов административных правонарушений и существенное (иногда кратное) увеличение размеров административных штрафов в рамках данного правового института.

2. Выявлены две устойчивые тенденции в данной области:

– расширение числа составов административных правонарушений в области нарушения требований законодательства о персональных данных;

– ужесточение санкций уже имеющихся составов административных правонарушений в области нарушения требований законодательства о персональных данных.

3. Выявлена проблема частичного пересечения составов административных правонарушений (ст. 13.14 и 13.14.1 КоАП РФ), доказательством чему служат определённые неблагоприятные правовые последствия:

– разглашение охраняемой законом информации лицом, получившим доступ к таким сведениям вне служебного положения, строго формально не образует состав административного правонарушения;

– исключения, перечисленные в ст. 13.14.1 КоАП РФ, по непонятным причинам отсутствуют в аналогичной статье 13.14 КоАП РФ, что не соответствует достижению баланса частных и публичных интересов в данной области;

– административная ответственность по обоим составам административных правонарушений идентична в санкциях обеих статей, несмотря на то что по ст. 13.14 КоАП РФ субъектом ответственности является лицо, совершившее данное административное правонарушение в силу наличия служебного положения.

4. Разработаны предложения по развитию модели административной ответственности за нарушения законодательства о персональных данных. Выявлена проблема частичного пересечения двух составов административных правонарушений (ст. 13.14 и 13.14.1 Кодекса Российской Федерации об административных правонарушениях), в связи с чем предложен вариант её устранения путём введения единой статьи 13.14 Кодекса Российской Федерации об административных правонарушениях в новой редакции, которая будет предусматривать два самостоятельных состава административного правонарушения.

В частности, обосновано, что административно наказуемыми станут все незаконные действия по получению и (или) распространению информации, доступ к которой ограничен федеральным законом, за исключением случаев, предусмотренных статьей 5.53, частями 1–2.1, 10–18 статьи 13.11, статьей 14.29, частью 5 статьи 15.19, частью 2 статьи 17.13 Кодекса Российской Федерации об

административных правонарушениях, если эти действия не содержат признаков уголовно наказуемого деяния. Также предложен дополнительный квалифицирующий состав административного правонарушения, в рамках которого будет установлена административная ответственность за незаконные действия по получению и (или) распространению информации, доступ к которой ограничен федеральным законом, совершённые должностным лицом (лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 и статьей 17.13 Кодекса Российской Федерации об административных правонарушениях), за исключением случаев, если эти действия не содержат признаков уголовно наказуемого деяния.

5. Объективная сторона административного правонарушения, предусмотренная ст. 13.11 КоАП РФ, требует доработки в части установления бланкетной гипотезы к положениям законодательства о персональных данных, а именно в целях совершенствования юридической техники следует не перечислять виды неправомерных действий по поводу персональных данных, а установить общее условие в виде: «невыполнение оператором обязанностей и (или) требований законодательства в области персональных данных».

ЗАКЛЮЧЕНИЕ

По итогам нашего комплексного научного исследования публично-правового регулирования в сфере использования цифровых технологий при обработке персональных данных можно сделать определённые теоретические выводы и предложения по совершенствованию законодательства в данной области.

В современных условиях ускорения развития информационных технологий всё большую значимость приобретают правовые исследования в области различных технологических аспектов цифровых технологий. Наиболее передовыми и широко внедряемыми технологиями являются цифровые технологии, которые в последнее время начали применяться в том числе для обработки персональных данных. Правовое регулирование данных процессов исключительно частноправовыми средствами не позволяет достичь баланса интересов между всеми участниками этих правоотношений, с одной стороны, и между участниками правоотношений и публичными интересами – с другой. В связи с чем публично-правовое регулирование в сфере использования цифровых технологий при обработке персональных данных и, соответственно, правовые исследования с публично-правовых позиций обретают особую научно-практическую значимость.

Вследствие вышесказанного выявленные автором правовые пробелы, правовые коллизии и иные проблемные аспекты в области применения различных цифровых технологий при обработке персональных данных (технологии распределённого реестра, облачные технологии и технологии искусственного интеллекта) обусловливают выбор диссертантом цели разработки и обоснования концептуальных теоретических основ публично-правового регулирования использования цифровых технологий при обработке персональных данных, а также в выработке подходов и предложений по совершенствованию российского законодательства в рассматриваемой сфере. В ходе проведённого научного исследования выбранной проблематики были получены определённые выводы,

которые позволяют констатировать, что вышеуказанная цель успешно достигнута посредством решения определённой последовательности задач.

Ниже изложены некоторые наиболее важные выводы, которые были получены в рамках достижения поставленной цели диссертационного исследования и решения соответствующих научных задач.

Проведённое исследование правовой природы персональных данных позволило сформулировать авторское определение понятия «персональные данные»: это любая информация о физическом лице (субъекте персональных данных), которая позволяет идентифицировать данное лицо, за исключением, если такая информация содержится в обезличенном виде, а также иная информация, напрямую названная таковой в законе.

Помимо этого, автор обосновывает необходимость вывести презумпцию относимости информации к персональным данным физического лица. В целях обеспечения защиты прав субъектов персональных данных, с учётом расширения процессов цифровизации в современном государстве и обществе, предложена специальная информационно-правовая презумпция относимости данных к персональным данным физического лица: «Любую информацию следует относить к числу персональных данных, если субъект этой информации заявляет о том, что данная информация определяет или позволяет его определить (идентифицировать). Обязанность по доказыванию обстоятельств, свидетельствующих об обратном, возлагается на лицо, осуществляющее обработку персональных данных».

Относительно правовой природы персональных данных был получен вывод о том, что исследуемая правовая категория относится к такой крупной правовой категории, как «информация», и находится в одном ряду с иными специальными категориями охраняемой законом информации, а также что структурно данный правовой институт объединяет не только нормы различных отраслей, но и отраслей различной правовой принадлежности, с превалирующей публично-правовой составляющей.

Для цели развития науки информационного права выявлены и обоснованы правовые признаки, которым должны отвечать сведения, относящиеся к

персональным данным, в качестве обязательных в процессе их отнесения к таковым: возможность определить конкретного субъекта по данным; возможность связать данные для соотношения информации и субъекта; возможность произвести умозаключение, что данные принадлежат конкретному субъекту; возможность обособления конкретных персональных данных друг от друга; персональные данные должны отвечать всем вышеуказанным признакам одновременно.

Диссертантом подчёркивается вывод о том, что с научно-практической точки зрения представляется целесообразным отнести данные о наличии инвалидности к числу общедоступных персональных данных. Наличие инвалидности – это социальный статус, и к специальным категориям персональных данных данные о наличии инвалидности не должны относиться. Такой подход позволит не допускать дополнительных оснований для дискриминации лиц с ограниченными возможностями. Для гражданско-правовых, трудовых и ряда иных правоотношений данные о наличии инвалидности (без указания о заболевании и иных данных, составляющих медицинскую тайну) необходимы для учёта различных льгот и иных мер поддержки, а также специальных требований к рабочему месту и характеру трудовой функции.

В ходе исследования специфики правовой природы персональных данных был обоснован вывод о том, что информация о социальном статусе, а также иная информация об относимости к специальным социальным категориям (например, об инвалидности) сама по себе не должна быть отнесена к специальным категориям персональных данных, особенно в случае, если такая информация требуется для предоставления дополнительных социальных и иных гарантий.

В результате раскрытия специфики правовой природы обработки персональных данных с использованием цифровых технологий было выявлено, что каждый термин: «предоставление», «распространение», «доступ» – является самостоятельной правовой категорией, влекущей необходимость применения различных средств правового регулирования. Соответственно, смешивание вышеуказанных правовых категорий может привести к определённым неблагоприятным последствиям.

В связи с этим в целях повышения эффективности института обработки персональных данных и обеспечения прав субъектов персональных данных предложено закрепить специальную терминологическую базу методов обработки ПДн для достижения наибольшей эффективности правового регулирования и защиты конституционных прав гражданина и соблюдения принципов обработки ПДн. Наиболее удачным вариантом в таком случае будет выбор пути упрощения правопонимания категории «обработка персональных данных» посредством исключения отдельной составной части данной категории в виде «передачи персональных данных». Результатом такого решения будет несколько иное формулирование понятия категории «обработка персональных данных», которое будет пониматься как «любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, распространение, предоставление, доступ, обезличивание, блокирование, удаление и уничтожение персональных данных».

В рамках исследования правовой основы использования цифровых технологий при обработке персональных данных (несмотря на введение в уголовное законодательство нескольких специальных составов преступлений в отношении компьютерной информации, содержащей персональные данные) обоснована недостаточность имеющихся средств уголовно-правовой защиты общественных отношений в области персональных данных, несмотря на введение ст. 272.1 в УК РФ. Ввиду чего предложено установить уголовную ответственность за совершение деяния, которое выражается в «неправомерных действиях с персональными данными или иной охраняемой законом информацией при условии, если такие деяния повлекли тяжкие последствия».

Тяжкие последствия в настоящем случае понимаются в смысле соответствующих положений Постановления Пленума Верховного Суда РФ от 15.12.2022 №37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях,

совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».

