МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В.ЛОМОНОСОВА
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

*На правах рукописи*

**Ильюшина Инна Сергеевна**

# Правовое регулирование и защита персональных данных в виртуальной среде организаций

5.1.2 Публично – правовые (государственно – правовые) науки

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук, доцент
Северин В.А.

Москва – 2025

# ОГЛАВЛЕНИЕ

# ВВЕДЕНИЕ

***Актуальность темы исследования.*** Эволюционные изменения, порождаемые применением новых информационных и коммуникационных технологий, повсеместно оказывают существенное влияние на все сферы жизнедеятельности общества. Постоянное совершенствование уже имеющихся и вновь создаваемых технологический решений предоставляют новые, ранее не известные возможности, меняя подчас до неузнаваемости привычные, ставшие традиционными, формы существования, основанные в большинстве своем на личных и присутственных взаимоотношениях. Еще относительно недавно вся информация существовала «на бумаге», а удаленные коммуникации, оставляющие следы и порождающие возникновение правовых последствий, были представлены незначительным кругом технически обеспеченных возможностей, например, передача информации с помощью факса, телефонограммы при том, что последняя все равно была зафиксирована на том или ином материальном носителе. Крайне осторожно начиналось и подвергалось в последствие законодательному регулированию использование записывающих аудио-видео устройств, в частности, в судопроизводстве. На данном уровне технологического развития информация существовала в среде устного общения, носителями которой были физические лица, и на материальном носителе в том или ином виде, например, на бумаге, кассете, диске. Внедрение же современных цифровых технологий в течение последних десятилетий стимулировало формирование совершенно новых общественных отношений, протекающих в цифровой форме в виртуальном пространстве, и это не просто отношения по обороту информации — это цифровые отношения в информационной среде[1]. При этом «цифровая технология противопоставляется аналоговой: аналоговые технологии основаны на способе

[1] Борисов М. А., Будник Р.А., Войниканис Е. А., Дейнеко А.Г., Елин В.М., Ерофеева Е.В., Жарова А.К., Монахов В. Н., Околёснова О. А., Перепелица Е. В., Петрин И. В., Примакова А.В., Серго А. Г., Тедеев А. А., Федотов М.А., Шаблинский И. Г., Якимовская Н. Л. Информационное право: Учебник для вузов / Под общей редакцией Федотова М.А. М.: Юрайт, 2023. С. 38.

представления информации в виде какой-либо непрерывной (аналоговой) физической величины, и данная величина является носителем информации, а цифровая технология основана на способе представления информации в виде чисел (обычно с использованием двоичной системы счисления) в электронном виде, значение которых является носителем информации»[2], а программный код является «способом фиксации», т.е. речь идет о нормах, кодифицированных в виде программного обеспечения[3]. Цифровая же среда охарактеризована как среда логических объектов, используемая для описания (моделирования) других сред, в частности, электронной и социальной) на основе математических законов[4]. Таким образом, как верно указано Е.А. Савченко, само понятие формы в цифровой среде претерпело существенные изменения[5].

Информация, включая и информацию личностного характера, генерируемая в виртуальной среде организаций, не только претерпевает объективные изменения за счет создания ее новых видов[6], ранее не имеющих аналогов, но и изначально создается, используется и хранится в новом формате – цифровом, что одновременно придает ей и новые свойства – способность к мгновенному распространению и неограниченному масштабированию. Сам же формат позволяет сохранять и накапливать огромное количество информации по сравнению с ее письменной и иной фиксацией. Действительно, «настоящая реальность такова, что любая активность человека, связанная с цифровой средой, фиксируется устройствами в ИКТ среде и составляет информацию, которую ученые стали называть цифровым

---

[2] Крохина Ю.А. Проблемы правового регулирования цифровых технологий, применяемых Центральным банком РФ и финансовыми институтами // Мониторинг правоприменения. 2022. № 4 (45). С. 33.

[3] Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник / Под редакцией акад. Б.Н. Топорнина Спб.: Юрид.центр Пресс, 2001. С. 151.

[4] п.4.2.11 ГОСТ Р 52292-2004. Национальный стандарт РФ. Информационная технология. Электронный обмен информацией. Термины и определения // М.: ИПК Издательство стандартов. 2005.

[5] Савченко Е.А. Культурные права человека в условиях цифровизации // Вестник Томского государственного университета. Право. 2023. № 49. С. 151-164.

[6] 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.

следом или цифровой тенью»[7], что очень точно охарактеризовано такими учеными как А.К. Жарова, В.М. Елин, А.В. Минбалеев. Спектр же полезного использования такого рода информации поистине безграничен как с практической, так и с научной точки зрения. В этой связи очень верно утверждение М.А. Федотова о том, что «современным миром правит информация, развитие информационных и цифровых технологий определяет практически все: от качества жизни людей и условий развития экономической деятельности до национальной безопасности и эффективности оказания государственных услуг»[8]. Так, в Стратегии развития информационного общества в Российской Федерации 2017 – 2030 годы[9] (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»[10]. Одновременно с этим «обеспечение баланса между своевременным внедрением современных технологий обработки данных и защитой прав граждан, включая право на личную и семейную тайну»[11], поименовано в Стратегии в качестве одной

[7] Жарова А.К., Елин В.М., Минбалеев А.В. Парадигма цифрового профилирования деятельности человека: риски, угрозы, преступления: монография // М.: РУСАЙНС, 2024. С.19.
[8] Федотов М.А. Информационное право: учебник для бакалавриата, специалитета и магистратуры. М.: Юрайт, 2019. С. 11.
[9] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СЗ РФ. 15.05.2017. № 20. Ст. 2901.
[10] пункт 46 Стратегии.
[11] пункт 31 Стратегии.

из национальных целей развития Российской Федерации. Действительно, «диджитализация общественных отношений и всех сфер жизнедеятельности общества в определенной степени меняет существующий механизм защиты прав и свобод человека и гражданина», как верно отмечено Черкасовым К.В.[12].

Нельзя не согласиться с мнением Л.Д. Кутейникова, О.А. Ижаева, В.А. Лебедева, С.С. Зенина о том, что «цифровая среда стала одной из самостоятельных сфер жизнедеятельности общества, а возникающие в этой связи общественные отношения являются сравнительно новыми, и нельзя утверждать, что в правовой науке сформировались устоявшиеся подходы к их регулированию. На первый взгляд такие традиционные конституционные права, как право на неприкосновенность частной жизни, право на свободу слова и выражения мнений, на информацию и некоторые другие виды прав, полноценно охватывают складывающиеся отношения в сфере информационных технологий. Однако невозможно игнорировать и тот факт, что правовые средства их обеспечения и защиты также должны учитывать особенности данных отношений»[13]. *Именно поэтому теоретические познания и выводы в области правового регулирования и защиты персональных данных нуждаются в адаптации к современным реалиям, поскольку 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.*

Так, виртуальная среда организации представляет собой определенное информационное пространство, где за счет функционирования интегрированной

---

[12] Черкасов К.В. Трансформация прав и обязанностей человека и гражданина в условиях цифрового общества и государства // Сборник материалов Всероссийской научно-практической конференции «Защита прав человека: теория и региональная практика». Хакасский государственный университет им. Н.Ф. Катанова. 2021. С.181-182.

[13] Кутейников Л.Д., Ижаев О.А., Лебедев В.А., Зенин С.С. Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности // LEX RUSSICA. 2022. Том 75 № 2 (183). С. 121-131.

системы, в которую входят аппаратные средства (оборудование) и программное обеспечение, совместно работающие для выполнения заранее определенных задач, а также различных коммуникационных сервисов мгновенного обмена сообщениями, таких как Яндекс.Телемост[14], Контур Толк[15] и им подобных, 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 других составляющих. *В этой связи приобрели актуальность вопросы формирования основ правоотношений, а также юридической регламентации создания и функционирования виртуальной среды организации посредством организационно-правовых мер на уровне локального нормотворчества.*

Характерной особенностью виртуальной среды организаций в части ее технической (аппаратной) составляющей является использование сотрудниками в процессе осуществления трудовой деятельности своих личных компьютеров, планшетов, смартфонов и других технических средств, позволяющих осуществлять хранение информации, в том числе и ограниченного доступа. Сложность и многообразие современных бизнес-задач, быстрота их реализации, возможность работать удаленно в совокупности с массовой доступностью высокотехнологичных средств производства, повлекли за собой естественные изменения технической инфраструктуры виртуальной среды организаций за счет вхождения в нее персональных компьютерных и иных устройств, *что также актуализировало вопросы правовой регламентации и возможности восполнения законодательных, методических и технических пробелов за счет локального нормотворчества, в том*

[14] https://www.google.com/search?client=safari&rls=en&q=яндекс.Телемост&ie=UTF-8&oe=UTF-8.
[15] https://kontur.ru/talk.

*числе и в области создания единой системы информационной безопасности, например, за счет установления и использования для входа в информационное пространство организации единых паролей, использования определенного программного обеспечения, антивирусных программ и других защитных мер.*

Не менее масштабной новеллой является и увеличение числа лиц, получающих доступ к информации конфиденциального характера, хранящейся в виртуальной среде организаций, что обусловлено все возрастающей коллаборацией целевых задач внутри производственного процесса. В современных реалиях исходный цифровой материал и иной контент, содержащий информацию ограниченного доступа, так или иначе задействованы в работе почти каждого сотрудника с различной степенью интенсивности, поскольку вся деловая активность оцифрована и проходит в виртуальной среде организаций, которая позволяет обеспечить такой доступ быстро и одномоментно для неограниченного числа лиц. Одновременно с этим некоторая производственная информация коммуникативного характера, фиксируемая в цифровом формате, например: аудио- и видеозаписи совещаний с партнерами, корпоративная переписка в мессенджере хранится в виртуальной среде различных организаций, т.е. одни и те же персональные данные, включая и характеризующие физиологические особенности, принадлежащие сотрудникам разных хозяйствующих субъектов, могут находиться на хранении у каждой из сторон в ее виртуальной среде, т.е. последние в равной мере являются совместными обладателями данной информации, при том, что подобного рода взаимоотношения со всеми правами и обязанностями сторон в отношении вышеуказанной информации, а также особенности обработки персональных данных в таких условиях в нормах действующего законодательства отдельно не выделены и не урегулированы. *В этой связи прежние регламенты и процедуры допуска лиц к информации конфиденциального характера, ориентированные в основном на традиционную, материализованную среду ее существования, на ограничение технической составляющей исключительно устройствами, принадлежащими организации, а также на допуск к данной информации исключительно сотрудников организации, уже не являются столь*

*эффективным средством защиты информации, в связи с чем определение способов их адаптации применительно к новой среде – виртуальной, выработка новых концептуальных подходов формирования разрешительной системы допуска, а также определение прав и обязанностей сотрудников, получивших доступ к данной информации и осуществляющих ее обработку в цифровом формате на личных компьютерных и иных технических устройствах, являются актуальными и востребованными.*

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 том, что 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. *В этой связи в целях совершенствования механизма защиты персональных данных в виртуальной среде организаций является актуальным проведение условного разграничения персональных данных в цифровой 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 или деловой партнер, использующие информацию персонального характера на своих компьютерных устройствах или иных гаджетах, несут ответственность за ее сохранность и обеспечение конфиденциальности.* При этом тенденция увеличения лиц, вовлекаемых в процесс обработки (использования и хранения) персональных данных, – сотрудников и третьих лиц – партнеров, а также использования технологий мгновенной коммуникации с возможностью цифровой фиксации всей информации (мессенджеры, онлайн-платформы различного назначения и иные подобные технологии) с привлечением личных технических средств 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, *что актуализировало тему совершенствования правового механизма защиты персональных данных в виртуальной среде организаций.* Меры же 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 и иных устройствах, что делает контроль со стороны оператора персональных данных практически невозможным и влечет за собой переложение данной обязанности на последних.

