

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

На правах рукописи

Ильюшина Инна Сергеевна

**ПРАВОВОЕ РЕГУЛИРОВАНИЕ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ
В ВИРТУАЛЬНОЙ СРЕДЕ ОРГАНИЗАЦИЙ**

Специальность: 5.1.2 Публично – правовые (государственно – правовые) науки

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата юридических наук

Москва – 2025

Диссертация подготовлена на кафедре правовой информатики, информационного и цифрового права юридического факультета МГУ имени М.В. Ломоносова

Научный руководитель – *Северин Виталий Андреевич,*
доктор юридических наук, доцент

Официальные оппоненты *Минбалеев Алексей Владимирович,*
доктор юридических наук, профессор,
ФГАОУ ВО «Московский государственный
юридический университет имени О.Е.
Кутафина (МГЮА)», кафедра
информационного права и цифровых
технологий, заведующий кафедрой;
Черкасов Константин Валерьевич,
доктор юридических наук, доцент,
ФГБОУ ВО «Всероссийский
государственный университет юстиции
(РПА Минюста России), кафедра
административного, финансового и
информационного права, профессор;
Савченко Елена Алексеевна,
кандидат юридических наук, ФГНИУ
Институт законодательства и
сравнительного правоведения при
Правительстве Российской Федерации,
отдел социального законодательства,
научный сотрудник.

Защита диссертации состоится «27» марта 2025г. в 15 часов 30 минут на заседании диссертационного совета МГУ.051.4 Московского государственного университета имени М. В. Ломоносова по адресу: Москва, Ленинские горы, д.1, стр.13-14, 4-й учебный корпус, Юридический факультет, ауд. 536а.

E-mail: dissovet@law.msu.ru.

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М. В. Ломоносова (Ломоносовский просп., д. 27) и на портале: <https://dissovet.msu.ru/dissertation/3348>.

Автореферат разослан «___» февраля 2025 г.

Ученый секретарь
диссертационного совета,
кандидат юридических наук

Н.С. Малютин

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Использование информационных и коммуникационных технологий порождает создание и оборот информации в цифровом формате, которая обладает новыми, более совершенными свойствами - способностью к мгновенному распространению и неограниченному масштабированию, а также ранее неизвестную среду ее существования – виртуальную, ставшую уже привычным и естественным жизненным пространством, в котором непрерывно происходит обмен данными, онлайн взаимодействие и т.п. Так, в Стратегии развития информационного общества в Российской Федерации 2017 – 2030 годы¹ (далее по тексту – Стратегия) отдельно отмечено, что «информационные и коммуникационные технологии оказывают существенное влияние на развитие традиционных отраслей экономики» и уже «стали частью современных управленческих систем во всех отраслях экономики». «Значительное увеличение объема данных, источниками и средствами распространения которых являются промышленные и социальные объекты, различные электронные устройства, приводит к формированию новых технологий, а их повсеместное применение способствует развитию нового этапа экономики - цифровой экономики и образованию ее экосистемы». В этой связи план реализации Стратегии включает в себя «совершенствование законодательства Российской Федерации, административных процедур (в том числе в электронной форме) и бизнес-процессов коммерческих организаций, а также создание благоприятных условий для применения информационных и коммуникационных технологий». Одновременно с этим «обеспечение баланса между своевременным внедрением современных технологий обработки данных и защитой прав граждан, включая право на личную и семейную тайну», поименовано в Стратегии в качестве одной из национальных целей развития Российской Федерации. Именно поэтому теоретические познания и выводы в области правового регулирования и защиты персональных данных нуждаются в адаптации к современным реалиям, поскольку

¹ СЗ РФ. 15.05.2017. № 20. Ст. 2901.

основополагающие права человека в области неприкосновенности частной жизни должны не только «научиться» существовать в новой среде – виртуальной, но и получить адекватную вызовам защиту, в связи с чем возникла объективная необходимость на базе уже имеющихся теоретических установлений разработать концепцию правового регулирования и защиты персональных данных именно в виртуальной среде организаций с учетом не только правовых, но и технических аспектов.

В отличие от реальной среды существования, где любое присутствие осязаемо, а информация материально зафиксирована, виртуальная среда организации представляет собой определенное информационное пространство, где за счет функционирования интегрированной системы, в которую входят аппаратные средства (оборудование) и программное обеспечение, совместно работающие для выполнения заранее определенных задач, а также различных коммуникационных сервисов, сопутствующих деловой активности, происходит создание, фиксация, использование и хранение информации, в том числе и персональных данных, в цифровом формате. При этом виртуальная среда организаций обладает индивидуальными признаками и по своей природе является динамичной, поскольку создается в каждом отдельном хозяйствующем субъекте с учетом объективных потребностей с возможностью внедрения и использования новых информационно-коммуникационных технологий, программного обеспечения, аппаратной части и т.п. В этой связи формирование основ правоотношений, а также юридическая регламентация создания и функционирования виртуальной среды организации осуществляются посредством организационно-правовых мер на уровне локального нормотворчества.