Обоснованность данного предложения дополнительно заключается в реализации взятых на себя Российской Федерацией обязательств в рамках Конвенции ООН о киберпреступлениях. Помимо этого, в качестве дополнительных квалифицирующих признаков, устанавливающих более суровую меру уголовной ответственности, следовало бы рассматривать совершение преступления группой лиц по предварительному сговору, или организованной группой, или лицом с использованием своего служебного положения.

На основе анализа истории развития правового регулирования в области персональных данных автором предложены некоторые наиболее важные стадии становления данного правового института, которые характеризуются в первую очередь уровнем правового регулирования и набором применяемых правовых средств. В связи с этим доказано, что важнейшие стадии в становлении и развитии правового регулирования персональных данных можно представить следующим образом:

I. Стадия концептуального развития принципов неотъемлемости информационных прав и свобод человека.

II. Стадия развития международно-правового регулирования обработки персональных данных посредством закрепления правовых основ и принципов.

III. Стадия становления и развития национального законодательства в зарубежных юрисдикциях в сфере регулирования обработки персональных данных.

IV. Стадия становления и развития отечественного законодательства в сфере публично-правового регулирования персональных данных.

V. Стадия правовой трансформации в области правового регулирования обработки персональных данных в условиях развития цифровых технологий.

Доказано, что основной проблемой публично-правового регулирования обработки персональных данных с использованием технологий искусственного интеллекта остаётся соблюдение баланса между требованиями по защите

персональных данных и необходимостью их использования для обучения систем искусственного интеллекта для цели выполнения задачи повышения доступности и качества данных. Введение полного запрета на обработку персональных данных с использованием искусственного интеллекта приведёт к фактическому блокированию любых разработок, связанных с развитием и внедрением искусственного интеллекта. Ввиду этого предлагается нормативное закрепление обязанности получения специального согласия на обработку персональных данных при использовании искусственного интеллекта.

Автором приводится и обосновывается вывод о том, что обезличивание персональных данных выступает методом снижения рисков нарушения прав субъектов персональных данных при обработке данных с использованием искусственного интеллекта, но само по себе не может обеспечивать абсолютные гарантии защиты прав субъектов персональных данных. Обезличенные данные содержат в себе цифровые следы, по которым с использованием технологий искусственного интеллекта возможно установить их соответствие тому или иному субъекту персональных данных. Ввиду чего требуется наличие отдельного согласия на обработку персональных данных при обработке персональных данных с использованием искусственного интеллекта. Таким образом, развитие публично-правового регулирования обработки персональных данных при использовании и обучении искусственного интеллекта не будет препятствовать минимизации рисков раскрытия персональных данных неопределённому кругу лиц без согласия и ведома субъекта. Такое согласие представляется обязательным, по крайней мере до завершения процесса эксперимента и выработки полноценного правового и технического регулирования.

В работе отмечается проблема публично-правового регулирования обработки персональных данных с использованием технологий искусственного интеллекта, которая заключается в необходимости разработки и принятия цельного, единого источника правового регулирования искусственного интеллекта. Выявлено, что отдельные федеральные законы не обеспечивают комплексный нормативно-правовой подход к регулированию данной области, а

направлены на правовое регулирование лишь точечных процессов обработки персональных данных с использованием искусственного интеллекта. Предложено решение в виде принятия комплексного федерального закона, регулирующего искусственный интеллект, в том числе в части регулирования процессов, связанных с обработкой обезличенных персональных данных с помощью технологии искусственного интеллекта.

При решении научной задачи по обоснованию специфики публично-правового регулирования в сфере использования технологий распределённого реестра при обработке персональных данных обоснован тезис о том, что использование блокчейн-технологии отличается высокой степенью анонимизации, что обеспечивает высокий уровень соблюдения конституционных прав граждан при обработке персональных данных. Учитывая децентрализованное хранение данных, а также специальный порядок действий в отношении блокчейна, при котором сохранённые данные защищены от несанкционированных действий в том числе с использованием инструментов шифрования, использование блокчейн-технологии в большей степени способно гарантировать высокий уровень анонимизации персональных данных. Вышеуказанная специфика технологии распределённого реестра создаёт более высокую степень доверия к данным в цепочке блокчейна.

Автором обоснована необходимость законодательного закрепления обязанности применения операторами персональных данных специальных мер, направленных на реализацию возможности эффективного уничтожения персональных данных в блокчейне (чтобы после удаления на одном устройстве данные становились неразборчивыми для идентификации любого, кто может получить доступ к данным по цепочке хранения), например с помощью шифрования и удаления ключей дешифрования. Указанные рекомендации предлагаются в целях минимизации рисков, связанных с обеспечением контроля над кругом субъектов, которые могут получить доступ к персональным данным при использовании технологии блокчейн и иных схожих технологий.

Автором выявлена проблема публично-правового регулирования в сфере использования технологий распределённого реестра при обработке персональных данных, которая заключается в том, что затруднительно установить эффективный и точный механизм контроля над кругом лиц, которые могут получить доступ к персональным данным при использовании блокчейн-технологий. В целях минимизации рисков, связанных с обеспечением контроля над кругом субъектов, которые могут получить доступ к персональным данным при использовании технологии блокчейн и иных схожих технологий, обоснована необходимость законодательного закрепления обязанности применения операторами персональных данных специальных мер, направленных на реализацию возможности эффективного уничтожения персональных данных в блокчейне (чтобы после удаления на одном устройстве данные становились неразборчивыми для идентификации любого, кто может получить доступ к данным по цепочке хранения), например с помощью шифрования и удаления ключей дешифрования. Таким образом, закрепление требований к обязательному применению шифрования или обязательному удалению ключей дешифрования при обработке персональных данных посредством использования технологии блокчейн, а также путём применения технологий управления доступом к данным и технологий доказательства нулевого разглашения является наиболее эффективным правовым механизмом достижения целей и принципов законодательства в области персональных данных.

В условиях особого развития сервисов публичных облаков в Российской Федерации, роста решений на рынке и перехода к публичным облакам во всех сферах, в том числе государственных и частных, доказана необходимость специального правового регулирования функционирования публичных облаков, которое подробно и системно позволило бы установить правовую основу деятельности владельцев публичных облаков, а также разграничить и закрепить нормативно виды публичных облаков и специфику их правового регулирования. Автором обосновывается, что данная задача может быть решена путём

разграничения и нормативного закрепления правовой специфики следующих видов публичных облаков:

– программное обеспечение как услуга (Software-as-a-Service / SaaS);

– платформа как услуга (Platform-as-a-Service / PaaS);

– инфраструктура как услуга (Infrastructure-as-a-Service / IaaS);

– рабочее место как услуга (Desktop as a Service / DaaS).

Автором обосновано, что действующее нормативно-техническое регулирование применения публичных облаков не позволяет должным образом определить термин «публичное облако». В связи с этим предложено правовое определение понятия «публичное облако», в качестве которого следует понимать «услугу, позволяющую пользователю обеспечить обработку, хранение, управление и резервное копирование данных с помощью предоставления доступа к сервисам сервера, программному обеспечению и техническим средствам». Выявлено, что основными формами применения публичных облаков в публичных целях являются: программное обеспечение как услуга; платформа как услуга; инфраструктура как услуга; рабочее место как услуга. Также аргументировано предложение по изменению наименования термина «публичное облако» на более точную формулировку термина: «сервисы облачной обработки данных». Предложенная формулировка термина более точно позволяет понять суть технологии и не меняет смысл широкого многообразия применения технологии.

Также в ходе выполнения задачи формулирования специфики публично-правового регулирования в сфере использования облачных технологий при обработке персональных данных выявлена проблема, связанная с риском невыполнения требований об удалении персональных данных, хранящихся на публичных облаках. Хранение и обработка, уничтожение данных компанией-исполнителем (обработчиком) на облачных серверах технически может осуществляться неопределённое время, даже после их удаления пользователем облачного сервиса. Решение такой проблемы исключительно правовыми средствами представляется малоэффективным, ввиду чего предложено

установление административной ответственности за невыполнение требования субъекта персональных данных об их удалении.

Показана актуальная проблема обработки персональных данных, связанная с этическими вопросами при использовании цифровых технологий. Продемонстрирована необходимость учёта этического аспекта при разрешении некоторых вопросов в области персональных данных исходя из ситуационного правового регулирования в конкретном случае, в связи с чем необходимо выработать принципы и методы определения баланса между охраной частной собственности и правом на тайну частной жизни.

Выявлена этико-правовая проблема, которая заключается в использовании средств фотовидеофиксации как способе вмешательства в частную жизнь, нарушающем законодательство о персональных данных. Автором предлагается набор правил, определяющих законность установки средств фотовидеофиксации, используя которые, возможно найти этико-правовой баланс при публично-правовом регулировании обработки ПДн между правом на уважение частной жизни и защитой частной собственности.

Предложены правовые признаки, определяющие законность установки и универсального использования средств фотовидеофиксации гражданами в части недопустимости нарушения требований обработки персональных данных.

Для признания правомерности установки средств фотовидеофиксации (камер и других средств) необходимо соблюдение совокупности условий:

– средство фотовидеофиксации установлено для целей охраны имущества, жизни и здоровья;

– средство фотовидеофиксации установлено на личной территории;

– средство фотовидеофиксации не направлено на территорию и имущество другого лица как на главный объект съёмки*;*

– данные, полученные со средств фотовидеофиксации, не нарушают неприкосновенность частной жизни, личную и семейную тайну.