Коммуникация географически удаленных партнеров в виртуальной среде организаций «вызвала к жизни» проблему, связанную с установлением личности субъекта, претендующего на установление трудовых или иных экономических отношений. Законодательно закрепленные механизмы биометрической идентификации личности применимы в строго определенных случаях и находятся в исключительном ведении государства, а возможность создания и использования коммерческих биометрических баз данных более не предусмотрена. Целевое предназначение биометрических систем, разрешенных к использованию, ориентировано прежде всего на обеспечение жизнедеятельности различных государственных и социальных институтов, при том, что на уровне декларативного заявления интеграция коммерческих и иных экономических структур с вышеуказанными информационными системами тем не менее предполагается. Однако до настоящего момента механизм их взаимодействия законодательно не проработан, в связи с чем *в настоящем исследовании будет предпринята попытка рассмотреть актуальный вопрос о возможности удовлетворения потребностей заинтересованных лиц в данной прикладной области за счет использования иных сервисных и технологических решений подтверждающего характера без*

*использования биометрических идентификаторов за счет регламентации на базе локальных нормативных актов.*

Информация, создаваемая и накапливаемая в виртуальной среде организаций, представляет собой не только практический в периметре самой организации, но и научный интерес, поскольку может быть использована для достижения полезного результата в самых различных областях и сферах. Научные и исследовательские сообщества в области создания высоких технологий остро нуждаются в таких исходных данных, а ставший приоритетным на уровне государственной заинтересованности искусственный интеллект зиждется на использовании для обучения алгоритмических моделей большого количества данных. На фоне рассматриваемых структурных преобразований любая информация, включая и персональные данные, приобретает ранее не известную ей ценность, и не исключено, что в очень скором времени ее уничтожение будет признаваться нецелесообразным, равно как и иной сырьевой базы. В этой связи *в диссертационном исследовании предпринята попытка рассмотреть актуальный вопрос, связанный с возможностью организаций на законных основаниях распоряжаться аккумулированной в ее виртуальном пространстве информацией, включая и персональные данные, по своему усмотрению, включая и передачу последней для использования в научных и иных исследовательских целях как на безвозмездной основе, так и за плату.*

Основная ***научная проблема***, подлежащая изучению и разрешению, заключается в наличие пробелов в теоретической базе правового регулирования и защиты персональных данных именно в виртуальной среде их существования в условиях технологического развития общества при переходе в цифровую эпоху, для восполнения которых необходимо осмыслить и разработать новые концепции и парадигмы регулятивного характера, а также адаптировать или изменить уже существующие подходы.

***Объектом изучения*** являются информационно-правовые отношения, связанные с признанием, реализацией и защитой персональных данных в цифровом

формате, подлежащие регулированию в рамках информационного и цифрового права.

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

***Целью*** настоящего 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 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.

***Степень научной разработанности темы*** в целом характеризуется отсутствием в научно-правовой литературе комплексных исследований, посвященных правовому регулированию и защите персональных данных в виртуальной среде организаций при осуществлении коммуникаций посредством интернет-технологий, что обусловлено не столь значительным временным промежутком, прошедшим с момента перехода деловой активности в режим удаленной занятости и в цифровой формат, а также 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.

***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. Батурин, 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, конфиденциальностью сведений.

***Методологию и методы 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 правопорядках, 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.

***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.

***Эмпирическая основа*** 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.

***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 поддающейся 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.** Обосновывается внесение 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, обращаемых 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, обращаемым 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, обращаемых в виртуальной среде, требований Закона о персональных данных, связанных с защитой персональных данных от неправомерного или случайного доступа к ним.

***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 подготовке локальных нормативных актов в условиях цифровизации экономики. Отдельные выводы могут быть использованы в правоприменительной практике как органами государственной власти, так и практикующими юристами.

***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.

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

***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 обусловлена целями и задачами проведенного*** исследования и состоит из введения, трех глав, объединяющих девять параграфов, заключения и списка использованных нормативных правовых актов и научной литературы.

# ГЛАВА I. СУЩНОСТЬ И ПРАВОВАЯ ПРИРОДА ПЕРСОНАЛЬНЫХ ДАННЫХ

## § 1. Концепция правового регулирования и защиты персональных данных в виртуальной среде организаций

Для целей настоящего диссертационного исследования концептуальным фактором, вокруг которого и формируется само исследование, является виртуальная среда, ставшая неотъемлемой частью нашей жизни. Информационно-технологические достижения сделали виртуальную среду существования естественным жизненным пространством, в котором непрерывно происходит обмен данными, информацией, онлайн взаимодействие посредством ИКТ. Базовое понятие виртуальной среды в нормах действующего законодательства отсутствует, что тем не менее не препятствует выявлению ее характерных черт с учетом целей настоящего исследования. Так, к примеру, Е.А. Савченко определяет виртуальное пространство, как пространство обмена данными (данные – поддающееся многократной интерпретации представление информации в формализованном виде, пригодном для передачи, связи или обработки) между вычислительными устройствами – компьютерами, серверами, маршрутизаторами и другим оборудованием или программным обеспечением[16], что очень точно выражает существо рассматриваемой среды, куда переместились общественные отношения. Виртуальная среда организаций – это информационное пространство в цифровом формате в границах, определяемых самой организацией, которая порождает себе подобную информацию в электронном виде, именуемую также цифровой информацией. Создается виртуальная среда 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,

[16] Савченко Е.А. Право и виртуальное пространство: коллективная монография; отв. ред. Ю.А. Тихомиров // Москва: Проспект, 2025. – С. 33.

сопутствующих деловой активности. При этом в каждой организации с учетом ее объективных потребностей создается своя виртуальная среда, обладающая индивидуальными признаками, а границы ее определяются совокупностью аппаратного оборудования, задействованного в процессе осуществления уставной деятельности организации. Вышеозначенная техническая составляющая, генерирующая информационное пространство и определяющая ее границы, представлена компьютерными средствами, смартфонами, планшетами и другими устройствами как принадлежащими самой организации, так, и что является новым, находящимися в собственности сотрудников и иных третьих лиц, вступающих во взаимоотношения с организацией. Виртуальная среда используется для обработки информации на вышеуказанной инфраструктуре и ее хранении, а также для коммуникаций географически удаленных лиц. Как очень верно отмечено О.И. Немыкиной, «немаловажная особенность виртуального пространства – это мгновенный доступ к любой области пространства, в отличие от пространства ординарной реальности, где для этого требуется затрата значительных усилий и времени на перемещение из одной точки в другую»[17]. Таким образом, информационное пространство аккумулирует информацию в цифровом формате, доступном для визуального обозрения, а также для передачи и иного отображения. Создаваемая же в организации виртуальная среда по своей природе является динамичной, поскольку перманентно пополняется за счет внедрения и использования новых информационно-коммуникационных технологий, программного обеспечения и им подобных разработок, а также аппаратной части. При этом появление нового цифрового формата информации тем не менее нисколько не отразилось на таком ее юридическом свойстве, как двуединство информации и носителя[18], поскольку с технической точки зрения последняя также существует на материальных носителях как в локальном формате – компьютер, смартфон, планшет, внешний носитель информации и т.п. с возложением охранного бремени на их собственников и владельцев, - так и в ранее неизвестном «облачном»

[17] Немыкина О.И. Понятие виртуальности в филосовском контексте // Известия высших учебных заведений. Поволжский регион. Гуманитарные науки. Философия. 2011. № 1 (17). С. 53–62.
[18] Копылов В.А. Информационное право: Учебник. М.: Юристъ, 2002. С. 49–51.

типе хранения, когда информация сохраняется на удаленных физических серверах на стороне провайдера, который обеспечивает и их физическую защиту, и защиту самой информации. *В этой связи регламентация создания виртуальной среды должна осуществляться посредством организационно – правовых мер на уровне локального нормотворчества, а также мер технического характера, связанных с физическим созданием аппаратного комплекса и осуществлением его защиты.*

Информация личностного характера, генерируемая в виртуальной среде организаций, также претерпевает объективные изменения за счет создания ее новых видов, ранее не имеющих аналогов, в связи с чем необходимо с учетом существующей доктрины разрешить вопрос о возможности ее отнесения к категории персональных данных и определить способы защиты. Как правильно указал В.А. Северин, «цифровизация экономики и стремительное развитие информационных технологий неизбежно обусловливает дальнейшее совершенствование правового регулирования оборота личностно-значимой информации, охраняемой в режиме персональных данных»[19]. Базовым нормативным правовым актом, регулирующим отношения, связанные с обработкой персональных данных, является Федеральный Закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[20] (далее по тексту – Закон о персональных данных), согласно которому персональные данные – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[21]. В качестве цели данного Закона определено обеспечение защиты прав и свобод человека и гражданина[22] при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Последние входят в общий объем прав и свобод человека, наряду с достоинством личности, с правом определять и указывать свою

[19] Северин В.А. Правовой институт персональных данных в системе Российского права // Коммерческое право. 2020. № 4 (том 39). С. 36–37.
[20] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 08.08.2024) // СЗ РФ. 31.07.2006. № 31 (часть I). Ст. 3451. (Далее по тексту – Закон о персональных данных).
[21] Пункт 1 статьи 3 Закона о персональных данных.
[22] Глава 2 «Права и свободы человека и гражданина» Конституции РФ. Принята всенародным голосованием 12.12.1993 (с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. // СЗ РФ. 2014. № 31. Ст. 4398.