Характерной особенностью современных реалий в части технической (аппаратной) составляющей виртуальной среды организаций является повсеместное использование в данном информационном пространстве персональных компьютерных устройств сотрудников, смартфонов, планшетов и иных гаджетов, что является результатом широкого технического оснащения трудовых масс, а также интеграции технологических решений в производственный

процесс. Так, зачастую различная информация персонального характера, генерируемая в процессе деловой активности, например видеозаписи совещаний, голосовые и письменные сообщения, электронные письма, фотоизображения и т.п. информация в цифровом формате, используемая сотрудниками в процессе трудовой деятельности, хранится на их личных электронных устройствах за периметром корпоративной информационной среды организации, что значительно снижает уровень защиты, поскольку цифровой формат допускает не только визуальное обозрение, но и неограниченную передачу, масштабирование и иное отображение, а также расширяет круг лиц, получающих в связи с использованием технологических решений доступ к информации конфиденциального характера. Одновременно с этим, в отличие от еще недавнего времени, когда только строго определенные сотрудники хозяйствующей структуры могли получить доступ к информации конфиденциального характера, в том числе и персональным данным, и это никак не отражалось на экономическом результате и не тормозило целевую деятельность, современные реалии характеризуются все большим, если не сказать что практически полным вовлечением сотрудников в использование и хранение вышеуказанной информации за счет коллаборации производственных задач, необходимости сокращения времени от момента принятия решения до его реализации, использования в производственном процессе личных компьютерных средств и т.п.

Все эти необратимые и перманентно усложняющиеся отношения существенно снижают уровень защищенности информации и ее безопасности на фоне подчас невозможности для организации осуществления контрольных функций. При этом для операторов персональных данных настоящая действительность связана с увеличением обязанностей и более высокой ответственностью по сравнению с еще недавним прошлым, когда законодательные требования полностью соответствовали фактическим обстоятельствам существования деловой активности. Прежние регламенты и процедуры допуска лиц к информации конфиденциального характера, ориентированные на традиционную, материализованную среду ее существования, уже не являются

эффективным средством защиты информации, в связи с чем последние подлежат адаптации применительно к новой среде – виртуальной. Расширение круга лиц, получающих доступ с информации конфиденциального характера, с учетом использования последними личных компьютерных и иных технических средств актуализировало исследование и выработку новых подходов к системе разрешительного доступа к вышеозначенной информации именно в виртуальной среде организаций, а также к определению прав и пересмотру в сторону расширения обязанностей сотрудников, получивших доступ к данной информации и осуществляющих ее обработку в цифровом формате на личных компьютерных и иных технических устройствах.

Сама же информация личностного характера, генерируемая в виртуальной среде организаций, не только претерпевает объективные изменения за счет создания ее новых видов², ранее не имеющих аналогов, но и изначально создается, используется и хранится в новом формате – цифровом, что позволяет сохранять и накапливать огромное количество информации по сравнению с ее письменной и иной фиксацией. В этой связи с учетом существующей правовой доктрины необходимо исследовать вопрос о возможности отнесения подобного рода информации к категории персональных данных и, исходя из свойств данной информации к мгновенному распространению, масштабированию и хранению в цифровом формате, что порождает повышенные риски нарушения личностных прав, определить как способы ее защиты в условиях цифровизации делового сектора, так и способы обработки с учетом вышеозначенных особенностей.

В настоящее время деятельность любого хозяйствующего субъекта приводит к появлению и накоплению достаточно большого объема персональных данных в цифровом формате, которые имеют как практическую, так и научную ценность, а современные технологии, например искусственный интеллект, признанный наиболее эффективным средством анализа информационного потока,

² Например, информация пользовательского и индивидуального характера, присущая конкретному индивиду – видеозаписи сотрудника в период его нахождения за компьютерным устройством, скриншоты экранов, записи рабочих столов сотрудников, мониторинг Email, переписка в мессенджерах и соцсетях, данные кейлоггера, фиксирующего все нажатия клавиш на клавиатуре, и многие другие виды информации, порождаемые различными технологиями.

порождаемого человеческой деятельностью, позволяют извлекать из нее максимально полезный результат. Согласно Национальной Стратегии развития искусственного интеллекта на период до 2030 года³ предполагается «создание условий для эффективного взаимодействия государства, организаций, в том числе научных, и граждан в сфере развития искусственного интеллекта, что позволит российским технологиям искусственного интеллекта занять значительную долю мирового рынка», а «повышение доступности и качества данных, необходимых для развития искусственного интеллекта» отнесено к основным задачам развития искусственного интеллекта в нашей стране. В этой связи цифровая информация персонального характера, накапливаемая в виртуальной среде организаций, вполне может быть приравнена к «сырьевой базе», ведь недаром стала «крылатой» цитата британского математика и эксперта в области анализа данных Клайва Хамби, что «данные – это новая нефть»⁴, уничтожение которой, равно как и иной другой, будет являться не только нецелесообразным, но и откровенно вредным. Таким образом, возможности объединения научных исследований, предпринимательского результата и мер государственной поддержки в области полезного использования персональных данных, исполненных в цифровом формате, нуждаются в отдельном исследовании.

Указанные особенности современных общественных отношений в области обработки персональных данных и перспективы научно-технологического развития Российской Федерации обусловили выбор темы диссертационного исследования и её актуальность.

Степень научной разработанности темы в целом характеризуется отсутствием в научно-правовой литературе комплексных исследований, посвященных правовому регулированию и защите персональных данных, создаваемых в цифровом формате в виртуальной среде организаций, что обусловлено не столь значительным временным промежутком, прошедшим с момента перехода деловой активности в режим удаленной занятости, а также

³ Утверждена Указом Президента Российской Федерации от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации // СЗ РФ. 14.10.2019 г. № 41. Ст. 5700.

⁴ См.: Алексеев К.Н. Роль больших данных в цифровой экономике // Цифровая экономика. 2019. № 3 (7). С.93.

появлением новых технологических решений в сфере организации бизнес-моделей предпринимательской активности.