Соответствующие правовые признаки целесообразно закрепить в рамках приказа Роскомнадзора как уполномоченного органа в контексте обобщения

практики осуществления государственного контроля (надзора) в области персональных данных.

При решении задачи по раскрытию проблем правового регулирования использования цифровых технологий при обработке персональных данных, составляющих врачебную тайну, был сделан вывод о целесообразности в научно-практических целях внести изменения в действующий Закон об основах охраны здоровья, дополнив его положениями о допустимости предоставления медицинских данных умерших пациентов супругам, родственникам и иным заинтересованным лицам по их запросу. При этом учитывая цели такого запроса, чтобы минимизировать риски обнародования или использования полученных сведений в корыстных целях.

Автором была выявлена проблема соотношения норм о персональных данных с нормами законодательства в сфере охраны и социального обеспечения. В частности, была поставлена проблема об относимости данных о наличии инвалидности к числу общедоступных персональных данных. Обосновано, что наличие инвалидности – это социальный статус, и данные о ней не должны относиться к специальным категориям персональных данных. Данный подход позволит не допускать дополнительных оснований для дискриминации лиц с ограниченными возможностями.

Развитие законодательства в области административной ответственности за нарушения законодательства о персональных данных характеризуется регулярным включением в КоАП РФ новых составов административных правонарушений в области защиты ПДн и ужесточением санкций уже имеющихся составов административных правонарушений.

Автором была выявлена проблема частичного пересечения двух составов административных правонарушений (ст. 13.14 и 13.14.1 КоАП РФ), доказательством чему служат определённые неблагоприятные правовые последствия:

– разглашение охраняемой законом информации лицом, получившим доступ к таким сведениям вне служебного положения, строго формально не образует состав административного правонарушения;

– исключения, перечисленные в статье 13.14.1 КоАП РФ, по непонятным причинам отсутствуют в аналогичной статье 13.14 КоАП РФ, что не соответствует достижению баланса частных и публичных интересов в данной области;

– административная ответственность по обоим составам административных правонарушений идентична в санкциях обеих статей, несмотря на то что по статье 13.14 КоАП РФ субъектом ответственности является лицо, совершившее данное административное правонарушение в силу наличия служебного положения.

В работе автором доказывается обоснованность и предлагается вариант устранения проблемы соотношения и дифференциации ст. 13.14 и 13.14.1 КоАП РФ посредством формулирования ст. 13.14 КоАП РФ в новой редакции и признания ст. 13.14.1 КоАП РФ утратившей силу.

Вышеуказанные выводы и предложения позволяют констатировать, что все намеченные задачи диссертационного исследования были успешно решены. Помимо этого, основываясь на подведённых итогах научного исследования в области публично-правового регулирования в сфере использования цифровых технологий при обработке персональных данных, представляется возможным сформулировать некоторые предложения научно-теоретического плана, а также предложения по дальнейшему совершенствованию законодательства в исследуемой области.

К числу последних можно отнести научно-практические рекомендации по включению в Уголовный кодекс Российской Федерации общей статьи за нарушение законодательства в области персональных данных (при условии наступления тяжких последствий); нормативное закрепление требования о наличии специального согласия на обработку персональных данных посредством применения технологий искусственного интеллекта; установление законодательного требования о наличии специальных технических средств, обеспечивающих должный уровень защиты персональных данных при обработке с

помощью блокчейна; а также нормативное закрепление критериев правомерности использования средств фотовидеофиксации и многие другие предложения.

В научно-теоретическом плане были достигнуты определённые результаты и выдвинуты конкретные предложения, которые могут способствовать развитию науки информационного права, а также некоторых других публично-правовых наук: было предложено авторское определение категории «персональные данные», уточнена методология в части способов обработки персональных данных, выявлены наиболее важнейшие стадии в развитии правового регулирования персональных данных в целом и административной ответственности в данной области в частности, а также многие иные.

Достигнутые в результате проведённого исследования выводы и предложения могут быть применены для концептуальных разработок в сфере формирования комплексного представления о публично-правовом регулировании в сфере использования цифровых технологий при обработке персональных данных.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

I. Нормативные правовые акты

Международно-правовые акты:

1. Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981 // Собрание законодательства РФ. – 2014. – № 5. – Ст. 419.

2. Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определёнными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям. [Электронный ресурс]. Режим доступа: https://www.un.org/ru/documents/treaty/A-RES-79-243, свободный (дата обращения 01.02.2025).

3. Основные положения Организации по экономическому сотрудничеству и развитию (ОЭСР) о защите неприкосновенности частной жизни и международных обменов персональных данных, 1980. [Электронный ресурс]. Режим доступа: http://www.uipdp.com/upload/legislation/international/directive_oesr1.pdf (дата обращения: 01.06.2024).

4. Протокол о внесении изменений в Конвенцию о защите физических лиц при автоматизированной обработке персональных данных (CETS № 223) (Подписан в г. Страсбурге 10.10.2018) // Бюллетень Европейского суда по правам человека. Российское издание. − 2018. − № 12.

5. Руководство ООН относительно компьютерных файлов персональных данных. Принято Генеральной Ассамблеей ООН 14.12.1990 [Электронный ресурс]. Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/computerized_data.shtml, свободный (дата обращения: 01.06.2025).

Конституция, федеральные законы, законы субъектов Российской Федерации

6. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 года с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 года) // Официальный интернет-портал правовой информации http://pravo.gov.ru (дата обращения: 06.10.2022).

7. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Собрание законодательства РФ. – 1994. – № 32. – Ст. 3301.

8. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.

9. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Собрание законодательства РФ. – 2001. – № 2002. – № 1 (ч. 1). – Ст. 1.

10. Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» // Собрание законодательства РФ. – 2005. – № 52 (ч. 1). – Ст. 5573.

11. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451.

12. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3448.

13. Федеральный закон от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» // Российская газета. – 2014. – № 163.

14. Федеральный закон от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» // Собрание законодательства РФ. – 2011. – № 31. – Ст. 4701.

15. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» //

Российская газета. – 2017. – № 167.Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 23.07.2025) «Об основах охраны здоровья граждан в Российской Федерации» // Собрание законодательства РФ. – 2011. – № 48. – Ст. 6724.

16. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» // Собрание законодательства РФ. – 2011. – № 7. – Ст. 900.

17. Федеральный закон от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // Собрание законодательства РФ. – 2020. – № 17. – Ст. 2701.

18. Федеральный закон от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности» // Собрание законодательства РФ. – 2022. – № 29 (ч. III). – Ст. 5233.

19. Федеральный закон от 12.12.2023 № 589-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // Собрание законодательства РФ. – 2023. – № 51. – Ст. 9162.

20. Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства РФ. – 2023. – № 1 (ч. 1). – Ст. 19.

21. Федеральный закон от 08.08.2024 № 233-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий

искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных». Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202408080031, свободный (дата обращения: 01.06.2025).

Указы Президента Российской Федерации, постановления и распоряжения Правительства Российской Федерации:

22. Указ Президента РФ от 01.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» // Собрание законодательства РФ. – 1997. – № 10. – Ст. 1127.

23. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства РФ. – 2012. – № 45. – Ст. 6257.

24. Постановление Правительства РФ от 12.04.2012 № 287 «Об утверждении Положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации» // Собрание законодательства РФ. – 2012. – № 16. – Ст. 1885.

25. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. – 2016. – № 50. – Ст. 7074.

26. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017– 2030 годы» // Собрание законодательства РФ. – 2017. – № 20. – Ст. 2901.

27. Распоряжение Правительства России от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» // Собрание законодательства РФ. – 2017. – № 32. – Ст. 5138.

28. Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства РФ. – 2019. – № 41. – Ст. 5700.

29. Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // Собрание законодательства РФ. – 2020. – № 35. – Ст. 5593.

30. Постановление Правительства РФ от 29.06.2021 № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных» // Собрание законодательства РФ. – 2021. – № 27 (ч. III). – Ст. 5424.

31. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. – 2021. – № 27 (ч. II). – Ст. 5351.

32. Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Собрание законодательства РФ. – 2024. – № 20. – Ст. 2584.

33. Перечень поручений по реализации Послания Президента Федеральному Собранию. Утв. Президентом РФ 30.03.2024 № Пр-616.

Нормативные правовые и иные акты органов исполнительной власти:

34. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения». [Электронный ресурс]. Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71652212/?ysclid=lwchijkaii571205726, свободный (дата обращения: 01.06.2025).

35. Приказ Минздрава России от 24.12.2018 № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским

информационным системам медицинских организаций и информационным системам фармацевтических организаций» // Официальный интернет-портал правовой информации. [Электронный ресурс]. Режим доступа: http://www.pravo.gov.ru, свободный (дата обращения: 01.06.2025).

36. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.08.2022 № 128 «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных» // Собрание законодательства РФ. – 2022. – № 16. – Ст. 967.

37. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) // СПС «КонсультантПлюс».

Законодательство иностранных государств и международное законодательство:

38. Директива 97/66/ЕС Европейского парламента и Совета Европейского союза об использовании персональных данных и защите неприкосновенности частной жизни в сфере телекоммуникаций (Принята в Страсбурге 15.12.1997) // СПС «КонсультантПлюс».