национальную принадлежность, правом на труд и иными, аналогичными по своей значимости личностными правами. При этом частная жизнь, личная и семейная тайна, которая, к слову сказать, может затрагивать права и интересы всех членов семьи, способны тесно переплетаться с вышеуказанными правами и свободами граждан, например: неправомерные действия по раскрытию личной тайны может негативно отразиться на достоинстве личности, а диагноза – на возможности трудоустройства. Так, С.А.Авакьян предлагает относить к частной жизни «собственно личную жизнь человека; его жизнь в семье; трудовую (в широком смысле слова) деятельность; состояние здоровья; общение человека с другими людьми»[23]. О том, что персональные данные тесно связаны с частной жизнью также считают Л.К. Терещенко и О.И. Тиунов[24]. Одновременно с этим и Конституционный Суд РФ указал, что исключение информации, относящейся к персональным данным, из режима свободного доступа полностью соответствует предписаниям, направленным на защиту права на неприкосновенность частной жизни[25]. В свете вышеизложенного представляется очень верным вывод Ю.С. Телиной о том, что «институт права на неприкосновенность частной жизни состоит из отдельных правомочий лица, каждое из которых требует правовой охраны и защиты. Развитие же общественных отношений в информационной сфере и складывающаяся судебная практика предопределили формирование нового элемента структуры конституционного права на неприкосновенность частной жизни - права на защиту персональных данных»[26]. Одновременно с этим является очень актуальным и верным мнение М.А. Борисова и В.А. Северина: «В виду того, что в настоящее время активно развивается «цифровая экономика» целесообразно понятия «информация о частной жизни гражданина», «личная и семейная тайна» и «персональные данные» не отделять, т.к. в самое ближайшее время характер их

[23] Авакьян С.А. Конституционное право России. Учебный курс: Учеб. пособие: В 2 т. 5-е изд., перераб. и доп. М.: Норма, 2014. Т.1. С. 670.
[24] Терещенко Л.К., Тиунов О.И. Правовой режим персональных данных // Журнал российского права. 2014. № 12. С. 42–49.
[25] Определение Конституционного Суда РФ от 29.09.2011 г. № 1063-О-О // СПС «КонсультантПлюс».
[26] Телина Ю.С. Конституционное право гражданина на неприкосновенность частной жизни, личную и семейную тайну при обработке персональных данных в России и зарубежных странах. автореф.дис. … канд.юрид.наук. Москва. 2016. С. 5.

обработки (базы данных, массивы информации и т.д.) будет максимально унифицирован – фактически это будут единые данные»[27].

Тенденция рассматривать защиту персональных данных как самостоятельное право гражданина, т.е. отдельно от более широкого права на уважение частной и семейной жизни наметилась уже достаточно давно[28]. Одновременно с этим не всякая личностная информация будет являться персональными данными, поскольку для этого необходима определенная совокупность признаков, что непосредственно вытекает из содержания Закона о персональных данных:

- информация должна относиться либо к прямо определенному, либо к косвенно определяемому физическому лицу[29];

- информация передается вышеуказанным субъектом в добровольном порядке[30];

- обработка персональных данных, передаваемых субъектом персональных данных, осуществляется оператором персональных данных[31] в строго установленных им целях[32].

*Таким образом, если информация не отвечает хотя бы одному из вышеозначенных признаков, она не может быть отнесена к категории персональных данных и будет являться просто сведениями из частной жизни гражданина.* Одновременно с этим подобного рода разграничения влияют и на применимое к данным общественным отношениям право – законодательство о персональных данных, со своими четко определенными правами и обязанностями, или Гражданский Кодекс РФ в части регламентации охраны частной жизни гражданина.

---

[27] Борисов М.А., Северин В.А. К вопросу о совершенствовании системы классификации информации в условиях развития цифровой экономики // Пробелы в российском законодательстве. 2019. № 6 С.236.

[28] Терещенко Л.К.:1) О соблюдении баланса интересов при установлении мер защиты персональных данных // Журнал российского права. 2011. № 5. С. 5–12. ; 2) Саушкин С.О., Синцов Г.В. К вопросу о соотношения институтов защиты персональных данных и защиты неприкосновенности частной жизни // Гуманитарный научный вестник. 2020. №2. С. 172–177.

[29] Пункт 1 статьи 3 Закона о персональных данных.

[30] Пункт 1 статьи 9 Закона о персональных данных.

[31] Подпункт 2 пункта 1 статьи 3 Закона о персональных данных.

[32] Пункт 4 статьи 5 Закона о персональных данных.

Регулирование и предоставление адекватной защиты какой-либо информации напрямую связано не только с правильным определением ее статуса, но и со своевременностью совершения данных действий. *Придание какой-либо информации статуса персональных данных обусловлено:*

*- волеизъявлением оператора при определении видов персональных данных, подлежащих обработке, и целей их обработки;*

*- волеизъявлением субъекта персональных данных;*

*- компетентным установлением, посредством нормативного правового акта;*

*- судебным решением.*

Во избежание не только спорных ситуаций, но и с целью эффективного регулирования данных отношений *необходимо на уровне локального нормотворчества хозяйствующей структуры предусмотреть порядок отнесения информации, генерируемой физическими лицами при использовании конкретных технологических решений в виртуальной среде организации, к категории персональных данных, с разделением на виды в зависимости от применяемых технологий.*

Несомненно, технологическое развитие поступательно оказывает существенное влияние на все сферы общественной жизни. Так, еще в конце 19-го века американские юристы Сэмюэль Уоррен и Луис Брандейс, впервые сформулировавшие понятие «privacy» - право быть оставленным в покое или право быть предоставленным самому себе («the right to be alone»), в своей статье «Право на приватность» в Гарвардском правовом журнале они утверждали, что «приватность подвергается опасности со стороны новых изобретений и методов ведения бизнеса, и обосновывали необходимость создания специального «права приватности». С развитием научного и технического прогресса мы все более убеждаемся в справедливости указанных положений»[33]. И если предшествующие эпохи предлагали различные наборы фиксации информации на материальном

[33] Важорова М. А. История возникновения и становления института персональных данных // Государство и право: теория и практика: материалы I Междунар. науч. конф. (г. Челябинск, апрель 2011 г.). Челябинск: Два комсомольца. 2011. С.33-38. URL: https://moluch.ru/conf/law/archive/37/365/ (дата обращения: 17.12.2024).

носителе, будь то камень, пергамент, береста, бумага, то информационное развитие общества естественным образом внесло свои коррективы, выявив необходимость правового регулирования обращения с информацией о человеке, получившей наименование «персональные данные», уже в рамках автоматизации общественных отношений. Так, впервые понятие «персональные данные», означающие любую информацию об определенном или поддающемся определению физическом лице (субъекте данных), нашло свое закрепление в Конвенции 108 Совета Европы о защите прав физических лиц в отношении автоматической обработки персональных данных 1981 года[34]. Целью данной Конвенции являлось обеспечение на территории каждой Стороны для каждого физического лица, независимо от его гражданства или местожительства, уважения его прав и основных свобод и, в частности, его права на неприкосновенность частной жизни в отношении автоматизированной обработки касающихся его персональных данных («защита данных»). При этом под автоматизированной обработкой понимаются операции, осуществляемые полностью или частично с помощью автоматизированных средств.

Современные информационные технологии, под которыми понимаются процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов, ориентированные на решение конкретных прикладных задач обработки информации[35], предлагают не только новые жизненные концепции, но и значительно расширяют круг информации, оставляющей свой след в цифровой среде. Так, например, эпистолярный жанр, наравне с бумажным носителем, в настоящее время в подавляющем большинстве представлен в электронном виде. Возможность виртуального общения посредством мессенджеров позволяет сохранять и накапливать огромное количество информации по сравнению с устным общением. Предпринимательский сектор общества все больше отдает

---

[34] Российская Федерация ратифицировала Конвенцию Федеральным законом от 19.12.2005 № 160-ФЗ с заявлением. Конвенция вступила в силу для Российской Федерации 01.09.2013 // СПС «КонсультантПлюс».

[35] Полякова Т.А., Стрельцов А.А. Организационное и правовое обеспечение информационной безопасности: Учебник и практикум для бакалавриата и магистратуры. М.: Юрайт, 2016. С.17.

предпочтение взаимодействию в виртуальной среде, что значительно повышает экономический эффект деятельности по самым различным компетенциям. Коммуникации между территориально удаленными участниками бизнес-процесса, контроль за их деятельностью и много другое осуществляются с помощью интернета и иных технологий за счет создания локального коммуникативного пространства, что порождает появление достаточно большого множества персональных данных, таких как: аудио и видеозаписи собеседований претендентов на занятие вакантной должности, записи видеоконференций и голосового общения, фотографические и видеоизображения сотрудников в общем корпоративном чате и многое другое. Одновременно с этим программные продукты, ориентированные на современные методы контроля за занятостью в виртуальной среде, каждодневно собирают информацию пользовательского и индивидуального характера, присущего конкретному индивиду. Это различные видеозаписи, скриншоты экранов, записи рабочих столов сотрудников, мониторинг Email, переписки в мессенджерах и соцсетях, данные кейлоггера, фиксирующего все нажатия клавиш на клавиатуре, и многое другое, что в совокупности создает огромную базу персональных данных сотрудников в каждой конкретной организации, хранящуюся в виртуальной среде организаций в цифровом формате. *Таким образом, отличительной чертой рассматриваемой действительности является возможность цифровой фиксации практически всех действий сотрудников, что предполагает совершенствование регулятивного механизма и определение способов защиты подобного рода информации в условиях цифровизации делового сектора*.

Определенного рода технологическая стабильность, характеризуемая длительными промежутками времени между созданием и введением в эксплуатацию технических новшеств, уходит далеко в прошлое. Современной же действительности в области высоких технологий характерно значительное ускорение процесса создания и внедрения новейших цифровых решений, способных привносить кардинальные перемены в привычный жизненный уклад. На этом фоне особенно четко проявляется инертность правотворчества и ее

неспособность «успеть» за изменяющейся конъюнктурой общественных отношений в рассматриваемой области. Существующие нормативные правовые акты зачастую уже сложно применимы ко всему многообразию в сфере информационных отношений. *Все ускоряющейся процесс цифровизации требует применения более мобильных средств правового регулирования, которыми необходимо признать локальные нормативные акты, актуальные и эффективные средства быстрого реагирования на любые запросы и вызовы, возникающие при обработке персональных данных в виртуальной среде организаций.*

Поскольку речь идет о виртуальной среде организации, а также о локальных нормативных актах, то будучи исполненными в цифровом формате, последние по аналогии с нормативными правовыми актами должны быть в обязательном порядке размещены для ознакомления в ее информационном пространстве. В противном случае они не будут затрагивать права и обязанности лиц, получивших доступ к информации в виртуальной среде организации. *В обязательном порядке надлежит разработать механизм ознакомления сотрудников организации с вышеуказанными актами именно в виртуальной среде организаций и технического исполнения фиксации данного факта.*

Основной субъектный состав рассматриваемых правоотношений на законодательном уровне представлен субъектом персональных данных и оператором, осуществляющим их обработку. Именно между последними на основе юридических фактов возникают субъективные права и юридические обязанности, в частности обязанность по защите персональных данных, которая возлагается непосредственно на оператора. Если еще до недавнего времени позиционировалось, что только строго определенные сотрудники хозяйствующей структуры могли получить доступ к информации конфиденциального характера и это никак не отражалось на экономическом результате и не тормозило целевую деятельность, то 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. Все эти необратимые и перманентно усложняющиеся отношения существенно снижают уровень информационной безопасности на фоне подчас невозможности для организации осуществления контрольных функций. При этом законодательного установления о том, что лицо, получившее доступ к информации конфиденциального характера, не вправе разглашать ее содержание третьим лицам без получения на то согласия субъекта персональных данных уже явно недостаточно, и оно не учитывает всего разнообразия данных отношений, нуждающегося в правовом регулировании. В этой связи исходная база правового регулирования обработки и защиты персональных данных применительно к виртуальной среде организаций объективно нуждается в адаптации к таким условиям за счет выработки новой модели поведения, которой должны следовать сотрудники, получившие доступ к информации конфиденциального характера. Основу данной конструкции должно составлять правосознание, служащее саморегулятором поведения человека в результате осознания последним правовой действительность, а также культура информационной безопасности. Так, Ф.А. Абаевым обязательства работников, непосредственно осуществляющих обработку персональных данных, также представлены как часть комплекса мер по защите персональных данных работников в организации[36].