Вопросы как общего правового регулирования оборота персональных данных, так и специальных, более узких областей исследования, связанных с правом гражданина на неприкосновенность частной жизни, с защитой персональных данных работников, с определением места персональных данных в системе информации ограниченного доступа, конфиденциальностью информации и т.п. нашли свое отражение в научных трудах таких отечественных ученых, как Ф.А. Абаев, М.В. Бундин, А.В. Дворецкий, Г.Г. Камалова, Я.В. Кудашкин, А.В. Минбалеев, О.Б. Просветова, У.М. Станскова, В.А. Северин, Ю.С. Телина, Л.К. Терещенко и др.

Вместе с тем отдельное комплексное исследование проблемы правового регулирования и защиты персональных данных в организациях с различной степенью виртуальности до настоящего времени не проводилось.

Объектом диссертационного исследования являются информационно-правовые отношения, связанные с признанием, реализацией и защитой персональных данных в цифровом формате, подлежащие регулированию в рамках информационного и цифрового права.

Предметом диссертационного исследования выступают научные концепции, нормативные – правовые акты, а также правоприменительная практика, определяющие правовое регулирование и защиту персональных данных в условиях перехода экономической активности в цифровой формат.

Целью диссертационного исследования является изучение сущности и правовой природы персональных данных в условиях перехода правоотношений внутри общества и государства в цифровой формат на основе действующей нормативно-правовой базы регулирования в данной области и разработка положений и рекомендаций, направленных на формирование механизма правового регулирования защиты персональных данных в виртуальной среде организаций. Достижение указанной цели предполагает последовательное решение следующих задач:

- разработать концепцию правового регулирования и защиты персональных данных в виртуальной среде организаций;
- показать эволюцию правового регулирования и защиты персональных данных в России и за рубежом;
- дать характеристику и определить виды персональных данных, создаваемых при использовании информационных технологий и цифровых решений в виртуальной среде организаций;
- установить способы придания личностной информации о человеке статуса персональных данных;
- исследовать вопрос использования и распоряжения персональными данными в виртуальной среде организаций;
- исследовать способы установления и подтверждения личности в виртуальной среде организаций;
- определить правовой режим обработки персональных данных в виртуальной среде организаций;
- разработать разрешительную систему доступа лиц к персональным данным в виртуальной среде организаций;
- разработать меры организационно-правового и технического характера по обеспечению безопасности персональных данных в виртуальной среде организаций.

Теоретическая основа диссертационного исследования построена на фундаментальных изысканиях таких ученых, как С.А. Авакьян, И.Л. Бачило, В.А. Копылов, В.Н. Лопатин, А.В. Минбалеев, А.В. Морозов, М.М. Рассолов, В.А. Северин, Л.К. Терещенко, А.А. Тедеев, М.А. Федотов и др., непосредственно исследовавших проблемы правового регулирования отношений и в области информационного права, и на стыке с другими юридическими науками, связанными с проблемами информационной безопасности и защиты информации.

Существенное влияние на формирование теоретических положений автора оказали научные труды таких ученых, как Ю.М. Батулин, М.А. Борисов, О.В. Брежнев, М.А. Егорова, А.К. Жарова, С.С. Зенин, О.А. Ижаев, Б.Н. Кадников, Г.Г.

Камалова, В.А. Копылов, Ю.А. Крохина, Ю.В. Кузнецов, Л.Д. Кутейников, А.В. Кучеренко, В.А. Лебедев, В.Н. Лопатин, А.М. Лушников, М.Н. Малеина, Е.В. Мелякова, А.В. Минбалеев, А.В. Морозов, Т.А. Полякова, Е.А. Савченко, В.А. Северин, А.П. Сергеев, А.А. Стрельцов, У.М. Станскова, Э.В. Талапина, А.А. Тедеев, О.И. Тиунов, Т.А. Терещенко, М.А. Федотов, К.В. Черкасов и др.

Обращение к трудам Д. Белла, М. Витцеля, М. Кастельса, Э. Тоффлера, М. Уорнера, К.М. Шваба, в области философии, социологии и экономике позволило автору сформировать мировоззрение о концепции постиндустриального или информационного общества, связываемого с обществом знаний - «knowledge society», третьей волной, четвертой промышленной революцией и с шестым технологическим укладом.

В процессе предлагаемого исследования автором были изучены диссертационные работы Ф.А. Абаева, М.В. Бундина, А.В. Дворецкого, Г.Г. Камаловой, А.В. Кучеренко, Я.В. Кудашкина, О.Б. Просветовой, У.М. Стансковой, А.В. Семашко, Ю.С. Телиной. Каждая из вышеперечисленных работ посвящена как общим вопросам правового регулирования оборота персональных данных, так и специальной, более узкой области исследования, связанной с правом гражданина на неприкосновенность частной жизни, с защитой персональных данных работников, с определением места персональных данных в системе информации ограниченного доступа, конфиденциальности сведений и т.п.

Нормативная основа диссертационного исследования в области как информационного права, так и информационных технологий представлена Конституцией Российской Федерации, международными правовыми актами, федеральным законодательством, указами Президента Российской Федерации, постановлениями Правительства Российской Федерации, иными подзаконными актами, международными и национальными стандартами, а также законодательными актами Межпарламентской Ассамблеи государств-участников СНГ, Решениями Коллегии Евразийской экономической комиссии.

Эмпирическую базу диссертационного исследования составляет обобщенная автором правоприменительная практика, касающаяся защиты прав

человека на неприкосновенность частной жизни, а также восстановления нарушенных прав субъектов персональных данных, которая образована судебными актами Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации, судебными актами судов общей юрисдикции и арбитражных судов, действующих на территории Российской Федерации, а также аналитические, информационные и презентационные материалы различных информационных технологий, использующихся или предлагаемых к использованию в процессе обработки персональных данных.