39. Data Protection Act 1998, Section 1 (1). URL: https://www.legislation.gov.uk/ukpga/1998/29/section/1/1998-07-16 (дата обращения: 10.05.2024).

40. Amended Act on the Protection of Personal Information. URL: https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf (дата обращения: 02.05.2024).

41. California Consumer Privacy Act. URL: https://cppa.ca.gov/regulations/pdf/cppa_act.pdf (дата обращения: 10.05.2024).

42. Data Protection Act 2018, Section 3 (2), (3). URL: https://www.legislation.gov.uk/ukpga/2018/12/section/3 (дата обращения: 10.05.2024).

43. Data Privacy Act of 1974. URL: https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf (дата обращения: 10.05.2024).

44. Personal Information Protection Law of the People's Republic of China (PIPL) от 2021 года. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1716804666&tld=ru&lang=en&name=Personal-Information-Protection-Law-of-the-Peoples-Republic-of-China.pdf&text=Personal+Information+Protection+Law+of+the+People's+Republic+of+China+%28PIPL%29+от+2021+года&url=https%3A//www.china-briefing.com/news/wp-content/uploads/2021/08/Personal-Information-Protection-Law-of-the-Peoples-Republic-of-China.pdf&lr=43&mime=pdf&l10n=ru&sign=15649ac8fa4b45020874e2c17035c280&keyno=0, свободный (дата обращения: 01.06.2025).

45. Draft Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts. [Электронный ресурс]. Режим доступа: https://www.europarl.europa.eu/resources/library/media/20230516RES90302/20230516RES90302.pdf (дата обращения: 01.06.2024).

46. European Commission. Proposal for a regulation of the European Parliament and of the council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts. COM(2021) 206 final. Brussels, 21 April 2021. [Электронный ресурс]. Режим доступа: https://artificialintelligenceact.eu/the-act/ (дата обращения: 01.06.2024).

47. Рекомендации по искусственному интеллекту и защите данных. T- PD(2019)01. Страсбург, 25.01.2019. [Электронный ресурс]. Режим доступа: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8 (дата обращения: 01.06.2024).

48. Разъяснения Национального института стандартизации и технологий США. [Электронный ресурс]. Режим доступа:

https://docviewer.yandex.ru/?tm=1717182010&tld=ru&lang=ru&name=dk5pes2uk2wyu798vml6uc6jny1jizas.pdf&text=облачным+сервисом+%28публичным+облаком%29%2C+согласно+разъяснениям+Национального+института+стандартизации+и+технологий+США%2C&url=https%3A//ncsa.ru/upload/iblock/4eb/dk5pes2uk2wyu798vml6uc6jny1jizas.pdf&lr=43&mime=pdf&l10n=ru&sign=75a7f0a1e06e4f9bd164d9fc79252a8f&keyno=0, свободный (дата обращения: 01.06.2025).

49. Artificial Intelligence Act, Article 5: Prohibited Artificial Intelligence Practices. URL: https://artificialintelligenceact.eu/article/5/ (дата обращения: 01.06.2025).

50. Общий регламент по защите данных от 27.04.2016 г., или GDPR (General Data Protection Regulation), или Регламент ЕС 2016/679. [Электронный ресурс]. Режим доступа: https://ogdpr.eu/ru/gdpr-2016-679, свободный (дата обращения: 01.06.2025).

51. Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. [Электронный ресурс]. Режим доступа: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021PC0206, свободный (дата обращения 01.06.2025).

52. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of the European Union N L 119. 04.05.2016. P. 1.

Нормативно-технические и иные официальные документы:

53. ГОСТ Р 52292–2004. Информационная технология. Электронный обмен информацией. Термины и определения / Утвержден и введён в действие приказом Федерального агентства по техническому регулированию и метрологии от 29.12.2004 № 135-ст. – М.: ИПК Издательство стандартов, 2005.

54. ГОСТ 33707–2016 (ISO/IEC 2382:2015). Межгосударственный стандарт. Информационные технологии. Словарь / Введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22.09.2016 № 1189-ст. – М.: Стандартинформ, 2016.

55. ГОСТ Р ИСО/МЭК 27018–2020. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки (утв. и введён в действие Приказом Росстандарта от 10.11.2020 № 1042-ст). – М.: Стандартинформ, 2020.

56. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам (протокол от 04.06.2019 № 7). [Электронный ресурс]. Режим доступа: https://digital.gov.ru, свободный (дата обращения: 01.06.2025).

57. Цифровая трансформация и защита прав граждан в цифровом пространстве. Доклад Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека // Информация для всех. [Электронный ресурс]. Режим доступа: https://ifap.ru/pr/2021/n211213a.pdf (дата обращения: 11.06.2025).

58. ИСО/МЭК 27018:2019 «Информационные технологии. Методы обеспечения безопасности. Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки» (ISO/IEC 27018:2019 «Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors») // ФГБУ «Институт стандартизации». [Электронный ресурс]. Режим доступа: https://www.gostinfo.ru/catalog/Details/?id=6444427 (дата обращения: 01.06.2025).

59. ISO/IEC 17826:2022(en), 3.45 // ИСО – Международная организация по стандартизации. [Электронный ресурс]. Режим доступа: https://www.iso.org/ru/standard/83451.html (дата обращения: 01.06.2025).

60. Проект федерального закона № 992331-7 «О внесении изменений в Федеральный закон «О персональных данных» (в части уточнения порядка обработки персональных данных) // Система обеспечения законодательной деятельности. [Электронный ресурс]. Режим доступа: https://sozd.duma.gov.ru/bill/992331-7 (дата обращения: 12.09.2023).

61. Проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации» (в части установления ответственности за незаконные использование и передачу, сбор и хранение компьютерной информации, содержащей персональные данные) // Система обеспечения законодательной деятельности. [Электронный ресурс]. Режим доступа: https://sozd.duma.gov.ru/bill/502113-8 (дата обращения: 06.03.2024).

Материалы судебной практики:

62. Постановление Пленума Верховного Суда РФ от 24.02.2005 № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» // Бюллетень Верховного Суда РФ. – 2005. – № 4.

63. Постановление Пятнадцатого арбитражного апелляционного суда № 15АП-7769/2011 от 13.04.2011 по делу № А-32-2810/2011. [Электронный ресурс]. Режим доступа: https://kad.arbitr.ru/Card/3d6395b0-26ab-4a19-aff5-218daca534aa (дата обращения: 01.06.2024).

64. Постановление Федерального арбитражного суда Московского округа от 01.12.2011 по делу № А40-129859/10-146-801. [Электронный ресурс]. Режим доступа: https://kad.arbitr.ru/Card/caeb1566-f034-4a31-806b-ca5c26301056 (дата обращения: 01.06.2024).

65. Постановление Пленума Верховного Суда РФ от 28.06.2012 № 17 «О рассмотрении судами гражданских дел по спорам о защите прав потребителей» // Солидарность. – 2013. – № 31.

66. Постановление Пленума ВАС РФ от 30.07.2013 № 62 «О некоторых вопросах возмещения убытков лицами, входящими в состав органов юридического лица» // Российская газета. – 2012. – № 156.

67. Апелляционное определение Санкт-Петербургского городского суда от 03.02.2015 № 33-1644/2015 по делу № 2-3097/2014. [Электронный ресурс]. Режим доступа: https://sankt-peterburgsky–spb.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=39162742&delo_id=5&new=5&text_number=1 (дата обращения: 01.06.2024).

68. Апелляционное определение Ленинградского Областного суда от 20.04.2016 № 33-2182/2016. [Электронный ресурс]. Режим доступа: https://oblsud.lo.sudrf.ru/modules.php?name=information, свободный (дата обращения: 01.06.2025).

69. Определение Судебной коллегии по гражданским делам Верховного Суда РФ от 01.08.2017 № 78-КГ17-45. [Электронный ресурс]. Режим доступа: https://vsrf.ru/lk/practice/stor_pdf/1570148 (дата обращения: 01.06.2024).

70. Апелляционное определение Верховного суда Республики Татарстан от 17.08.2017 по делу № 33–13279/2017. [Электронный ресурс]. Режим доступа: https://vs.tat.sudrf.ru/modules.php?name=information&irid=9, свободный (дата обращения: 01.06.2025).

71. Решение Черемушкинского районного суда города Москвы от 18.06.2019 по делу № 12-973/2019. [Электронный ресурс]. Режим доступа: https://mos-gorsud.ru/rs/cheryomushkinskij/cases/docs/content/e7b8a497-09c7-4d1d-a7f9- 5827f76d6a20 (дата обращения: 01.06.2024).

72. Постановление Второго арбитражного апелляционного суда от 08.08.2019 № 02АП.5517/2019 по делу № А31-3955/2019. [Электронный ресурс]. Режим доступа: https://kad.arbitr.ru/Kad/PdfDocument/973f0e30-b841-4f1b-bc4e-d717e5ac05f0/033676ef-2a40-4da5-abe9-172a21f899b7/A31-3955-2019_20190808_Postanovlenie_apelljacionnoj_instancii.pdf (дата обращения: 01.06.2024).

73. Постановление Конституционного Суда Российской Федерации от 13.01.2020 № 1-П «По делу о проверке конституционности частей 2 и 3 статьи 13, пункта 5 части 5 статьи 19 и части 1 статьи 20 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» в связи с жалобой гражданки Р.Д. Свечниковой» // Собрание законодательства РФ. – 2020. – № 3. – Ст. 275.