*Получение сотрудниками вышеуказанных преференций неминуемо влечет за собой возложение на последних дополнительных обязанностей, связанных с защитой информации конфиденциального характера, а также разделение зон ответственности и определение мер воздействия в случае нарушения информационной безопасности.*

В практической деятельности организаций получило широкое распространение одновременная обработка одних и тех же персональных данных, включая и сведения, характеризующие физиологические особенности человека, принадлежащих сотрудникам разных хозяйствующих субъектов, например:

[36] Абаев Ф.А. Правовое регулирование отношений по защите персональных данных работника в трудовом праве: автореф. дис. … канд.юрид.наук. Москва, 2014. С.9

видеозаписи переговорных процессов, переписка в чатах, созданных с определенной целью, голосовые сообщения, размещение общих фотографических снимков и иная информация, фиксируемая в цифровом формате. *Таким образом, имеет место факт совместного владения вышеуказанной информацией несколькими организациями, которые являются операторами персональных данных, но при этом права и обязанности сторон, совместно создающих и, соответственно, совместно владеющих данной информацией, на уровне нормативно-правового регулирования предметно не установлены, в связи с чем целесообразно предусмотреть на уровне законодательного регулирования данный вид договора и разработать его условия.* Одновременно с этим дуализм рассматриваемой ситуации проявляется и в необходимости соблюдения прав самих субъектов персональных данных способами и в порядке, уже предусмотренными в законодательстве. Так, последние вправе требовать от оператора персональных данных, т.е. от организации прекращения обработки и уничтожения их персональных данных, сохраняемых в цифровом формате, что может идти не только вразрез с потребностям организации, но и создать угрозу нарушения договорных обязательств сторон по определению порядка совместного владения и пользования информацией.

*В целях преодоления подобного рода коллизий предлагается на уровне локального регулирования предусматривать возможность закрепления за организацией правового статуса обладателя информации, возникновение которого обусловлено либо фактом создания информации, либо получением на основании закона или договора права разрешать или ограничивать доступ к ней.*

При этом всем обладателям информации, если иное не предусмотрено федеральными законами, предоставляются следующие права[37]:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

---

[37] Статья 6 Федерального закона от 27.07.2006 № 149-ФЗ (ред. 22.06.2024) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 31.07.2006. № 31 (часть I). Ст.3448. (Далее по тексту – Закон об информации).

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Таким образом, при заключении с субъектом персональных данных договора, предоставляющего организации права разрешать или ограничивать доступ к персональным данным, последний наряду со статусом обладателя информации приобретает и вышеуказанные права. При этом на весь период действия договора подлежит распространению мораторий на осуществление субъектом персональных данных прав на отзыв согласия на обработку персональных данных и некоторых иных прав, предусмотренных законодательством о персональных данных. Все взаимоотношения сторон подлежат рассмотрению в соответствии с условиями договора. *В этой связи целесообразно предусмотреть в нормах действующего законодательства данный вид договора и разработать его условия.*

Одновременно с этим за счет применения предлагаемой правовой конструкции возможно на уровне легального допущения расширить горизонт возможностей по использованию информации, поскольку персональные данные поведенческого, предпочтительного и иного индивидуализирующего характера являются крайне востребованы как в целях достижения более положительного экономического эффекта, так и в целях развития научного, социального и им подобного потенциала.

Одним из основных признаков, наличие которого позволяет относить ту или иную информацию к категории персональных данных, является их добровольная передача оператору персональных данных, посредством выражения согласия на их обработку в установленной законодательством форме. Добровольность передачи

физическим лицом своих персональных данных является составляющей доктрины понимания персональных данных, согласно которой сведения о личности включаются в информационную систему различного рода отношений по инициативе граждан или в силу закона[38]. Саму же информацию персонального характера следует разделить на два вида – ту, которая уже сформирована и является известной для субъекта, например: паспортные данные, ИНН, СНИЛС, дата рождения, данные диплома об образовании и многое другое, что абсолютно понятно и не вызывает вопросов, - и ту, содержание которой уже совершенно не очевидно, и которая только будет создаваться в процессе осуществления сотрудником своей профессиональной деятельности. *Таким образом, субъект дает согласие на обработку его персональных данных, создаваемых в будущем, в связи с чем он не может находиться в неведении относительно обстоятельств создания персональных данных, что подразумевает обязательность ознакомления последнего со всеми технологиями и сервисами, используемыми организацией, включая и виртуальную среду.*

Одновременно с этим следует признать наличие неравенства положения между работниками, заключившими трудовой договор, и иными лицами, сотрудничающими с организацией по гражданско-правовым договорам, например: фрилансерами, персональные данные которых обрабатываются наравне с работниками последней. Так, защита персональных данных работников, включая исчерпывающие цели их обработки (содействие в трудоустройстве, продвижение по службе, обеспечение личной безопасности работника, контроля количества и качества выполняемой работы и обеспечение сохранности имущества), урегулированы положениями главы 14 Трудового Кодекса РФ[39], в то время как к иным лицам, работающим по гражданско-правовым договорам, положения данного акта кодификации уже не применимы, в связи с чем руководствоваться следует Законом о персональных данных, что предполагает возможность обработки последних в более широких целевых масштабах. Незначительно, но все же разнятся

[38] Бачило И.Л. Информационное право. М.: Издательство Юрайт, 2013. С. 124.
[39] Трудовой Кодекс РФ от 30.12.2001 № 197-ФЗ // СЗ РФ. 07.01.2002. № 1 (часть I). Ст. 3. (Далее по тексту – ТК РФ).

и права субъектов персональных данных, а также способы защиты нарушенных прав в части правового обоснования исковых требований. Таким образом, при прочих равных условиях статус субъектов персональных данных на настоящий момент не предусматривает единого законодательного подхода к правовому регулированию и защите персональных данных в виртуальной среде организаций, что не является ни рациональным, ни полезным с точки зрения правоприменения. *В этой связи необходимо выработать единый подход к данной проблеме, где во главу надлежит поставить не статус субъекта персональных данных, а факт обработки персональных данных в виртуальной среде организации, как специальный признак для единого подхода в правоприменении, а также предусмотреть для всех вышеуказанных субъектов равные права для защиты персональных данных в виртуальной среде организации.*

Вступление в любые взаимоотношения в виртуальном пространстве неминуемо сопряжено с обязательным установлением личности субъекта, где достоверность является основным приоритетом. Базовое понятие «установление личности» в действующем законодательстве отсутствует, в связи с чем для осознания его содержания возможно сослаться на положения статьи 42 Основ законодательства о нотариате[40], согласно которой установление личности гражданина должно производиться на основании паспорта или других документов, исключающих любые сомнения относительно его личности. Введение дистанционной занятости в области трудового права, совершение иных значимых действий в виртуальном пространстве в режиме онлайн, особенно актуализировало затронутую проблему. Существующие способы удостоверения личности посредством предъявления документа в электронной форме[41], на практике в виде электронного образа документа, когда последний, исполненный на бумажном носителе, преобразуется в электронный посредством сканирования или ксерокопирования, тем не менее не исключает рисков подмены. Что же касается оформление взаимоотношений на основании гражданско-правового договора, то

[40] Основы законодательства РФ о нотариате от 11.02.1993 № 4462-I (ред. от 12.12.2023). «Российская газета» от 13.03.1993. (Далее по тексту – Основы законодательства РФ о нотариате).
[41] Статья 312.2 ТК РФ.

вопрос о том, каким образом происходит установление личности контрагента в виртуальной среде организации никак не урегулирован, тем не менее не исключается использования электронного образца документа по аналогии с трудовым законодательством, когда изображение лица на экране монитора сравнивается со сканированной копией, например, паспорта.

При этом современные технологии уже достаточно давно позволяют устанавливать личность граждан с помощью биометрии, что в силу индивидуальных и неповторяющихся особенностей каждого субъекта способно полностью исключить ошибки идентификации, связанные с человеческим фактором. На настоящий момент на территории Российской Федерации создана и действует Единая биометрическая система (ЕБС) со статусом государственной информационной системы (ГИС)[42], что позиционируется как наивысшая степень защищенности биометрических персональных данных. Идентификация и (или) аутентификации физического лица с использованием ЕБС приравниваются к действиям по предъявлению документов, удостоверяющих его личность. Организации и индивидуальные предприниматели наряду с государственными органами, органами местного самоуправления, организациями финансового рынка, нотариусами поименованы в качестве пользователей ЕБС, но на практике возможность удостоверения личности с использованием ЕБС доступна не всем, что обусловлено объективными причинами. Так, для использования системы необходимо провести интеграцию с ЕБС за счет установки технологического оборудования, а также программного обеспечения, которые должны соответствовать строго установленным критериям защищенности и информационной безопасности. В некоторых случаях требуется пройти аккредитацию по целому ряду критериев, что в совокупности довольно серьезно сужает круг лиц, имеющих реальную возможность осуществить подобную интеграцию. Именно по этой причине, а также в связи с тем, что создание

[42] 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»» // СЗ РФ. 02.01.2023. № 1 (часть I). Ст. 19.