Методологическую основу исследования составляют как общие (анализ и синтез, логический, диалектический и системный методы), так и частные методы исследования (историко-правовой, формально-юридический, сравнительно-правовой). Обращение к методам анализа и синтеза позволило на основании изучения практики судебных органов выявить и сформулировать основные тенденции правоприменения в области обработки персональных данных в цифровом формате и их защите. Логический метод был использован при изложении темы исследования, включая выводы и предложения, а диалектический метод с учетом цифровизации информации личностного характера позволил выявить общие закономерности, имеющиеся в области обработки и защиты информации, включая и виртуальную среду ее существования. Системный метод исследования позволил автору обнаружить пробелы в нормативном регулировании обработки и защиты персональных данных, создаваемых, используемых и хранящихся в цифровом формате и предложить варианты их восполнения. С помощью историко-правового метода автор проследил эволюцию развития правового регулирования и защиты информации о субъекте в их хронологической последовательности и в различных правовых порядках, что позволило сделать прогноз развития нормативного регулирования процесса обработки и защиты персональных данных в условиях цифровизации. Формально-юридический метод составил основу изучения юридических понятий в исследуемой области, а также выявления их признаков, толкования, уяснения содержания и предписаний правовых норм, что позволило рассмотреть вопрос об их применении в условиях

цифровизации информации. Сравнительно-правовой метод позволил на основании сопоставления требований различных федеральных законов, подзаконных нормативных правовых актах, национальных стандартов, а также технологий, применяемых в соответствии с законодательным установлением, проанализировать и выявить специфические характеристики информации личностного характера, создаваемой и хранящейся в цифровом формате.

Теоретическая значимость диссертационного исследования заключается в том, что оно представляет собой комплексное исследование проблем правового регулирования и защиты персональных данных, исполненных в цифровом формате, в виртуальной среде организаций. Результаты исследования развивают и дополняют концепцию прав человека на неприкосновенность частной жизни. Выводы диссертационного исследования могут быть использованы как в дальнейших научных исследованиях, связанных с регулированием процесса создания персональных данных в цифровом формате с использованием различных технологий, их обработкой и защитой в виртуальной среде, так и в учебном процессе при преподавании информационного права, а также при подготовке учебно-методических рекомендаций, учебников и пособий по курсу «Информационное право».

Практическая значимость диссертационного исследования заключается в возможности использования ее результатов в процессе совершенствования информационного законодательства, а также при подготовки локальных нормативных актов в условиях цифровизации экономики. Отдельные выводы могут быть использованы в правоприменительной практике как органами государственной власти, так и практикующими юристами.

Научная новизна диссертационной работы определяется тем, что впервые комплексно рассмотрены проблемы правового регулирования и защиты персональных данных, создаваемых в цифровом формате, в процессе их обработки и защиты в виртуальной среде организаций с применением информационно-технологических решений. Конкретизация научной новизны выполненного исследования отражена в **основных положениях, выносимых на защиту:**

1. Виртуальная среда организации характеризуется совокупностью:

- локальных актов, которые формируют основу правоотношений хозяйствующего субъекта по использованию технологий коммуникативного общения для взаимодействия пользователей друг с другом как во внутренней информационной среде организации, так и с внешним миром посредством электронной почты, мессенджеров, социальных сетей и других подобных им сервисов; технологий, связанных с созданием информации в цифровом формате, ее использованием, перемещением и хранением; по определению круга субъектов, вовлекаемых в процесс создания информации в цифровом формате и претендующих на доступ к информации конфиденциального характера в процессе осуществления трудовой деятельности;

- виртуальной инфраструктуры – аппаратного комплекса хозяйствующего субъекта, программного обеспечения, компьютерных и иных устройств: смартфонов, планшетов, принадлежащих сотрудникам организации и допускаемых к процессу создания, использования, хранения и перемещения информации в цифровом формате в процессе деятельности хозяйствующего субъекта.

2. Персональные данные сотрудников, такие как табельный номер, адрес электронной почты, IP-адрес и другие аналогичные идентификаторы могут создаваться непосредственно хозяйствующим субъектом и (или) принадлежать ему на ином законном основании, что влияет на объем прав субъекта персональных данных и обязанностей самой организации, в частности, на право субъекта персональных данных требовать уничтожения указанных персональных данных, а организации – на обязанность получать согласие субъекта персональных данных на их обработку.

3. В целях организации эффективной защиты в виртуальной среде организации предлагается разграничение в ней персональных данных на информацию, которая поддается контролю со стороны организации, и информацию, не поддающуюся вышеуказанному контролю или со сниженной степенью контроля, когда: 1) разработчиком гарантируется обеспечение безопасности технологии; 2) сотрудником организации в процессе

производственной деятельности используется информация персонального характера на личном компьютерном или ином техническом устройстве.

4. Необходимо внести в круг субъектов правоотношений по обработке и защите персональных данных в виртуальной среде организаций лиц, осуществляющих обработку персональных данных в цифровом формате на личных компьютерных и иных технических устройствах, с определением их прав и обязанностей.

5. Сведения, характеризующие физиологические и биологические особенности человека, должны быть причислены к категории биометрических персональных данных и именоваться именно так, но с видовым разделением их на биометрические персональные данные, изначально предназначенные для установления личности, и данные, которые не используются для этих целей.