74. Определение Первого кассационного суда общей юрисдикции от 16.02.2022 по делу № 2-1106/2021 // СПС «КонсультантПлюс».

75. Постановление Конституционного Суда РФ от 13.07.2022 № 31-П «По делу о проверке конституционности пунктов 11 и 12 части 1 статьи 79 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» в связи с жалобой гражданки Ф.» // Российская газета. – 2022. – № 160.

76. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершённых с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» // Бюллетень Верховного Суда РФ. – 2023. – № 3.

77. Кассационное определение Третьего кассационного суда общей юрисдикции от 31.07.2024 по делу № 88–17092/2024. [Электронный ресурс]. Режим доступа: http://3kas.sudrf.ru/, свободный (дата обращения: 01.06.2025).

78. Определение Первого кассационного суда общей юрисдикции от 16.12.2021 № 88-28204/2021 по делу № 2-598/2021 // СПС «КонсультантПлюс».

II. Специальная юридическая литература

Книги, комментарии законодательства, учебники и учебные пособия:

79. Cloud computing Law, edited by Christopher Millard // Oxford University Press, 2013.

80. Абдулаев М.И. Теория государства и права: учеб. для выс. учеб. заведений. – М.: Магистр-Пресс, 2004.

81. Алексеев С.С. Общая теория права. Т. 1. – М., 1981.

82. Алексеев С.С. Общие дозволения и общие запреты в советском праве. – М.: Юрид. лит., 1989.

83. Алимов Э.В., Алимова Д.Р., Гаджиев Х.И. [и др.]. Защита данных: науч.-практ. комментарий к судебной практике / отв. ред. В.В. Лазарев, Х.И. Гаджиев. – М.: ИЗиСП, КОНТРАКТ, 2020.

84. Андриченко Л.В., Боголюбов С.А., Бондарь Н.С. [и др.]. Комментарий к Конституции Российской Федерации (постатейный) / под ред. В.Д. Зорькина. 2-е изд., пересмотр. – М.: Норма, Инфра-М, 2011.

85. Бачило И.Л. Информационное право: учеб. для вузов. – М.: Высшее образование, Юрайт-издат, 2009.

86. Бачило И.Л., Сергиенко Л.А., Кристальный Б.В., Арешев А.Г. Персональные данные в структуре информационных ресурсов. Основы правового регулирования. – Минск: Беллітфонд, 2006.

87. Бычков А.И. Категории персональных данных // СПС «КонсультантПлюс».

88. Венгеров А.Б. Теория государства и права: учебник. – 2-е изд. – М.: Омега-Л, 2005.

89. Витрук Н.В. Законность: понятие, защита и обеспечение // Общая теория права: курс лекций / под ред. В.К. Бабаева. – Нижний Новгород: Асгард, 1993.

90. Гаврилов Э.П. Комментарий к Закону «Об авторском праве и смежных правах». – М.: Былинина, 1996.

91. Гражданское право: в 4 т. Т. 1: Общая часть: учеб. для студентов вузов, обучающихся по направлению 521400 «Юриспруденция» и по специальности 021100 «Юриспруденция» / отв. ред. Е.А. Суханов. – 3-е изд., перераб и доп. – М.: Волтерс Клувер, 2006.

92. Гражданское право / под ред. Ю.К. Толстого, А.П. Сергеева. Ч. 1. – СПб., 1996.

93. Дьяконова М.О., Ефремов А.А., Зайцев О.А. [и др.]. Цифровая экономика: актуальные направления правового регулирования: науч.-практ. пособие / под ред. И.И. Кучерова, С.А. Синицына. – М.: ИЗиСП, НОРМА, 2022.

94. Жуйков В.М., Завриев С.С. Проблемы реализации принципов гражданского судопроизводства в правоприменительной деятельности: монография / В.М. Жуйков, С.С. Завриев. – М.: НОРМА, ИНФРА-М, 2024.

95. Зверева Е.А. Правовой режим информации в отношениях с участием субъектов предпринимательской деятельности: монография / Е.А. Зверева. – М.: Юстицинформ, 2008.

96. Информационно-технологическое обеспечение юридической деятельности (LegalTech): учебник / А.В. Минбалеев, Т.А. Полякова, М.Б. Добробаба и др. – М.: Проспект, 2022.

97. Иоффе О.С. Гражданско-правовая охрана интересов личности / под ред. Б.Б. Черепахина. – М.: Юридическая литература, 1969.

98. Камалова Г.Г. Искусственный интеллект для развития бизнеса и охрана персональных данных: правовые проблемы обеспечения баланса интересов // Право и бизнес: правовое пространство для развития бизнеса в России: коллективная монография: в 4 т. – М.: Проспект, 2020. – С. 122–130.

99. Комаров С.А. Общая теория государства и права: курс лекций. – М., 1996.

100. Копылов В.А. Информационное право: учебник. – 2-е изд., доп. – М.: Юристъ, 2002.

101. Красавчикова Л.О. Личная жизнь граждан под охраной закона. – М: Право, 1983.

102. Малеин Н.С. Охрана прав личности советским законодательством / отв. ред. А.И. Масляев. – М.: Наука, 1985.

103. Малюк А.А. Этика в сфере информационных технологий / А.А. Малюк, О.Ю. Полянская, И.Ю. Алексеева. – М.: Горячая линия-Телеком, 2011.

104. Матузов Н.И. Правовая система и личность. – Саратов: Изд-во Сарат. ун-та, 1987.

105. Минбалеев А.В. Проблемы цифрового права: учеб. пособие. – Саратов: Амирит, 2022.

106. Мордовец А.С. Социально-юридический механизм обеспечения прав человека и гражданина. – Саратов, 1996.

107. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка.: 72 500 слов и 7500 фразеологических выражений; Российская АН, Ин-т рус. яз., Российский фонд культуры. – 2-е изд., испр. и доп. – М.: Азъ, 1994.

108. Организационно-правовые основы защиты персональных данных: учеб. пособие / подготов. А.В. Гортинским. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1716999221&tld=ru&lang=ru&name=621.pdf&text=Организационно-правовые+основы+защиты+персональных+данных»+–+учебное+пособие%2C+подготовленное+А.+В.+Гортинским&url=http%3A//elibrary.sgu.ru/uch_lit/621.pdf&lr=43&mime=pdf&l10n=ru&sign=2832c9ed0ec3f296b88544a3601d6483&keyno=0, свободный (дата обращения: 01.06.2025).

109. Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика: монография. – М.: Статут, 2011.

110. Право и иные регуляторы в развитии цифровых технологий: монография / А.В. Минбалеев, А.В. Мартынов, Г.Г. Камалова [и др.]; Институт государства и права Российской академии наук. – М.; Саратов: Амирит, 2022.

111. Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций: коллективная монография: в 2 т. / Е.Н. Абанина, О.Ю. Авдевнина, Р.В. Амелин и др. – Саратов: Саратов. гос. юрид. академия, 2020.

112. Рассолов И.М. Теоретические проблемы интернет-права. – М., 2002.

113. Рассолов М.М. Информационное право. – М.: Юристъ, 1999.

114. Романовский Г.Б. Право на неприкосновенность частной жизни. – М.: М3-Пресс, 2001.

115. Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». – 2-е изд., перераб. и доп. – М.: Статут, 2021.

116. Савельев А.И. Электронная коммерция в России и за рубежом: правовое регулирование: монография. – М.: Статут, 2016.

117. Словарь иностранных слов, вошедших в состав русского языка: Материалы для лексической разработки заимствованных слов в рус. лит. речи: С портр. и краткой биогр. А.Н. Чудинова / сост. под ред. А.Н. Чудинова. – 3-е изд., тщательно испр. и знач. доп. (более 5000 новых слов) преимущественно соц.-полит. терминами, вошедшими в жизнь в последние годы. – СПб., 1910.

118. Стоякин Г.Н. Понятие «защита гражданских прав» // Проблемы гражданско-правовой ответственности и защиты гражданских прав. – Свердловск: Госиздат, 1973.

119. Тарасова В.А. Охрана прав граждан в пенсионном обеспечении. – М.: Практика, 1978.

120. Тедеев А.А. Информационное право. – М.: Эксмо, 2006.

121. Толковый словарь русского языка. Современная версия / В.И. Даль. – М.: Эксмо, 2004.

122. Толковый словарь русского языка: т. 1–4 / сост. Г.О. Винокур, Б.А. Ларин, С.И. Ожегов [и др.]; под ред. Д.Н. Ушакова. – М.: Гос. ин-т «Советская энциклопедия», 1935.

123. Черданцев А.Ф. Теория государства и права: учеб. для вузов. – М.: Юрайт-М, 1999.

124. Шафиров В.М. Обеспечение права: человекоцентристский подход: монография / В. Шафиров. – М., 2015.

125. Явич Л.С. Общая теория права. – Л.: Изд-во Ленинград. ун-та, 1976.

Статьи и иные публикации:

126. Артамонова Е.А. О производстве следственных действий в свете требований статьи 9 УПК РФ // Нравственные начала в уголовном процессе: сб. статей по материалам Всероссийского круглого стола / под общ. ред. К.Б. Калиновского, Л.А. Зашляпина. – СПб., 2021.