коммерческих биометрических систем (КБС) не предусмотрено, набирают популярность и пользуются спросом иные технологии, позволяющие устанавливать личность человека без выделения биометрических дескрипторов[43] и, соответственно, без обращения к ЕБС, или подтверждать персональные данные (ПЦД ПД)[44] при обращении к различным сервисам без раскрытия их содержания. При этом в среде разработчиков подобные технологии именуются как небиометрическая сверка лиц, что очень точно определяет направление их развития в рассматриваемой области в качестве альтернативы биометрии, применение которой на настоящий момент имеет определенного рода особенности. *Широкая востребованность подобных технологий в совокупности с вышеизложенными обстоятельствами требует законодательной регламентации и введения в имеющийся понятийный аппарат соответствующего определения, характеризующего нарождающееся направление в области сверки данных о личности человека в режиме дистанционного доступа без применения биометрических шаблонов.*

***Таким образом, концепция совершенствования правового механизма регулирования и защиты персональных данных в виртуальной среде организаций предполагает:***

*- определение порядка создания виртуальной среды организации посредством организационно – правовых мер, а также мер технического характера;*

*- четкое разграничение персональных данных от иной личностной информации посредством признаковой идентификации;*

*- установление на уровне локального нормотворчества порядка отнесения информации, генерируемой физическими лицами при использовании конкретных технологических решений в виртуальной среде организации, к категории персональных данных с разделением на виды в зависимости от применяемых технологий;*

[43] URL: https://smartengines.ru/face-verification/
[44] URL: https://public.kryptonite.ru/PTsD_PD_presentation.pdf

*- предусмотреть локальные акты в системе координат правового регулирования и защиты персональных данных в виртуальной среде организаций;*

*- разработать механизм размещения локальных нормативных актов, исполненных в цифровом формате, в информационном пространстве организации;*

*- разработать механизм ознакомления сотрудников организации и иных лиц с вышеуказанными актами в виртуальной среде организаций с возможностью технической фиксацией данного факта.*

*- предусмотреть возможность установления договорных отношений между организациями, совместно создающими, использующими и хранящими персональные данные каждая в своей виртуальной среде, с определением существенных условий такой договорной конструкции, прав и обязанностей сторон, порядка расторжения договора, ответственности за нарушение условий сохранения конфиденциального характера информации и иных условий;*

*- предусмотреть возможность установления договорных отношений между субъектом персональных данных и иным лицом с целью наделения последнего правом разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам, а также определить существенные условия договора, права и обязанности сторон, порядок расторжения договора, ответственность сторон за нарушение условий сохранения конфиденциального характера информации и иных условий;*

*- поименовать отдельно в качестве субъектов правоотношений по обработке и защите персональных данных в виртуальной среде организаций лиц, получающих доступ к данной информации конфиденциального характера в силу производственной необходимости, с определением их прав и обязанностей, а также разработать модель поведения, основанную на ответственном отношении и самоконтроле каждого сотрудника, получившего доступ к вышеуказанной информации;*

*- выработать единый подход к обработке персональных данных в виртуальной среде организаций, основанный на главенстве факта обработки данной информации, как специального признака, а не субъекта персональных*

*данных, а также предусмотреть для всех субъектов, коммуницирующих в виртуальном пространстве, равные права для защиты их персональных данных в изучаемой среде организации;*

*- регламентировать порядок применения небиометрических технологий, позволяющих устанавливать личность в виртуальном пространстве без обращения к ЕБС, а также технологий подтверждения персональных данных посредством обращения к различным сервисам.*

## § 2. Эволюция развития правового регулирования и защиты персональных данных в Российской Федерации

Информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу, которую в настоящее время именуют персональными данными, существует и используется с давних времен. Одновременно с этим регулирование и защита информации персонального характера также имеет длительную историю развития. Изучение отечественного правового наследия в данной области позволило выявить определенные закономерности в развитии правового института персональных данных, что оказало положительное влияние на понимание общих тенденций, которые сохраняют свою актуальность и по сей день, при переходе общественных отношений к информатизации и цифровой экономике.

Так, любое технологическое развитие общества порождает возникновение не только новой информации о человеке, но и ранее не известной формы ее фиксации, например, изначально изображение человека существовало в виде портрета, в дальнейшем появились технологии дагерротипа - прототип фотоснимка, фотографии, ксерокопии, видеоизображения и, как итог, на современный момент – цифрового формата, способных к быстрому и неограниченному масштабированию, в отличие от рукописного изображения. Возможность сохранения информации в неизменном виде позволяет извлекать различного рода полезные результаты, что по мере развития общества увеличивает не только ее ценностные характеристики и сам их масштаб, но и области применения. Вышеуказанные изменения влекут за собой создание более совершенного механизма защиты как самой информации, так и ее носителей, что обусловлено возрастанием негативных последствий в случае ее нарушения или преодоления. Одновременно с этим глубина регулирования и защиты информации персонального характера, предоставляемой на уровне законодательного установления, напрямую зависит от степени признания в обществе тех или иных ценностей, напрямую связанных с неприкосновенностью

частной жизни, вплоть до их практически полного отрицания, что будет наглядно проиллюстрировано на дореволюционном, советском и постсоветском периодах развития нашего государства.

При этом, как показало проведенное исследование, с появлением новой виртуальной среды существования информации рассматриваемые тенденции и закономерности развития регулирования и защиты личностной информации нисколько не изменились, что позволило использовать полученные результаты при выработке механизма правового регулирования и защиты персональных данных в виртуальной среде организаций.

Как указывалось ранее в диссертационном исследовании, зарождение такой юридической категории как «право на неприкосновенность частной сферы» произошло в США в конце 19-го века. При этом отечественное законодательство к этому моменту уже имело достаточное количество нормативных правовых актов, регламентирующих порядок оборота информации частного характера, а также их защиты. Но, как совершенно верно отмечено А.В. Майоровым и Е.Н. Попериной, «развитие прав человека в России шло по особому пути»[45]. Таким образом, *в России существование сферы частных интересов в той или иной степени признавалось задолго до момента ее формирования в качестве отдельной правовой категории.* Так, одно из первых упоминаний о персональных данных на уровне законодательного установления относится ко времени Московского церковного собора 1666-1667 годов, получившего название Никоновского церковного собора, которым предписано ведение метрических книг, предназначавшихся для внесения записей о рождении, о совершающихся браках и о смерти. По факту велись данные записи не всеми обязанными лицами и не на регулярной основе. Впоследствии в 1702 году Петр I издает Указ «О подаче в Патриарший духовный приказ приходским священникам недельных ведомостей о родившихся и умерших»[46], в соответствии с которым уже все приходские священники, правда на тот период только города

[45] Майоров А.В., Поперина Е.Н. Формирование и развитие права на неприкосновенность частной жизни // Юридическая наука и правоохранительная практика. 2012. № 3 (21). С.35.
[46] Полное собрание законов Российской империи (далее ПСЗ)-I. Т. IV. № 1908 // СПС «КонсультантПлюс».

Москвы, должны были вести в метрических книгах письменный учет всех родившихся, умерших и вступивших в брак в возглавляемом им приходе и передавать данные сведения в патриарший приказ. Прибавления к Духовному Регламенту[47], утвержденные Петром I в 1722 году, предписывают уже повсеместное ведение метрических книг[48]. Церковный метрический учет велся вплоть до его отмены в 1918 года, когда данная функция была передана иным светским органам. Метрики о рождении, о браке и о смерти содержали следующий обязательный «набор» персональных данных: имя, дата рождения и крещения; имена родителей; возраст; вероисповедание; место жительства; национальность; сословная принадлежность; дата венчания; дата и причина смерти; место захоронения. Помимо метрических книг персональные данные содержались и в ревизских сказках - аналог современной переписи населения, где поименно перечислялись все члены семьи с указанием возраста, даты смерти, если таковая имела место быть в периоды между переписями, факта отдачи в рекруты, перевода на другое место жительства. *Применительно к современному понятийному аппарату виды персональных данных, подлежащих обработке (сбор, хранение, использование), а также операторы персональных данных (лица и структуры, ответственные за совершение вышеуказанных действий), определялись на уровне законодательного закрепления, что имеет место и по сей день. Таким образом, в этой части прослеживается преемственность механизма правового регулирования оборота и защиты информации личностного (частного) характера посредством законодательного установления.*

Целью такого учета являлась экономическая, статистическая и правовая упорядоченность во всех сферах жизни. Например, на основании данных метрического учета и ревизских сказок устанавливалась численность податного населения, что позволяло рассчитывать размер платежей в казну как всего государства, так и отдельно взятого помещика, владельца крепостных крестьян.

---

[47] ПСЗ-1. Т. XX. № 14948. С. 883 // СПС «КонсультантПлюс».

[48] Камалова Г.Г. История охраны конфиденциальности сведений в России // Диалог со временем. 2019. Выпуск 66. С. 336–345.

Данные по учету населения применялись также при формировании рекрутских наборов, для изучения демографического, миграционного и иных процессов. Безусловно, сфера применения вышеуказанных данных была значительно шире, поскольку их информационный потенциал довольно велик и охватывал собой не только государственные нужды, но и частноправовые отношения. Что же касается правовой функции, то и государство, и частные лица в целях идентификации всегда были заинтересованы в наличии достоверных и полных сведений персонального характера. Так на основании данных метрического учета устанавливались различные факты, имеющие правовое значение, например достижение возраста, допустимого для вступления в брак или для отдачи в рекруты; установление родства для вступления в наследство или для доказывания законности рождения и многое другое. Ярким примером могут служить «мертвые души», которые скупал Павел Иванович Чичиков[49]. Ведь это ничто иное, как персональные данные умерших крестьян, которые до момента очередной ревизии числились как живые.

По совокупности данных факторов государство уже и в те времена осуществляло защиту персональных данных на законодательном уровне как для сохранности и защиты от подделок материального носителя этой информации и исключения фальсификации, так и в известной степени с целью соблюдения конфиденциальности информации и прав личности, что является актуальным и в наше время, поскольку целью Закона о персональных данных является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Так, для того чтобы избежать фальсификации и утраты метрических книг последние велись в двух экземплярах, из которых один, приходской, хранился в церковной ризнице, а второй передавался в органы епархиального управления – духовные консистории. Впоследствии метрические книги изготавливались типографским способом с водяными знаками и

[49] Гоголь Н.В. Мертвые души. М.: Азбука. 2024. 352 с.

филигранью. Также в церквях были заведены печати, которыми метрические книги опечатывались[50]. Одновременно с этим были установлены и общие предписания для хранение метрических книг, исключающие возможность доступа в ним лиц, не имеющих на то соответствующего разрешения. Своим Указом от 17 мая 1802 года[51] Синод ввел персональную ответственность священников за каждую запись в метрической книге посредством указания на фамилию того, кто совершал требу. Таким образом, *отнесение персональных данных к категории информации ограниченного доступа не является чем-то новым, а представляет собой логическое продолжение изначально выработанной политики государства в области рассматриваемых отношений.* Интересным представляется и тот факт, что *вышеуказанные меры нашли свое практически полное воплощение в положениях Закона о персональных данных, согласно которому оператор при обработке персональных данных обязан принимать необходимые меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных*[52], что также свидетельствует в пользу преемственности методов правового регулирования и защиты информации персонального характера.