6. При построении разрешительной системы доступа к персональным данным в виртуальной среде организаций необходимо учитывать следующие цели нормативного правового регулирования в данной сфере: 1) с соблюдением оператором и иными лицами, получившими доступ к персональным данным, обрабатываемым в виртуальной среде организации, требований конфиденциальности в соответствии с Законом о персональных данных, т.е. защита прав субъекта персональных данных; 2) с соблюдением лицами, получившими доступ к персональным данным, обрабатываемым в виртуальной среде организаций, требований конфиденциальности в соответствии с иными законами, регулирующими охрану какой-либо тайны, к примеру коммерческой тайны, которой непосредственно являются сами персональные данные или в состав которой они входят, т.е. защита прав оператора персональных данных и иных обладателей информации; 3) с соблюдением оператором персональных данных, обрабатываемых в виртуальной среде, требований Закона о персональных данных, связанных с защитой персональных данных от неправомерного или случайного доступа к ним.

Личный вклад автора. Выносимые на защиту результаты получены лично автором.

Достоверность результатов диссертационного исследования обусловлена использованием теоретических постулатов информационного права и современными исследованиями, анализом нормативной правовой базы в области правового регулирования и защиты персональных данных и соответствующей судебной практикой. Одновременно с этим автором проработан значительный объем эмпирического материала, связанный с изучением современных технологий, способных создавать персональные данные в цифровой среде и предлагаемых в информационной среде – Интернет к практическому применению.

Апробация результатов исследования. Основные положения, выводы и рекомендации отражены в четырех опубликованных статьях в изданиях, рекомендованных ВАК, в докладах на VI Международной конференции «Информационное общество, цифровая экономика и информационная безопасность» (2023 год), а также Научно-практической конференции «Актуальные вопросы информационного и цифрового права», посвященной созданию кафедры правовой информатики (2024 год).

Структура диссертации. Диссертация состоит из введения, трех глав, включающих девять параграфов, заключения, списка использованных нормативных правовых актов и научной литературы.

II. ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность выбранной темы диссертационного исследования, охарактеризована степень ее разработанности, осуществлен выбор предмета и объектов исследования, определены цели, задачи и методологические основания исследования, представлена новизна, теоретическая и практическая значимость результатов исследования.

Глава первая «СУЩНОСТЬ И ПРАВОВАЯ ПРИРОДА ПЕРСОНАЛЬНЫХ ДАННЫХ» посвящена теоретическим обобщениям, необходимым для проведения исследования, и состоит из трех параграфов.

В первом параграфе *«Концепция правового регулирования и защиты персональных данных в виртуальной среде организаций»* излагается общая концепция правового регулирования и защиты персональных данных в виртуальной среде организаций. Так, поступательно выявлены и охарактеризованы фактические признаки виртуальной среды, виды информации, создаваемой и хранящейся в данной среде существования, а также технологии, способные генерировать новую информацию в цифровом формате. Принципиально обозначен подход к вопросу о возможности организаций распоряжаться накапливаемыми в их виртуальной среде персональными данными, посредством использования имеющихся правовых возможностей. Рассмотрены изменения, затрагивающие субъектный состав лиц рассматриваемых правоотношений, а также проблемы установления и подтверждения личности в виртуальной среде организаций. На базе имеющихся теоретических установлений разработан механизм правового регулирования и защиты персональных данных именно в виртуальной среде организаций с учетом не только правовых, но и технических аспектов, а также обоснован вывод о необходимости разработки локальных актов в системе координат правового регулирования и защиты персональных данных в виртуальной среде организаций, примерное содержание которых структурно предлагается автором.

Второй параграф *«Эволюция развития правового регулирования и защиты персональных данных в Российской Федерации»* посвящен анализу исторической ретроспективы правового регулирования персональных данных в России и за рубежом. Концептуально понятие персональных данных и их защиты связаны с деятельностью американских юристов Сэмюэлем Уорреном и Луи Брэндайсом, которые в 1890 году ввели в оборот категорию *privacy*, и которая идентифицируется с неприкосновенностью частной жизни. Данное утверждение достаточно часто используется в научных работах, связанных с тематикой персональных данных. При этом в отечественном правотворчестве постулаты, связанные с охраной и защитой частной жизни гражданина, являются далеко не новыми и возникли они задолго до американского «права быть оставленным в

одиночестве». Обусловлено это тем, что российская государственность сформировалась значительно раньше и рассматриваемые гуманистические идеи были ей далеко не чужды. Так, автором выявлена и показана историческая последовательность развития юридической защиты права на неприкосновенность частной жизни субъекта с учетом общественно-политических изменений и развитием основных прав и свобод человека и гражданина в Российской Федерации. Системный анализ отечественного правотворчества позволяет не только наглядно показать эволюцию развития данного института, но и ввести в научный оборот новую информацию, которая ранее не использовалась в научных исследованиях, что способствует развитию современной науки.

В третьем параграфе *«Определение информации, относящейся к персональным данным»* отражены результаты исследования вопроса о том, какая информация из общего числа сведений может быть отнесена к категории персональных данных. Так, установлено, что персональными данными информация может стать только при наличии следующей совокупности условий:

- обязательными субъектами отношений по обработке персональных данных являются субъект персональных данных и оператор персональных данных;
- информация в добровольном порядке передается субъектом персональных данных оператору, осуществляющему их обработку;
- оператор осуществляет обработку персональных данных в строго определенных целях.

Одновременно с этим выявлены и охарактеризованы способы придания информации о человеке статуса персональных данных посредством:

- волеизъявления оператора персональных данных;
- законодательного закрепления;
- судебного установления;
- волеизъявления субъекта персональных данных.