127. Архипов В.В. Виртуальное право: основные проблемы нового направления юридических исследований // Известия высших учебных заведений. Правоведение. – 2013. – № 2 (307).

128. Афанасьев С.Д., Терещенко И.А., Яцкевич Д.А. Биометрическая идентификация и права человека: демаркационная линия // Закон. – 2022. – № 3.

129. Батурин Ю.М. Информационно-технологический вызов человечеству // Наука и техника: Вопросы истории и теории: материалы XLII Международной годичной научной конференции Санкт-Петербургского отделения Российского национального комитета по истории и философии науки и техники Российской академии наук, Санкт-Петербург, 25–29 октября 2021 г. – СПб.: Санкт-Петербургский филиал федерального государственного бюджетного учреждения науки «Институт истории естествознания и техники им. С.И. Вавилова РАН», 2021.

130. Бачило И.Л. Важный шаг в регулировании информационных прав граждан: К принятию ФЗ «О персональных данных» // Законы России. – 2006. – № 11.

131. Бембеева Б.С. Право на защиту персональных данных и различные категории персональных данных / Б.С. Бембеева // Право в сфере Интернета: сб. статей / отв. ред. М.А. Рожкова. – М.: Статут, 2018. – EDN VNLNWS. [Электронный ресурс]. Режим доступа: https://www.elibrary.ru/download/elibrary_36521757_34882333.pdf, свободный (дата обращения: 01.06.2025).

132. Бережной А. Облачные вычисления: Новое или хорошо забытое старое? // Системный администратор, спецвыпуск «Облачные вычисления». – 2011. – Март.

133. Боброва Н.А. Гарантии реализации государственно-правовых норм // Закон. – 1984.

134. Бобров К. О разграничении понятий «правовая охрана» и «правовая защита» человека // Закон и право. – 2008. – № 8.

135. Бочкарев А.Е. Распределение бремени доказывания в гражданском процессе по спорам о качестве медицинских услуг // Медицинское право. – 2017. – № 6. – С. 5–9.

136. Бояринцева О.А. Актуальные вопросы правового регулирования баз данных в условиях цифровой трансформации государственного управления // Аграрное и земельное право. – 2020. – № 7 (187).

137. Букалерова Л.А., Лапшин В.Ф., Остроушко А.В. Риск-ориентированный подход в области правового регулирования обеспечения информационной безопасности несовершеннолетних // Вестник Сургутского государственного университета. – 2021. – № 1.

138. Бундин М.В. К вопросу о содержании персональных данных // Информационное право. – 2019. – № 4.

139. Бундин М.В. Опыт правового регулирования права на частную жизнь и персональных данных в Соединенных Штатах Америки // Журнал зарубежного законодательства и сравнительного правоведения. – 2012. – № 3 (34).

140. Варлен М.В. Информационный, технологический, экономический и финансовый суверенитет как новейшие типы автономности // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2023. – № 9 (109).

141. Викторова Н.Г. Цифровая экономика: развитие облачных технологий в России и за рубежом / Н.Г. Викторова, Ф.Г. Шухов // Век качества. – 2019. – № 2.

142. Волкова А.Ю. Персональные данные как объект уголовно-правовой охраны // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3.

143. Волова А.А. Соотношение понятий «правовая охрана» и «правовая защита» // Молодой учёный. – 2023. – № 43 (490).

144. Воронков Н.А. Определение персональных данных // Молодой учёный. – 2022. – № 27 (422).

145. Вуколова Т. Законодательство о персональных данных в Германии и России. Сравнительно-правовое исследование // ИС. Авторское право и смежные права. – 2016. – № 4.

146. Дмитрик Н.А. История, смысл и перспективы института персональных данных // Вестник гражданского права. – 2020. – Т. 20. – № 3.

147. Добробаба М.Б. Понятие персональных данных: проблема правовой определённости // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2023. – № 2.

148. Добробаба М.Б. Правовое обеспечение защиты персональных данных при использовании технологий искусственного интеллекта // Информационное право. – 2023. – № 3 (77).

149. Долинская В.В. Защита прав в сфере персональных данных в России и ЕС // Законы России: опыт, анализ, практика. – 2019. – № 9.

150. Донских А.Г. Актуальные проблемы использования персональных данных в деятельности СМИ // Вестник НГУ. Серия: История, филология. – 2021. – № 6. – Т. 20: Журналистика. – С. 150.

151. Ефремов А.А. Государственный суверенитет в условиях цифровой трансформации // Правоведение. – 2019. – Т. 63. – № 1.

152. Жарова А.К. Опыт правового обеспечения безопасности персональных данных (на примере Аргентины и Великобритании) // Информационное право. – 2017. – № 4.

153. Жеребцов А.Н., Малышев Е.А. Применение цифровых технологий в процессе публичного управления миграционными процессами в Российской Федерации // Lex Russica (Русский закон). – 2023. – Т. 76. – № 12 (205).

154. Зубарев С.М. К вопросу о сущности контрольных процедур в государственном управлении // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2016. – № 5 (21).

155. Зюбанов К.А. Распространение сведений о гражданине, распространение персональных данных. [Электронный ресурс]. Режим доступа: https://pravo.hse.ru/digitalperson/dissemination, свободный (дата обращения: 01.06.2025).

156. Изотов Н.Н. Взаимосвязь «защиты» и «охраны» интеллектуальной собственности // Юриспруденция. – 2005. – № 8.

157. Исакова Л.В., Статуева К.Е. Международно-правовое регулирование защиты персональных данных работников // Новый университет. Серия: Экономика и право. – 2015. – № 4 (50).

158. Казакевич Е.И., Губин Е.П. Защита прав и свобод человека при обработке персональных данных в период цифровой трансформации // Уральский журнал правовых исследований. – 2022. – № 4 (21).

159. Камалова Г.Г. Искусственный интеллект для развития бизнеса и охрана персональных данных: правовые проблемы обеспечения баланса интересов // Право и бизнес: правовое пространство для развития бизнеса в России: коллективная монография: в 4 т. – М.: Проспект, 2020.

160. Канашевский В.А. Юридические проблемы использования российскими банками облачных услуг зарубежных провайдеров // Lex Russica (Русский закон). – 2019. – № 3 (148).

161. Кириллова Е.А. Правовой статус и принципы использования технологии больших данных (Big Data) // Российская юстиция. – 2021. – № 2.

162. Ковалев С. Д. Актуальные проблемы правового регулирования оборота и защиты персональных данных в России в цифровую эпоху // Вестник Владимирского юридического института. – 2022. – № 4(65).

163. Комиссарова Е.Г. Формально-логические аспекты понятия «правовая природа» // Вестник Пермского университета. Юридические науки. – 2012. – № 2 (16).

164. Кропачев Н.М., Архипов В.В. Традиционные духовно-нравственные ценности в контексте цифровой трансформации общества: теоретико-правовые аспекты // Вестник Санкт-Петербургского университета. Право. – 2023. – Т. 14. – № 2.

165. Крюков Д.Ю., Мокрецов Ю.В. Актуальные проблемы правового регулирования оборота и защиты персональных данных в России // Вестник института: преступление, наказание, исправление. – 2017. – № 2 (38).

166. Кудашкин Я.В. Особенности правовой природы и классификации персональных данных в России // Право и государство: теория и практика. – 2018. – № 1 (157).

167. Латыпов Д.Н. Соотношение охраны и защиты гражданских прав // Актуальные проблемы российского права. – 2009. – № 1.

168. Лескина Э.И. Доктринальные аспекты правовых режимов данных в условиях развития технологий больших данных // Журнал российского права. – 2024. – Т. 28. – № 7. – С. 122–136. [Электронный ресурс]. Режим доступа: https://jrp.jes.su/s1605-65900000622-5-1-ru-230/, свободный (дата обращения: 11.11.2025).

169. Лескина Э.И. Понятие и объект оборота данных // Законодательство. – 2025. – № 3. – С. 42–49.

170. Литвин И.И. Особенности сбора, обработки и защиты персональных данных искусственным интеллектом // Вестник Уральского юридического института МВД России. – 2021. – № 4.

171. Лушников А.М. Защита персональных данных работника: сравнительно-правовой комментарий гл. 14 Трудового кодекса РФ // Трудовое право. – 2009. – № 9.

172. Мордовец А.С. Социально-юридический механизм обеспечения прав человека и гражданина. – Саратов, 1996.

173. Мартынов А.В., Бундин М.В. О правовых принципах применения искусственного интеллекта при осуществлении органами исполнительной власти контрольно-надзорной деятельности // Журнал российского права. – 2020. – № 10.

174. Минбалеев А.В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 2 (4).

175. Минбалеев А.В., Филоненкова В.А. Проблемы защиты персональных данных и цифрового профиля человека в сети «Интернет» в условиях пандемии // Вестник ЮУрГУ. Серия: Право. – 2020. – № 3. – Т. 20.

176. Минбалеев А.В. Формирование экономики данных в России в условиях многополярного мира: проблемы правового обеспечения // Экономика и управление. – 2023. – Т. 29. – № 8.

177. Мираев А.Г. Понятие персональных данных в Российской Федерации и Европейском союзе // Юридическая наука. – 2019. – № 5.