Первый акт кодификации уголовной отрасли права в истории России был подписан Императором Николаем I в 1845 года и введен в действие в 1846 году[53]. Назывался он Уложением о наказаниях уголовных и исправительных (далее по тексту – Уложение 1846 года). Статьей 1912 данного Уложения предусматривалась ответственность «за всякий какого-либо рода подлог в актах о рождении, бракосочетании или смерти, как подлинных, так и в выдаваемых засвидетельствованных копиях сих актов». «За означение родившихся,

---

[50] Антонов, Д.Н., Антонова И.А. Метрические книги России XVIII - начала XX в. М., 2006. С. 52.
[51] ПСЗ I. Т. XL. Общее приложение к собранию. К Т. XXVII. № 20266а // СПС «КонсультантПлюс».
[52] Пункт 1 статьи 19 Закона о персональных данных.
[53] Уложение о наказаниях уголовных и исправительных. Санкт-Петербург: Тип. 2 отделения собств. Е.И.В. канцелярии, 1845. - [4], IV, 898, XVII. С. 32.

сочетавшихся браком и умерших в метрических книгах не непосредственно после исправления относящихся к каждому случаю духовных треб, а по проистечении времени, более или менее продолжительного, на память, или по показаниям семейств, или по каким-либо отдельным запискам и вообще за неисправное ведение метрических книг, исповедных росписей и обыскных книг, а равно и за хранение оных не в самой церкви и за неотсылку их куда следует в свое время, виновные священно- и церковно-служители» подвергались наказанию в соответствии с положениями статьи 1913 вышеуказанного Уложения. Таким образом, с 1846 года лица, виновные в нарушении обязанности по охране материальных носителей персональных данных о рождении, бракосочетании, смерти и, соответственно, защите самих этих персональных данных, а также по их исправному ведению подлежали уже уголовному преследованию, в отличие от более раннего периода, когда таковую ответственность можно было отнести к категории дисциплинарной. При этом любое ужесточение наказания преследует строго определенную цель - минимизировать возможность совершения правонарушения в какой-либо области общественных отношений под страхом привлечения к более серьезному виду ответственности. *Применительно к рассматриваемым обстоятельствам данный факт следует расценивать как повышение степени значимости персональных данных в информационной системе государства.*

Известны нашей ранней истории и документы, удостоверяющие личность владельца с учетом его биометрических персональных данных[54], сведений, которые характеризуют физиологические особенности человека, на основании которых можно установить его личность и которые используются для этого. Как один из примеров можно привести Указ Петра I, изданный 6 июня 1724 года, «Плакат о зборе подушном и протчем»[55], который позволил крестьянам временно отлучаться со своего места жительства для заработка или по каким-либо иным

[54] Галиуллина Д.Р. История развития биометрических документов в России // Вестник науки и образования. 2015. № 9 (11). С. 42–43.

[55] Байбурин А.К. К антропологии документа: паспортная «личность» в России // Антропология социальных перемен. Сборник статей к 70-летию В.А.Тишкова. М., 2011. С. 533–555.

делам. Крестьянам выдавался соответствующий документ – «покормежное письмо», или «пропускное», где указывались не только имя, возраст, место жительство крестьянина, но и описывалась его внешность с учетом характерных примет: «а для предосторожности в тех пропускных письмах описывать того, кто отпущен будет, рост, лицо, и неприменныя приметы, дабы кто другои воровати получа оное не волгался». Небезынтересно и Циркулярное предложение министра народного просвещения попечителям учебных округов от 3 ноября 1879 года № 12074[56], где предусмотрено, что «в целях предупреждения попыток выдержать испытание на звание аптекарского ученика посредством подставного лица, возбуждено было ходатайство о разрешении применять к лицам, желающим подвергнуться сему испытанию, следующие предосторожности: требовать от экзаменующегося, кроме документов, представления и фотографической своей карточки». Данная карточка впоследствии прикреплялась надлежащим образом к аттестационному документу и заверялась печатью. *Таким образом, информация о физиологических особенностях человека, именуемая в настоящее время биометрическими персональными данными, имела хождение и использовалась в целях индивидуализации личности достаточно давно, постоянно модернизируясь с появлением новых технических изобретений.*

26 апреля 1715 года Петром I издается Артикул воинский[57], где в главе 18 «О поносительных письмах бранных и ругательных словах», в Артикуле 149 значилось: «Кто паскивли, или ругательныя письма тайно сочинит, прибьет и распространит, и тако кому непристойным образом какую страсть или зло причтет, чрез что его доброму имени некакой стыд причинен быть может, онаго надлежит наказать таким наказанием, каковою страстию он обруганного хотел обвинить». Здесь мы можем видеть попытку узаконения возможности

[56] Аптекарский Устав. Раздел Б. «История фармацевтического сословия». Стр. XXXIII. Извлеченный из Свода законов полных собраний законов, распубликованных циркуляров Министерства внутренних дел, постановлений Медицинского совета и разъясняемый историей законодательства / [соч.] Н. Варадинова, д-ра прав и философии, чл. С.-Петерб. и Венского фармацевтического и других ученых обществ. С.-Петербург: Тип. М-ва вн. дел, 1880. - 12, LXX. Место хранения оригинала: РГБ. [Электронный ресурс]. htpps://www.prlib.ru> item (дата обращения: 23.12.2024). ; Там же. Раздел А. «Права и обязанности фармацевтов». С. 13. Свод законов. Т.III. Устав врачебный. Раздел А. «Ученые степени и звания».

[57] Российское законодательство X-XX вв.: в 9 т. Т.4. Законодательство периода становления абсолютизма / Отв. ред. А.Г.Маньков. М., Юридическая литература. 1986. С. 354.

привлечения к ответственности пасквилянта, который указанным в Артикуле способом разгласил какую-либо информацию о потерпевшем, включая и так называемую информацию конфиденциального характера, что явно обозначает данную проблему как значимую, поскольку она нашла свое решение в комплексе предпринятых государственных реформ.

В 1813 году «Комиссией составления законов» под руководством Сперанского был подготовлен Проект уголовного уложения Российской Империи[58], который все же так и не был принят. Но это была первая в истории попытка кодифицировать нормы уголовной отрасли права. В текст Проекта было включено две статьи, законодательно закрепляющие ответственность за разглашение профессиональной тайны и за чтение чужих писем[59], что свидетельствовало о наличии запроса общества на государственную защиту частной жизни. Так, согласно § 466 «Когда те, коим по должности их или ремеслу, например: врачи, повивальные бабки и проч., вверенные или известные происшествия, могущие причинить стыд и бесчестье другим или несогласие в семействах, откроют оные; то таковых за открытие (исключая случаи, где закон именно повелевает открывать) наказывать с отрешением от должности и с запрещением ремесла и привилегий и лишением свободы». Параграфом 467 было предусмотрено, что «Тому же наказанию (§ 466) и на таковом же основании подвергается распечатывающий или истребляющий чужие письма с намерением нанести вред или бесчестье другому».

Несмотря на это, попытка узаконить право на защиту частной жизни была все же реализована в Уложении 1846 года, когда впервые в истории России была введена и законодательно регламентирована тайна переписки, а также ответственность за разглашение профессиональной тайны[60]. Так, статьей 1528 предусмотрена ответственность почтового чиновника, почтальона или иного

[58] РГИА Ф. 1251 Оп. 1, часть 1 Д. 10.
[59] Безверхов А.Г., Коростелев В.С. «Проект уголовного уложения Российской Империи 1813 года», утв. редакционно-издательским советом Самарского государственного Университета в качестве монографии, изд. «Самарский университет». 2013.
[60] Кадников Б.Н. О становлении и развитии законодательства об охране частной жизни // Общество и право. 2016. № 2 (56). С. 30–33.

служителя почты, которые «не по неосторожности, а с какой-либо целью передавал кому-либо письма, адресованных на имя другого, без разрешения последнего». Статьей 1530 предусмотрено наказание «не только за распечатывание, хотя бы из одного только любопытства, отданного для отправления с почтою или полученного по почте письма, но и за сообщение содержания письма кому – либо другому». Разглашение сведений, являющихся профессиональной тайной, например врачебной, адвокатской каралось статьей 2019 Уложения 1846 года, согласно которой «тот, кто хотя не дозволяя себе настоящей клеветы, но с намерением оскорбить честь какого-либо лица или повредить оному, распространит такое сведение, которое было ему сообщено, по знанию его или особой к нему доверенности, с обещанием сохранять его в тайне, подлежит наказанию». Но при этом в Уложении 1846 года предусмотрены и ограничения абсолютной врачебной тайны, которые предусматривают для всех категорий врачей наказание за несообщение полиции о выявлении «всякой повальной и прилипчивой болезни» (статья 1029 Уложения), о рождении «странных и необыкновенных уродах» (статья 1092 Уложения). Впоследствии Врачебным Уставом 1857 года[61] данный перечень был расширен за счет добавления дополнительных заболеваний, как правило могущих повлечь массовое заражение. *Здесь можно наблюдать некую параллель с положениями Закона о персональных данных[62], согласно которым защита жизни, здоровья или иных жизненно важных интересов других лиц поставлено в приоритет над соблюдением прав субъекта персональных данных, связанных с санкционированием последним совершения каких-либо действий с его персональными данными*. Имелась в Уложении 1846 года и статья 450, согласно которой подвергались уголовному преследованию чиновники, которые «разглашали посторонним дела или сообщения, бумаги, вверенные последним по службе, в случае если от вышеуказанных действий распространится молва, для чьей-либо чести оскорбительная». *Как можно видеть из вышеизложенного*

[61] Энциклопедический словарь Брокгауза и Ефрона. т.VII (1892). С. 344 // СПС «КонсультантПлюс».
[62] Подпункт 3 пункта 2 статьи 10 Закона о персональных данных.

*речь идет о некоем подобии служебной и профессиональной тайны, правила поведения в отношении которой актуальны и в настоящее время, поскольку Законом о персональных данных предусмотрено, что операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных*[63]. Единожды введенный особый охранный статус информации конфиденциального характера более никогда не терял своей актуальности и последовательно развивался во вновь принимаемых законодательных актах вместе с технологическим развитием общества. Так, изобретение телеграфа повлекло за собой принятие в 1857 году Устава Телеграфического[64], где в пункте 55 содержалось предписание о том, что «Все без исключения депеши и все, что только касается телеграфа, в каком бы то ни было отношении, сохранять в совершенной тайне и никому и никогда и ни в каком случае не объявлять; равно не открывать, кем и к кому депеша подана, а также не оставлять депеш так, чтобы кто-либо из посторонних мог оные видеть». Аналогичное положение содержал и Устав Телеграфный 1876 года[65], где в статье 8 говорилось, что «содержание телеграммы, составляя тайну отправителя и получателя, никому постороннему не сообщается. Равномерно не открывается и того, кем и к кому телеграмма подана».