Результаты анализа норм действующего законодательства, а также изучения судебной практики позволили обосновать вывод о необходимости именовать все сведения, характеризующие физиологические и биологические особенности

человека, вне зависимости от целей их получения и использования биометрическими персональными данными с видовым разделением на биометрические персональные данные, предназначенные для установления личности, и просто биометрические персональные данные. При этом отдельно исследована особенность биометрических персональных данных переходить из одной категории в другую, когда сведения, характеризующие физиологические и биологические особенности человека, изначально не предназначенные для установления личности, могут при определенных условиях быть использованы для этих целей.

Глава 2 «ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБОРОТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ВИРТУАЛЬНОЙ СРЕДЕ ОРГАНИЗАЦИЙ»

посвящена выявлению и исследованию характерных признаков виртуальной среды организаций, в которой создаются, используются и хранятся персональные данные в цифровом формате, и состоит из трех параграфов.

В параграфе первом *«Характеристика и виды персональных данных в виртуальной среде организаций»* дается представление о виртуальной среде организаций, которая характеризуется совокупностью аппаратной инфраструктуры, технологий, программного обеспечения и т.п. привычными элементами цифровой действительности, а также описанием моделей коммуникаций, видов технологий, предполагаемых к использованию, способов обработки персональных данных и установлением их перечня, определением круга субъектов, вовлекаемых в процесс создания информации и претендующих на доступ к информации конфиденциального характера, контура сетей и т.п., что в итоге формирует основу правоотношений под которую уже и производится технологическое оснащение. Все вышеизложенное способствует появлению определенных различий в виртуальной среде организаций, в связи с наличием у каждой своих индивидуальных потребностей.

В состав персональных данных в виртуальной среде организации входят те, которые изначально создаются и хранятся в рассматриваемой среде, а также те, которые будучи отраженными на материальном носителе, впоследствии в

результате оцифровки попадают в вышеуказанную среду. В первую группу, в свою очередь, включаются персональные данные, создаваемые в процессе использования информационно-коммуникационных технологий, таких как корпоративная электронная почта, различные чаты для обмена сообщениями в режиме реального времени, скайп, посредством которого возможно осуществлять не только текстовую и голосовую, но и видеосвязь с возможностью фиксации в электронном виде всего процесса и т.п., а также в области контроля – это, к примеру программы, которые фиксируют все нажатия клавиш на компьютере (кейлогеры), делают скриншоты рабочего стола или записывают видео (видеологеры), отслеживают файловую работу, собирают данные по работе с программами и интернет-сайтами, отслеживают отправления по электронной почте и многие другие, перечень и назначение которых постоянно расширяется.

Одновременно с этим в исследовании предложена признаковая совокупность элементов, связанных с рассматриваемой информацией и направленная на определение прав и обязанностей в части обработки персональных данных и осуществления их защиты, а также оптимизацию сопряженного с этим процесса нормативного регулирования. Условно персональные данные, обрабатываемые в виртуальной среде организаций, предложено сгруппировать по следующим признакам:

- информация, получаемая от коммуникативного общения и от осуществления контрольных полномочий;
- источники поступления (в рамках локального контура и/или за его пределами);
- субъектный состав (сотрудники организации и/или третьи лица);
- обычные персональные данные и биометрические персональные данные как предназначенные для установления личности человека, так и не предназначенные для этих целей.

Параграф второй «Использование и распоряжение персональными данными в виртуальной среде организаций» посвящен рассмотрению вопроса, связанного с использованием и распоряжением персональными данными в

виртуальной среде организаций. В нормах действующего законодательства применительно к персональным данным отсутствует понятие или какое-либо иное указание на собственника информации личностного характера. В правовом обороте используется законодательное определение понятия «обладатель информации», которым является лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам, т.е. решать вопрос о ее получении другими лицами и о способах ее использования как им самим, так и другими лицами. В этой связи предлагается предоставлять организациям легальную возможность использовать рассматриваемую информацию личностного характера как для внутреннего потребления, так и передавать ее сторонним организациям, например, в научно-практических целях или для использования в иных предметных разработках той или иной области, посредством приобретения последними правового статуса обладателя информации.

В третьем параграфе *«Установление и подтверждение личности в виртуальной среде организаций»* выявлены и систематизированы способы достижения вышеуказанной цели. Так, установление личности возможно посредством:

- предъявления удостоверяющего личность документа (в рамках виртуальной среды коммуникации удостоверение личности происходит посредством визуального сравнения лица человека с фотографией в документе, к примеру копии паспорта в виде PDF-файла);

- биометрических персональных данных (в РФ создана и действует Единая биометрическая система (ЕБС), которой придан статус государственной информационной системы (ГИС), что гарантирует наивысшую степень защищенности данных. Действия по идентификации и (или) аутентификации физического лица с использованием ЕБС приравниваются к действиям по предъявлению документов, удостоверяющих личность такого физического лица. С помощью ЕБС предполагается оказание как коммерческих, так и государственных услуг, например, открытие счетов, вкладов, получение кредитов, оплата покупок и

проезда, дистанционное получение e-SIM и сдача экзаменов, участие в судебных заседаниях в режиме видеосвязи, нотариальные услуги. Что же касается возможности установления личности физического лица в режиме дистанционного доступа, например при проведении собеседования с претендентом на занятие вакантной должности или предполагаемым партнером при вступлении в гражданско-правовые отношения с использованием ЕБС, то на настоящий момент механизм такой практической интеграции отсутствует;

- технологических решений подтверждения личности без применения биометрических шаблонов (данный раздел представлен отечественными разработками:

- позволяющими проводить сверку лиц без выделения биометрических дескрипторов, когда удостоверение личности происходит только по паспорту без обращения к (ЕБС) и без применения биометрических шаблонов за счет того, что система сверяет фото в документе, например паспорте гражданина РФ - с его селфи. После загрузки в систему двух вышеуказанных изображений, последняя на основе метрических характеристик дает оценку тому, насколько они похожи. Процесс максимально схож со сверкой лиц, которую обычно осуществляет человек. Разработчики именуют ее небюметрической сверкой лиц, что очень верно отражает не только ее существо, но и само направление развития технологий в данной области, как некой альтернативы биометрии;
- платформой цифрового доверия для подтверждения персональных данных при обращении к различным сервисам без раскрытия содержания этих персональных данных, имеющая перспективу широкой востребованности. Так, персональные данные гражданина хранятся только у него и, так называемого, инспектора персональных данных, например, паспортные данные в МВД РФ, СНИЛС в ПФР, ИНН в ФНС. Гражданин, используя индивидуальный модуль доверия (ИМД), предоставляет свои данные поставщику цифровых сервисов и услуг в виде зашифрованного блока данных, при этом последний не имеет доступа к содержанию этих данных,

он лишь имеет возможность передать этот зашифрованный блок данных инспектору персональных данных (МВД РФ, ПФР, ФНС) и получить от него заключение о соответствии этих данных данным, хранящимся у него);

- цифрового профиля гражданина (совокупность цифровых записей о гражданине, содержащихся в информационных системах государственных органов и организаций, предоставляющего сведения о гражданине, содержащиеся в ЕСИА или других государственных информационных системах, взаимодействующих с ЕСИА посредством единой системы межведомственного электронного взаимодействия, с его согласия третьим лицам в интересах самого гражданина (например, предоставление банку проверенных сведений, необходимых для заполнения кредитной заявки).

- электронного способа идентификации личности (цифровой идентификатор (Digital ID) — это электронный способ идентификации личности в цифровом пространстве, который на основе уникальности связывается с конкретным лицом и используется для подтверждения личности или авторства в различных цифровых процессах, таких как онлайн-аутентификация, цифровые подписи, доступ к онлайн-сервисам и многое другое. Набор технологий и интеллектуальных устройств для верификации личности по цифровой информации представлен биометрическими персональными данными, цифровыми паспортами или ID, паролями, ПИН-кодами, QR-кодами.

Глава 3 «МЕХАНИЗМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ВИРТУАЛЬНОЙ СРЕДЕ ОРГАНИЗАЦИЙ» посвящен рассмотрению особенностей защиты персональных данных в цифровом формате в виртуальной среде организаций состоит из трех параграфов.

В первом параграфе *«Правовой режим обработки персональных данных в виртуальной среде организаций»* обосновывается утверждение о возрастающей роли локального нормотворчества в правовом регулировании обработки персональных данных в виртуальной среде организаций, поскольку в каждой организационной структуре создается своя виртуальная среда, которая, как правило, не является стабильной за счет манипуляций с различными технологиями.

Именно локальные нормативные акты, являясь по своей природе более мобильным средством правового реагирования на различные ситуационные изменения, способны в полной мере обеспечить регулирование в области применения различных технологий, связанных с созданием информации в цифровом формате, ее использованием и хранением, а также технологий телекоммуникационного пространства для взаимодействия пользователей друг с другом как во внутренней информационной среде организации, так и с внешним миром посредством мессенджеров, социальных сетей, сервисов беспроводного взаимодействия для организации видеоконференций, вебинаров, групповых чатов и т.п. Использование данных технологий влечет за собой увеличение числа лиц, получающих доступ к персональным данным, включая и персональные данные, характеризующие физиологические особенности человека, с одновременным расширением аппаратной составляющей виртуальной среды организаций за счет использование личных компьютерных средств, смартфонов, планшетов, в связи с чем обосновывается вывод о необходимости внесения в круг субъектов правоотношений по обработке и защите персональных данных в виртуальной среде организаций лиц, осуществляющих обработку персональных данных в цифровом формате на личных компьютерных и иных технических устройствах, с определением их прав и обязанностей. Обосновывается тезис о необходимости разделения зон ответственности по защите информации между теми, кто предоставляет определенного рода информационные технологии и декларирует определенные условия безопасности использования предлагаемого коммуникативного продукта в части защищенности информации, включая и персональные данные, и теми, кто их использует.

Параграф второй «Разрешительная система доступа к персональным данным в виртуальной среде организаций» посвящен выявлению и рассмотрению особенностей разрешительной системы доступа к персональным данным в виртуальной среде организаций. Выявлены и исследованы цели создания такой системы, которые разделены на три направления.

- первое – это соблюдение конфиденциальности. При этом состояние конфиденциальности, когда операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных сохраняется до тех пор, пока последний своим волевым решением не прекратит ее существование, дав согласие на раскрытие и распространение, т.е. конфиденциальность персональных данных полностью зависит от желаний и предпочтений субъекта персональных данных. В этой связи обосновывается потенциальная возможность получения от субъекта персональных данных такого согласия на раскрытие и распространение персональных данных как определенных, так и тех, которые будут создаваться в процессе трудовой или иной деятельности, а также в результате коммуникативного общения в цифровой среде. Наличие подобного согласия на предоставление и раскрытие данной информации существенно облегчит правовую регламентацию возможности ее использования всеми сотрудниками, а не только теми, кто имеет специально установленный доступ. Поскольку форма такого согласия Законом не оговорена, как не оговорено и право субъекта персональных данных данное согласие отозвать, регулирование рассматриваемых правоотношений должно происходить в рамках локальной разрешительной системы доступа к персональным данным организации с определением формы согласия, срока его предоставления, порядка отзыва и т.п. критериев;

- второе – это причисление персональных данных к активам организации, имеющим ценность в интересах достижения целей деятельности и находящимся в ее распоряжении. При этом персональные данные в силу своей универсальности способны вступать в коллаборацию и с иными тайнами, например государственной, защитой свидетелей и т.п., когда и личность человека, и его внешние данные, характеризующие его физиологические особенности, и иные сведения должны быть недоступны для третьих лиц. Разрешительная система доступа в каждом конкретном случае должна учитывать требования законодательных норм, регулирующих конкретные отношения. Так, конфиденциальность видеозаписи совещания подлежит сохранению и в

отношении биометрических персональных данных, и в отношении коммерческой тайны, к которой может быть отнесена информация о проведении переговоров;

- третье – это соблюдение оператором персональных данных требований Закона о персональных данных, согласно которым при обработке персональных данных он обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним.