178. Михайлова И.А. Персональные данные и их правовая охрана: некоторые проблемы теории и практики // Законы России: опыт, анализ, практика. – 2017. – № 10.

179. Наумов В.Б., Архипов В.В. Понятие персональных данных: интерпретация в условиях развития информационно-телекоммуникационных технологий // Российский юридический журнал. – 2016. – № 2.

180. Никитченко А.А. Теоретико-правовые аспекты соотношения понятий «охрана» и «защита» результатов интеллектуальной деятельности // Вестник ТОГУ. – 2012. – № 1 (24).

181. Петрыкина Н.И. К вопросу о конфиденциальности персональных данных // Законы России: опыт, анализ, практика. – 2007. – № 6.

182. Полякова Т.А., Камалова Г.Г. Ценностные изменения развития информационного права России // Правовое государство: теория и практика. – 2023. – № 2 (72).

183. Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. – 2020. – № 5.

184. Попова А.В. К вопросу о регламентации и содержании системы правовых принципов взаимодействия человека с искусственным интеллектом, роботами и объектами робототехники // Правовое государство: теория и практика. – 2020. – № 4-1 (62).

185. Пороховская Т.И. Концепт приватности: нормативное содержание в сфере межличностных отношений // Учёные записки Крымского федерального университета имени В.И. Вернадского. Социология. Педагогика. Психология. – 2014. – № 1.

186. Рассолов И.М., Чубукова С.Г., Микурова И.В. Анализ возможного применения к регулированию отношений по поводу генетической информации институтов персональных данных, личной тайны, врачебной тайны // Lex russica (Русский закон). – 2020. – № 4.

187. Ростовщиков И.В. Права личности в России: их обеспечение и защита органами внутренних дел / И.В. Ростовщиков; науч. ред. Н.В. Витрук. Волгоград: ВЮИ, 1997.

188. Савельев А.И. На пути к концепции регулирования данных в условиях цифровой экономики // Закон. – 2019. – № 4.

189. Самович Ю.В. О понятии правовая защита // МИТС-Наука: международный научный вестник: сетевое электронное научное издание. – 2006. – № 1.

190. Санникова Л.В., Харитонова Ю.С. Цифровые активы как объекты предпринимательского оборота // Право и экономика. – 2018. – № 4.

191. Сатикова Д.М. Обработка персональных данных с использованием облачных сервисов // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. – 2018. – № 4.

192. Сербин Д.С. Право на приватность в концепции Сэмюэла Уоррена и Луиса Брандейса // Взаимодействие институтов власти и общества в сфере защиты прав человека: материалы VIII международной научно-практической конференции аспирантов, преподавателей, практических работников, Саратов, 1–2 июля 2015 года. – Саратов: Саратовский источник, 2015.

193. Сергиенко Л.А. Правовая защита персональных данных. Цели и принципы правового регулирования // Проблемы информатизации. – 1995. – № 1.

194. Смирнов А.П. Соотношение понятий «охрана прав» и «защита прав» // Вестн. Том. гос. ун-та. – 2010. – № 331.

195. Стремоухов А.В. Право человека на защиту и формы его защиты в Российской Федерации // Ленинградский юридический журнал. – 2017. – № 1 (47).

196. Талапина Э.В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права РАН. – 2018. – Т. 13. – № 5.

197. Талапина Э.В. Эволюция прав человека в цифровую эпоху // Труды Института государства и права РАН. – 2019. – № 3. – Т. 14.

198. Терещенко Л.К. Государственный контроль в сфере защиты персональных данных // Право: журнал Высшей школы экономики. – 2018. – № 4.

199. Тимофеев И.В. Цифровая информатизация и информационная безопасность в современном здравоохранении: конституционно-правовой подход к проблеме // Конституционное и муниципальное право. – 2019. – № 12.

200. Уоррен С., Брендейс Л.Д. Право на приватность. [Электронный ресурс]. Режим доступа: http://rus.triz–guide.com/1662.html, свободный (дата обращения: 01.06.2025).

201. Фаизова А.Г. Правовые риски защиты персональных данных лиц, использующих облачные сервисы, и пути их минимизации // Молодой учёный. – 2023. – № 27 (474).

202. Хабриева Т.Я., Капустин А.Я., Габов А.В., Черногор Н.Н. Конфликт интересов: природа, предупреждение, социальное регулирование // Журнал зарубежного законодательства и сравнительного правоведения. – 2018. – № 3 (70).

203. Холодная Е.В. О государственном контроле/надзоре за деятельностью операторов персональных данных // Актуальные вопросы теории и практики реализации публичной власти: сб. науч. трудов по материалам IV Ежегодных Саратовских административно-правовых чтений, Саратов, 11–12 октября 2018 года / Саратовская государственная юридическая академия. – Саратов: ИП Коваль Юлия Владимировна, 2018.

204. Хохлова Е.В. Об охране персональных данных уголовным законом // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3.

205. Цареградская Ю.К. Криптовалюта, цифровые финансовые активы, цифровые права: терминологическое многообразие в процессе формирования правовой действительности // Право и цифровая экономика. – 2021. – № 2 (12).

206. Чаннов С.Е. Некоторые вопросы анализа цифровых профилей государственных и муниципальных служащих в целях противодействия коррупции // Кадровик. – 2025. – № 6.

207. Чеботарева А.А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе. [Электронный ресурс]. Режим доступа: http://igpran.ru/prepare/a.persons/ChebotarevaAA/Chebotareva_avtoref.pdf (дата обращения: 11.11.2025).

208. Шайхеев Т.И. Правовые позиции судов по экономическим спорам в примерах из судебной практики // Арбитражные споры. – 2022. – № 3.

209. Шумилин А.С. Метод обеспечения защиты персональных данных в медицинской облачной системе // Вопросы кибербезопасности. – 2023. – № 4 (56).

210. Щетинина А.Б. Проблема ответственности за нарушение законодательства Российской Федерации в области персональных данных // Вопросы устойчивого развития общества. – 2022. – № 6.

Диссертации и авторефераты:

211. Бикбулатова Ю.С. Информационно-правовое регулирование отношений, формирующихся при использовании облачных вычислений (сервисно-ориентированных распределённых информационных систем): дис. ... канд. юрид. наук. – М., 2018.

212. Бундин М.В. Персональные данные в системе информации ограниченного доступа: дис. ... канд. юрид. наук. – М., 2017.

213. Джафарова Н.И. Административная ответственность за правонарушения в области оборота информации: дис. … канд. юрид. наук. – М., 2021.

214. Ефремова М.А. Уголовно-правовая охрана информационной безопасности: дис. ... докт. юрид. наук. – М., 2017.

215. Игумнов В.В. Публично-правовое регулирование цифрового профилирования в Российской Федерации: дис. … канд. юрид. наук. – М., 2024.

216. Коженинков С. Н. Меры защиты в советском праве: автореф. дис. … канд. юрид. наук. – Свердловск, 1968.

217. Кораблев А.В. Идентификация информационных рисков использования облачных технологий в банковской деятельности: дис. … канд. экон. наук. – Самара, 2017.

218. Лазаров А.А. Информационно-правовое регулирование социального кредитования (скоринга): дис. … канд. юрид. наук. – М., 2023.

219. Соловкин С.В. Публично-правовое регулирование процессов автоматизированного сбора данных о человеке в условиях цифровой трансформации: дис. ... канд. юрид. наук. – Москва, 2024.

220. Федосин А.А. Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации: дис. … канд. юрид. наук. – Саранск, 2009.

Интернет-источники на русском языке:

221. Доклад Президента Российской Федерации В.В. Путина 20 мая 2022 г. на заседании Совета Безопасности Российской Федерации «О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства». [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1716999516&tld=ru&lang=ru&name=988fe6c43f2b5e1e8142e33d505d.pdf&text=Доклад+Президента+Российской+Федерации+В.В.+Путина+20+мая+2022+г.+на+заседании+Совета+Безопасности+Российской+Федерации+»О+повышении+устойчивости+и+безопасности+функционирования+информационной+инфраструктуры+государства»&url=http%3A//uc-pps.ru/files/ckeditor/8f/ef/988fe6c43f2b5e1e8142e33d505d.pdf&lr=43&mime=pdf&l10n=ru&sign=c863d62cd3c68f98a91533e4dfbbc90d&keyno=0, свободный (дата обращения: 01.06.2025).

222. Жорина А.В. Соотношение понятий «охрана» и «защита авторских прав». [Электронный ресурс]. Режим доступа:

https://sibadvokat.ru/statiy/sootnoshenie-ponyatiy-ohrana-i-zashhita-avtorskih-prav?ysclid=lw29obb85r101925365, свободный (дата обращения: 01.06.2025).

223. Журкина О.В. Нормы международного права и их влияние на национальное законодательство в вопросе о соотношении понятий «защита» и «охрана» // Matters of Russian and International Law. [Электронный ресурс]. Режим доступа: http://www.publishing-vak.ru/file/archive-law-2013-9/6-zhurkina.pdf, свободный (дата обращения: 01.06.2025).

224. Зоркольцев Р.Д. Персональные данные, получаемые через Интернет: практические вопросы. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1717183117&tld=ru&lang=ru&name=Zorkolcev.pdf&text=Зоркольцев цев+Р.Д.+Персональные+данные%2C+получаемые+через+Интернет%3A+практические+вопросы&url=http%3A//planeta51.ru/content/files/Zashita/Zorkolcev.pdf&lr=43&mime=pdf&l10n=ru&sign=b9bc79c3a832a11d3d51b3456ffca52f&keyno=0, свободный (дата обращения: 01.06.2025).