В 1864 году принимается Устав о наказаниях[66], налагаемых мировыми судьями, где статьей 137 предусматривалась ответственность «за разглашение, с намерением оскорбить чью-либо честь, сведений, сообщенными втайне или же узнанных вскрытием чужого письма или другим противозаконным образом». В 1885 году выходит в свет новое Уложение о наказаниях уголовных и исправительных[67], заменившее собой предыдущее Уложение 1846 года и Устав о

---

[63] Статья 7 Закона о персональных данных.
[64] Свод законов Российской Империи. 1857. Типография Второго Отделения Собственной Е.И.В. Канцелярии. т.12, часть 1, тетрадь 3, Ст. 11.
[65] Типография Второго Отделения Собственной Е.И.В. Канцелярии, 1876. С. 4.
[66] Судебные Уставы 20 ноября 1864 года, с изложением рассуждений, на коих они основаны. 1866. СПб. Часть первая, Стр. III-IV.
[67] Уложение о наказаниях уголовных и исправительных 1885 года / издано проф. Ипм.Училища правоведения… Н.С. Таганцевым. 5-е изд., доп. Санкт-Петербург: тип. М.Стасюлевича, 1886. С.714.

наказаниях, налагаемых мировыми судьями. В общем и целом данный Устав сохранил все нормы, связанные с наказанием за небрежное ведение метрических книг (статья 1442), за распечатывание писем (статья 1104). Но при этом появились некоторые интересные новшества, касающиеся защиты информации о частном лице. Так, согласно положениям статьи 1039 Уложения «За всякое оглашение в печати о частном или должностном лице, или обществе, или установлении, такого обстоятельства, которое может повредить их чести, достоинству или доброму имени» (отличие от ст.1535 «клевета, состоящая в несправедливом обвинении кого-либо в деянии, противным правилам чести» и в отличие от ст.1040 «оскорбительные отзывы, заключающие злословие или брань без указания позорящего обстоятельства»). В пункте 15 примечания к статье 1039 содержится комментарий о том, что «ответственность за оскорбление, указанное в статьях 1039 и 1040, вовсе не требуют чтобы лица оскорбленные были названы по имени; для применения ее достаточно таких указаний, по которым бы вполне можно было определить о ком идет речь в данной статье». *Таким образом, современное определение персональных данных – «информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу» - отнюдь не является законодательной новеллой, поскольку правовое содержание понятия «косвенно определяемое физическое лицо» было известно отечественной юриспруденции уже на рубеже 19-20 веков.*

Уголовное Уложение 1903 года[68] представляло собой более усовершенствованный и проработанный документ, вобравший в себя весь предыдущий опыт и современные на тот момент реалии. Так, в главе 28 «Об оскорблении» содержались две статьи: статья 531, предусматривающая наказание за «опозорение разглашением, хотя бы в отсутствие опозоренного, обстоятельства, его позорящего», и статья 533, согласно которой подлежал ответственности виновный в оскорблении в распространенных или публично выставленных произведении печати, письме или изображении. Сверх того,

[68] Новое Уголовное Уложение, высочайше утвержденное 22 марта 1903 года. СПб.: Изд. В.П.Анисимова.1903. С. 250.

наказанию подлежал и редактор или издатель повременного издания, виновный «в помещении в оном оскорбительных произведений, писем или изображений». Глава 29 «Об оглашении тайн» содержала три статьи на рассматриваемую тему. Статья 541 предусматривала ответственность за разглашение профессиональной тайны, поскольку речь шла о лицах, обязанных по своему званию хранить в тайне доверенные им сведения. Таковыми лицами могли быть адвокаты, врачи, следователи, духовники. Статья 542 предусматривала ответственность «за самовольное вскрытие заведомо чужих письма, депеши или иной бумаги при условии, что виновный огласил заключавшееся в скрытых им бумагах сведение, могущее опозорить лицо, к коему оно относилось». «Умышленное оглашение состоящим на службе в кредитном установлении, акционерном обществе или банкирском заведении сведений о кредитах частных лиц, доверившим оным свое имущество или имущественный интерес», каралось в соответствии со статьей 544 Уголовного Уложения.

20 июля 1914 года, в связи с началом Первой мировой войны было утверждено Временное положение о военной цензуре[69], в соответствии со статьей 2 которого военной цензуре подлежали почтовые отправления и телеграммы. При этом статьей 30 данного Положения предусмотрено, что «сведения, полученные должностными лицами военно-цензурных установлений при исполнении служебных обязанностей, являются тайной, вверенной им по службе. За разглашение таковых тайн, служащие по военной цензуре, подлежат ответственности на общем основании».

Наравне с законодательством в данной области активно развивалась и научная мысль, примером чего может служить работа профессора церковного права Петербургского университета и священнослужителя Русской православной церкви Михаила Горчакова «О тайне супружества»[70], увидевшая свет в 1880 году. Констатируя наличие особого внимания, которое предается брачному праву в обществе и законодательной правительственной деятельности,

---

[69] Собрание узаконений и распоряжений Правительства. Отдел I. № 192. 20.07.1914. Ст. 2057 // СПС «КонсультантПлюс».

[70] Санкт-Петербург: тип. В.С. Балашева, 1880. IV. С. 55.

автор монографии, наряду с общими рассуждениями о существе брачного союза, выносит суждение о том, что «личные взаимоотношения между супругами должны храниться в тайне и не разглашаться без какой-либо нужды», в связи с чем было определено сохранять тайну супружества всем, кому она станет известной по определенным причинам и обстоятельствам[71]. Таким образом, неприкосновенность семейной тайны являлась предметом пристального внимания задолго до конституционного закрепления основных прав человека.

*Наряду с имеющимися узаконениями научные изыскания в области прав на неприкосновенность частной и семейной жизни находились в постоянной динамике, что свидетельствует о наличии в дореволюционной России стойкой тенденции к совершенствованию правового регулирования данного института, поскольку вне всякого сомнения защита персональных данных, связанных с личной жизнью человека, – это продукт развития прав человека и личности, что невозможно без одновременного развития самого общества, в котором потенциал, связанный с расширением объема личностных прав, подлежащих защите со стороны государства и ужесточении ответственности за их разглашение, был настолько значим, что послужил формированию той фундаментальной основы, на принципах которой строится современное правовое регулирования и защита персональных данных.*

При этом следует констатировать, что революционные события 1917 года коренным образом изменили взгляды на человеческую личность вообще и на ее права в частности[72], что нашло свое отражение в новом революционном законодательстве. 22 ноября 1917 г. Советом Народных Комиссаров РСФСР был принят декрет «О суде» № 1[73], согласно которому отмененными признавались все законы, противоречащие декретам Центрального Исполнительного Комитета Советов рабочих, солдатских и крестьянских депутатов и Рабочего и

---

[71] Шугай А.А. Защита персональных данных: формирование и развитие научных взглядов. Научные стремления / ООО «Лаборатория интеллекта» и Центр молодежных инноваций. Минск: «Энциклопедикс». 2013. Выпуск 7. С. 40–43.

[72] Майоров А.В., Поперина Е.Н. Формирование и развитие права на неприкосновенность частной жизни // Юридическая наука и правоохранительная практика. 2012. № 3 (21). С. 34–38.

[73] Декреты Советской власти. Т. 1. М., 1957.

Крестьянского правительства, а также программам-минимум Российской социал-демократической рабочей партии и партии социалистов-революционеров. Таким образом, вся правовая база, связанная с государственной защитой информации персонального характера, формировавшаяся на протяжении предшествующих веков, применению не подлежала. Но в дело правового регулирования общественных отношений смело вступило народное революционное творчество. Так в монографии Т.Н. Нуркаевой[74] можно ознакомиться с интересной информацией – «наказом Камышевскому народному гласному суду[75], выработанному общим собранием граждан 4 февраля 1918 года, где в специальном разделе «Об оскорблении чести, угрозах и насилии» выделялись следующие составы: нанесение обиды на словах или в письме; нанесение обиды действием; разглашение сведений, сообщенных втайне или же узнанных вскрытием чужого письма или другим образом». Поскольку данный наказ давался общим собранием граждан, то налицо совместное нормотворчество отдельного социума, который, как можно видеть из текста наказа, нуждался в защите личностных прав, что даже в столь неоднозначный период истории нашего государства свидетельствовал о жизнеспособности подобного рода потребностей. *Здесь допустимо провести некую параллель с настоящей действительностью, когда отсутствие четкого и предметного правового регулирования персональных данных и их защиты в виртуальной среде организаций восполняется за счет локального нормотворчества*, безусловно в рамках норм действующего законодательства, но все же исходя из индивидуальных потребностей каждого юридического лица.

Подобное положение вещей, когда правовой вакуум восполнялся посредством местечкового законотворчества просуществовал отчасти до 1919 года, периода введения в действие Руководящих начал по уголовному праву

---

[74] Нуркаева Т.Н. Уголовно-правовая охрана личности, ее прав и свобод: вопросы теории и практики. ООО «Проспект». 2017. С. 255.

[75] Материалы Народного комиссариата юстиции. Народный суд. М., 1918. Вып. 11. 56-57 с. из статьи Ульянченко А.М. «История развития уголовного законодательства России об ответственности за преступления против неприкосновенности частной жизни». 2006. Известия Вузов. Северо-Кавказский регион. Общественные науки. 2006. № 2, ст. 74–77.

РСФСР[76], которые содержали только общие положения, особенная же часть в них отсутствовала и, видимо, компенсировалась за счет подобных наказов общих собраний граждан. Полностью же таковая практика прекратила свое существование только в 1922 году с введением в действие первого Уголовного Кодекса республики. Декларация прав трудящегося и эксплуатируемого народа[77], утвержденная III Всероссийским съездом Советов 3 января 1918 года, хоть и имела многообещающее название, но никак не затронула вопросы гарантии государством защиты личностных прав граждан. Впоследствии данная Декларация без каких-либо изменений вошла в Конституцию РСФСР, утвержденную V Всероссийским съездом Советов. При этом никаких прав на защиту тайны переписки, профессиональных тайн, личной жизни «Основной Закон» страны не содержал, что в свете цивилизационного развития общества, несомненно, можно считать огромным шагом назад.