В третьем параграфе «Меры организационно – правового и технического характера по обеспечению безопасности персональных данных в виртуальной среде организаций» обосновывается вывод о том, что разработка мер технического характера должна проводиться с учетом особенностей формирования и наполнения виртуальной среды каждой, отдельно взятой организации. В целях создания сбалансированной защиты персональных данных в виртуальной среде организаций для сохранения ее конфиденциальности, целостности и доступности необходимо определить основные подходы и политику организации в области: создания ИТ-инфраструктуры организации; использования программного обеспечения и антивирусной защиты как организацией, так и ее сотрудниками (использование только сертифицированного программного обеспечения, антивирусной защиты и т.п.); использования сотрудниками и иными лицами личных компьютерных средств, мобильных телефонов и иных гаджетов при получении доступа в виртуальную среду организации; работы в корпоративной сети, а также с такими инструментами как мессенджеры, онлайн-платформы различного назначения и т.п.; применения программ с различным целевым назначением, в результате использования которых будут создаваться и храниться в виртуальной среде организации персональные данные сотрудников; хранения персональных данных в виртуальной среде организации (локальное, облачное, комбинированное и т.п.); работы в условиях удаленного доступа, а также с сетью Интернет; создания, предоставления и использования паролей и иных идентификаторов и средств доступа в виртуальную среду организации; обеспечения и защиты критически

значимой информации при взаимодействии с третьими лицами в виртуальной среде организации.

Одновременно с этим обосновывается целесообразность проведения условного разграничения персональных данных в виртуальной среде на информацию, которая поддается контролю со стороны организации, и информацию, не поддающуюся вышеуказанному контролю или со сниженной степенью контроля, когда обеспечение безопасности гарантируется разработчиком технологии, или когда сотрудник организации, использующий информацию персонального характера на своем компьютерном устройстве или гаджете несет ответственность за ее сохранность и обеспечение конфиденциальности. При этом чем выше степень концентрации надзорной функции, возлагаемой на конкретное лицо или службу с применением строго определенных технических средств и программного обеспечения, тем выше и контроль со стороны организации. В данных условиях и при отсутствии иных «неизвестных» хозяйствующая структура имеет наивысшую степень контроля над персональными данными в ее виртуальной среде. Снижение же данного контроля вплоть до его полной утраты происходит по мере увеличения лиц, вовлекаемых в процесс обработки (использования и хранения) персональных данных, – сотрудников и третьих лиц – партнеров, а также при использовании технологий массового использования (мессенджеры, онлайн-платформы различного назначения и т.п.) с привлечением личных технических средств. При этом тенденция свидетельствует в пользу ослабления контроля и защиты со стороны оператора персональных данных в сторону увеличения контроля и защиты персональных данных сотрудниками и третьими лицами, использующими и хранящими вышеуказанную информацию.

Меры технического характера по обеспечению безопасности персональных данных в виртуальной среде организаций напрямую зависят от вышеуказанной градации. Условно их предлагается разделить на две категории: обязательные к исполнению и рекомендательного характера. Первые относятся непосредственно к оператору персональных данных и находятся в его зоне ответственности, а вторые – к сотрудникам и третьим лицам, использующим и хранящим персональные

данные на личных компьютерных устройствах и иных гаджетах, что делает контроль со стороны оператора персональных данных практически невозможным и влечет за собой переложение данной обязанности на последних.

III. ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИОННОГО ИССЛЕДОВАНИЯ ИЗЛОЖЕНЫ В СЛЕДУЮЩИХ ПУБЛИКАЦИЯХ

Список работ, опубликованных в рецензируемых научных изданиях, рекомендованных для защиты в Диссертационном совете МГУ по специальности 5.1.2 Публично – правовые (государственно – правовые) науки

1. Ильюшина И.С. Историческая ретроспектива развития правового регулирования и защиты персональных данных в дореволюционный период // Информационное право. 2023. № 4 (78). С.38-41 (0,5 п.л.). (2-летний импакт-фактор РИНЦ: 0,675).

2. Ильюшина И.С. Способы придания информации статуса персональных данных // Право и государство: теория и практика. 2024. № 5 (233). С.159-161 (0,375 п.л.). (2-летний импакт-фактор РИНЦ: 0,076).

3. Ильюшина И.С. Идентификация физических лиц с использованием биометрических персональных данных в виртуальных организациях // Вестник Московского университета. Серия 26. Государственный аудит. 2023. № 4. С.94-105 (0,75 п.л.). (2-летний импакт-фактор РИНЦ: 0,153).

4. Ильюшина И.С. Использование и распоряжение персональными данными в виртуальной среде организаций // Пробелы в российском законодательстве. 2024. № 6. С.48-56 (0,56 п.л.). (2-летний импакт-фактор РИНЦ: 0,259).