225. Информационная аналитика в издании The Economist. [Электронный ресурс]. Режим доступа: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data, свободный (дата обращения: 01.06.2025).

226. Информация с сайта СПС «Гарант». [Электронный ресурс]. Режим доступа: https://www.garant.ru/news/1364613/, свободный (дата обращения: 01.06.2025).

227. Исследование облачной зрелости российского бизнеса 2023 // Cloud и «Технологии доверия», 2022. [Электронный ресурс]. Режим доступа: https://docviewer.yandex.ru/?tm=1717182167&tld=ru&lang=ru&name=tedo-cloud-event.pdf&text=Исследование+облачной+зрелости+российского+бизнеса+2023+//+Cloud+и+»Технологии+доверия»%2C+2022&url=https%3A//data.tedo.ru/technology/tedo-cloud-event.pdf&lr=43&mime=pdf&l10n=ru&sign=f971079df43aabe71075452fd7820e6f&keyno=0, свободный (дата обращения: 01.06.2025).

228. Использование больших данных в финансовом секторе и риски финансовой стабильности: доклад для общественных консультаций. Банк России. [Электронный ресурс]. Режим доступа: https://www.cbr.ru/Content/Document/File/131359/Consultation_Paper_10122021.pdf (дата обращения: 16.03.2025).

229. Кодекс этики в сфере ИИ. [Электронный ресурс]. Режим доступа: https://ethics.a-ai.ru/assets/ethics_files/2023/05/12/Кодекс_этики_20_10_1.pdf (дата обращения: 11.04.2025).

230. Концепция комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики. [Электронный ресурс]. Режим доступа: https://%D0%9E%D1%82%D1%87%D0%B5%D1%82_%D0%98%D0%A2%D0%9E%D0%93_3_%D1%8D%D1%82%D0%B0%D0%BF%20(1).pdf/, свободный (дата обращения: 01.06.2025).

231. Матвеева Т. Выступление на Петербургском Международном юридическом форуме. Информация с сайта СПС «Гарант». [Электронный ресурс]. Режим доступа: https://www.garant.ru/news/1464529/?ysclid=ltx7wq8o8o183188278/, свободный (дата обращения: 01.06.2025).

232. Обзор Федерального закона о проведении в Москве эксперимента в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта. [Электронный ресурс]. Режим доступа: https://zakon.ru/blog/2020/06/10/obzor_federalnogo_zakona_o_provedenii_v_moskve_eksperimenta_v_celyah_sozdaniya_neobhodimyh_uslovij_d?ysclid=ltu6zlfbfy656981848, свободный (дата обращения: 01.06.2025).

233. Ответ Минцифры РФ по провайдерам хостинга от 10.10.2023 № П25–22415ОГ. [Электронный ресурс]. Режим доступа: https://t.me/privacyexpert/1393 (дата обращения: 01.06.2025).

234. Ответ Роскомнадзора от 02.04.2012 № 01111907234. [Электронный ресурс]. Режим доступа: https://rppa.ru/_media/analitika/01shr-07432_02.04.2012.pdf, свободный (дата обращения: 01.06.2025).

235. Отчет «Интернет в России в 2022–2023 годах: состояние, тенденции и перспективы развития». [Электронный ресурс]. Режим доступа: https://raec.ru/live/analytics/14235/ (дата обращения: 01.06.2025).

236. Проект федерального закона № 950900-7 «О внесении изменения в статью 8 Федерального закона «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных». [Электронный ресурс]. Режим доступа: https://sozd.duma.gov.ru/bill/950900-7?ysclid=ltu979in6z178864765, свободный (дата обращения: 01.06.2025).

237. Разъяснения Прокуратуры Акбулакского района. [Электронный ресурс]. Режим доступа: https://xn--80aafb8bpdbc2g.xn--p1ai/2021/11/3308/, свободный (дата обращения: 01.06.2025).

238. Садовников Д. Обзор закона КНР о защите персональной информации (Personal Information Protection Law of the People’s Republic of China (PIPL)). [Электронный ресурс]. Режим доступа: https://zakon.ru/blog/2021/9/17/obzor_zakona_knr_o_zaschite_personalnoj_informaciipersonal_information_protection_law_of_the_peoples (дата обращения: 02.11.2023).

239. Словарь русских синонимов. [Электронный ресурс]. Режим доступа: https://sinonim.org/, свободный (дата обращения: 01.06.2025).

240. Справочная информация, размещенная в справочной системе «Интернет». [Электронный ресурс]. Режим доступа: https://t.me/privacyexpert/1100, свободный (дата обращения: 01.06.2025).

241. Статистика Роскомнадзора по утечкам данных // РБК. 23.02.2024. [Электронный ресурс]. Режим доступа: https://www.rbc.ru/rbcfreenews/65d7ef3d9a7947d8608dbbb3 (дата обращения: 01.06.2025).

242. Статья Бена Лорика о методах анонимизации данных. [Электронный ресурс]. Режим доступа:

https://www.wipo.int/tech_trends/ru/artificial_intelligence/ask_the_experts/techtrends_ai_lorica.html, свободный (дата обращения: 01.06.2025).

243. Урошлева А. Коммерциализация персональных данных и понятие «биг дата» – злободневные вопросы IT-сферы // Информационно-правовой портал ГАРАНТ.РУ. [Электронный ресурс]. Режим доступа: https://www.garant.ru/article/1229761/ (дата обращения: 01.12.2025).

244. Утечки информации из облака возросли в два раза. [Электронный ресурс]. Режим доступа: https://securenews.ru/utechci-informatsii-vozrosli/ (дата обращения: 01.06.2025).

245. Шитов А. Интервью на круглом столе конференции OS DAY 23.06.2023. Информация с сайта РИА Новости. [Электронный ресурс]. Режим доступа: https://ria.ru/20230628/zakon-1880810358.html, свободный (дата обращения: 01.06.2025).

246. Шубина Т.Б. Теоретические проблемы защиты права: автореф. дис. … канд. юрид. наук. – Самара, 1997.

Интернет-источники на иностранных языках:

247. Доклад «Consumer Data Rights and Competition – Background note». [Электронный ресурс]. Режим доступа: https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf, свободный (дата обращения: 01.06.2025).

248. Информация о статусе Конвенции о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. с официального интернет-сайта Совета Европы. URL: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108 (дата обращения: 20.05.2025).

249. Структура обеспечения приватности Азиатско-Тихоокеанского экономического сотрудничества. [Электронный ресурс]. Режим доступа: https://www.apec.org/docs/default-source/press/newsrelease/2005/04_amm_014rev1.pdf (дата обращения: 02.05.2025).

250. Artificial Intelligence Act: MEPs adopt landmark law. URL: https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law (дата обращения: 16.03.2025).

251. Bozeman B. Public Values and Public Interest: Counterbalancing Economic Individualism. Washington, D.C.: Georgetown University Press., 2007. 224 p. data // Cambridge Dictionary. URL: https://dictionary.cambridge.org/dictionary/english/data (дата обращения: 14.12.2025).

252. Eustice J.C. Flying into the cloud without falling: understanding the intersection between data privacy law and cloud computing solutions. URL: https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-andcloud-computing (дата обращения: 01.06.2025).

253. Gellert R. Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies // International Data Privacy Law. – 2021. – Vol. 11. – № 2.

254. Guryanova A., Astafeva N., Filatova N., Khafiyatullina E., Guryanov N. Philosophical View on Human Existence in the World of Technic and Information // The Impact of Information on Modern Humans / Advances in Intelligent Systems and Computing. – Vol. 622. – Springer, Cham, 2018.

255. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic cash system. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 08.07.2025).

256. Opinion 4/2007 on the Concept of Personal Data. WP 136, 20 June 2007. Article 29 Data Protection Working Party. P. 16–18. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, свободный (дата обращения: 01.06.2025).

257. PIPEDA in brief. URL: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/ (дата обращения: 02.05.2024).

258. Purtova N. The law of everything. Broad concept of personal data and future of EU data protection law // Law, Innovation and Technology. – 2018. – Vol. 10. – № 1.

259. Schwartz P.M. The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures // Harvard Law Review. – 2013. – Vol. 126. – № 7.

260. Solove D.J. Introduction: Privacy Self-Management and the Consent Dilemma // Harvard Law Review. – 2013. – Vol. 126. – № 7.

261. Solove D.J. The Myth of the Privacy Paradox // George Washington Law Review. – 2020. – Vol. 89. – № 1.

262. The economic potential of generative AI: The next productivity frontier. [Электронный ресурс]. Режим доступа: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#key-insights, свободный (дата обращения: 01.06.2025).

263. Wachter S., Mittelstadt B. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI // Columbia Business Law Review. – 2019. – Vol. 2019. – Issue 2.

264. Zuboff S. Big other: Surveillance Capitalism and the Prospects of an Information Civilization // Journal of Information Technology. – 2015. – Vol. 30. – № 1.

Приложение

Схема № 1. Логическая схема понятия «передача персональных данных»



Схема № 2. Предлагаемая логическая схема понятия (исключая понятие «передача»)