Принятие в 1922 году Уголовного Кодекса РСФСР[78] ситуацию никак не изменило[79]. Не привнесли ничего нового в область регулирования государственной защиты личностных прав граждан ни Конституция СССР 1924 года[80], ни Конституция РСФСР 1925[81] года, а Уголовный Кодекс РСФСР в редакции 1926 года, просуществовавший до 1961 года, полностью соответствовал основному Закону государства. И лишь 15 февраля 1929 года, спустя 12 лет после Великого Октября, постановлением СНК СССР[82] были введены в действие устав почтовый, телеграфный, телефонный и радио связи СССР, пункт 6 которого гласил, что «содержание всех видов почтовой, телеграфной и радиотелеграфной корреспонденции составляет тайну корреспондирующих лиц. Служащим связи общего пользования и специального назначения воспрещается нарушать означенную тайну, а также давать

[76] Собрание узаконений и распоряжений рабочего и крестьянского Правительства, № 66, 1919. 590 с.
[77] Декларация прав трудящегося и эксплуатируемого народа. 3 (16).01.1918 г. // Декреты Советской власти. Т. 1. М., 1957.
[78] Хрестоматия по истории отечественного государства и права 1917-1991 годов. М.: Зерцало, 1997. Ст. 63–68.
[79] Важорова М. А. Указ. соч. С. 33-38.
[80] Чистяков О.И. Конституция СССР 1924 года. Учебное пособие. М.: Зерцало-М, 2004.
[81] Известия ЦИК СССР и ВЦИК, 26.05.1925, № 118; Собрание узаконений и распоряжений Рабоче-крестьянского Правительства РСФСР. 1925. № 30. Ст. 218.
[82] СЗ СССР. 1929. № 22. Ст.193. Ст.194.

посторонним лицам какие-либо сведения о том, кем и кому корреспонденция подана или кем и от кого получена. За нарушение правил настоящей статьи служащие связи несут уголовную ответственность в порядке, устанавливаемом законодательством союзных республик». Поскольку уголовным законодательством РСФСР ответственность за нарушение вышеуказанной тайны предусмотрена не была, гарантии ее сохранения носили декларативный характер, но все же следует признать, что это был шаг вперед.

Продолжение развития правового регулирования личностных прав граждан нашло свое отражение в Конституции СССР 1936 года[83]. Как очень точно указано А.А. Троицкой, основные права возможно характеризовать как права, укрепившиеся в качестве таковых в сознании и именно поэтому включаемые в тексты конституций [84]. Так, согласно положениям статьи 128 Конституции СССР неприкосновенность жилища граждан и тайна переписки гарантировались на уровне основного закона государства. Однако, несмотря на данную декларацию, каких-либо репрессивных мер за нарушение этой тайны введено не было[85]. И только в Уголовном Кодексе 1961 года[86] впервые нашли свое отражение нормы о защите прав граждан на тайну переписки. Так, в статье 135 Кодекса предусматривалось наказание за нарушение тайны переписки граждан. Впоследствии в 1982 году в данную статью будут внесены изменения и уголовно наказуемыми станут деяния, связанные с нарушением не только тайны переписки, но и тайны телефонных переговоров и телеграфных сообщений. Еще раньше, в 1970 году, вводится в действие статья 124.1 Уголовного Кодекса РСФСР, предусматривающая ответственность за разглашение тайны усыновления против воли усыновителя.

Основополагающим документом международного уровня в области защиты прав и свобод человека является Всеобщая декларация прав человека,

---

[83] Известия ЦИК СССР и ВЦИК. 1936. № 283.

[84] Троицкая А.А. Основные права: происхождение, юридическая природа и пределы защиты // Сравнительное конституционное обозрение, 2013. № 1 (92). С. 67

[85] Терещенко Л.К., Тиунов О.И. Правовой режим персональных данных // Журнал российского права. 2014. № 12. С. 42–49.

[86] Ведомости Верховного Совета РСФСР. 1960. № 40. Ст. 591.

провозгласившая тот круг основных прав и свобод человека, которыми должны обладать все люди в мире вне зависимости от каких бы то ни было различий, как-то: в отношении расы, цвета кожи, пола, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного, сословного или иного положения[87]. Так, в частности, в статье 12 Декларации наглядно нашла свое отражение вышеуказанная концепция прайвеси («privacy»), согласно которой никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию и каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств. Таким образом, впервые за всю историю человечества на международном уровне был принят нормативный акт, декларирующий не только основные права и свободы человека, но и необходимость их защиты, что и было впоследствии реализовано в правоприменительной практике. Несмотря на то что данная Декларация имеет рекомендательный статус, на ее основании было принято два документа, имеющих уже обязательную силу для государств – участников, - Международный пакт о гражданских и политических правах и Международный пакт об экономических, социальных и культурных правах.

18 сентября 1973 года Указом Президиума ВС СССР[88] был ратифицирован Международный пакт о гражданских и политических правах от 16 декабря 1966 года[89], который обязывает государств-участников уважать гражданские и политические права людей. Данный Пакт вступил в силу 23 марта 1976 года. Статьей 17 данного Пакта предусмотрено, что «никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его

[87] Статья 2. Всеобщей декларации прав человека (принята Генеральной Ассамблеей ООН 10 декабря 1948 г.) // «Российская газета» от 10.12.1995.
[88] Указ Президиума ВС СССР от 18.09.1973 № 4812-VIII «О ратификации Международного пакта об экономических, социальных и культурных правах и Международного пакта о гражданских и политических правах». Ведомости Верховного Совета СССР. 1973. № 40. Ст. 564.
[89] Ведомости Верховного Совета СССР. 1976. № 17. Ст. 291.

жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств». Данные положения Пакта нашли непосредственное отражение в Конституции СССР, принятой 7 октября 1977 года[90], и Конституции РСФСР от 12 апреля 1978 года[91], согласно которым гарантировалось, что «личная жизнь граждан, тайна переписки, телефонных переговоров и телеграфных сообщений охраняются законом. Уважение личности, охрана прав и свобод граждан – обязанность всех государственных органов, общественных организаций и должностных лиц».

*Таким образом, личностные права граждан, деклассированные на начальном этапе становления советского государства, оказались вновь востребованными под влиянием внутренних запросов общества, когда отрицание естественного права каждого человека на уважение его частной жизни стало уже неприемлемым в силу общего культурного и образовательного уровня населения, а также в связи с интеграцией в мировое сообщество.*

5 сентября 1991 года Съездом народных депутатов СССР была принята Декларация прав и свобод человека № 2393-1[92], провозгласившая, что законы, закрепляющие естественные, неотъемлемые, ненарушенные права и свободы, должны соответствовать Всеобщей декларации прав человека, Международным пактам о правах человека, другим международным нормам и самой Декларации. В продолжение нормотворчества в данной области 22 ноября 1991 года Верховным Советом Российской Федерации принята Декларация прав и свобод человека и гражданина[93], статья 9 которой закрепила права граждан на:

- неприкосновенность его частной жизни, на тайну переписки, телефонных переговоров, телеграфных и иных сообщений;

- уважение и защиту его чести и достоинства;

---

[90] Ведомости Верховного Совета СССР. 1977. № 41. Ст. 617.
[91] Ведомости Верховного Совета РСФСР. 1978. № 15. Ст. 407.
[92] Ведомости СНД и ВС СССР. 1991. № 37. Ст. 1083.
[93] Ведомости СНД и ВС СССР. 1991. № 52. Ст. 1865.

- недопущение сбора, хранения, использования и распространение информации о частной жизни лица без его согласия.

11 марта 1992 года введен в действие Закон № 2487-1 «О частной детективной и охранной деятельности в РФ»[94], статья 7 которого запрещала собирать сведения, связанные с личной жизнью, политическими и религиозными убеждениями отдельных лиц, а также осуществлять видео- и аудиозапись, фото- и киносъемку в служебных или иных помещениях без письменного согласия на то соответствующих должностных или частных лиц. Практически через два года после принятия Декларации прав и свобод человека и гражданина - 12 декабря 1993 года - на всенародном голосовании принимается Конституция РФ[95], в статьях 23 и 24 которой закреплены права каждого на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений[96]. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Поправки к Конституции 2020 года данных норм никоим образом не коснулись.

Понятие «персональные данные» в Российской Федерации впервые прозвучало в Федеральном законе от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации»[97], который характеризовал персональные данные как сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность. Непосредственно в массиве данного законодательного акта персональным данным была посвящена отдельная статья[98], согласно которой персональные данные были отнесены к категории конфиденциальной информации, а также было установлено, что не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную

[94] Ведомости СНД и ВС СССР. 1992. № 17. Ст. 888.
[95] Российская газета. 1993. № 237.
[96] Проскурякова М.И. Конституционно-правовые рамки защиты персональных данных в России // Вестник СПбГУ. 2016. Сер.14. вып.2. С. 12–24.
[97] СЗ РФ. 31.07.2006. № 31 (часть I). Ст. 3448.
[98] Там же. Ст. 11.

тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения. Неправомерность же деятельности органов государственной власти и организаций по сбору персональных данных могла быть установлена в судебном порядке по требованию субъектов, действующих на основании статей 14 и 15 данного Федерального закона и законодательства о персональных данных. Таким образом, следует признать, что с учетом положений статьи 23 Конституции РФ, согласно которой каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну персональные данные в свете вышеуказанного Федерального закона являются не чем иным, как отдельным порождением от права каждого на неприкосновенность его частной жизни, в чем бы то ни выражалось.

Формирование законодательства о персональных данных происходит и в следующем 1996 году, когда 13 июня принимается новый Уголовный Кодекс РФ № 63-ФЗ[99], в который внесено три статьи, касающиеся рассматриваемой проблематики. Это статья 137 «Нарушение неприкосновенности частной жизни», введенная в правоприменительный оборот впервые и предусматривающая ответственность за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Статья 138 Уголовного Кодекса предусматривала ответственность за нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений, но данная норма новеллой не являлась, поскольку содержалась в предыдущем Уголовном Кодексе 1960 года. Еще одной новой нормой являлась статья 140 «Отказ в предоставлении гражданину информации», согласно которой под страхом наказания запрещался неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо

[99] СЗ РФ. 17.06.1996. № 25. Ст. 2954.

предоставление гражданину неполной или заведомо ложной информации. Буквально следом за принятием нового Уголовного Кодекса выходит в свет указа Президента РФ от 6 марта 1997 года № 188[100], которым устанавливается перечень сведений конфиденциального характера. Пунктом 1 значатся сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные). Как видно из вышеизложенного дается еще одна законодательная формулировка понятия «персональные данные».

16 октября 1999 года на Межпарламентской ассамблее государств-участников СНГ был принят модельный закон «О персональных данных»[101], который был рекомендован вышеуказанным государствам для использования при разработке национального законодательства. Так, персональными данными предлагалось считать информацию (зафиксированную на материальном носителе-материальных объектах (в том числе физических полях), в которых персональные данные находят свое отображение в виде символов, образов и сигналов) о конкретном человеке, которая отождествлена или может быть отождествлена с ним. При этом в данном законе впервые была предпринята попытка описать виртуальную среду обработки персональных данных, представляемую в виде некоего физического поля, что в дальнейшем не нашло своего развития в действующем законодательстве.

К персональным данным модельным законом отнесены биографические и опознавательные данные, личные характеристики, сведения о семейном, социальном положении, образовании, профессии, служебном и финансовом положении, состоянии здоровья и прочие. С учетом вышесказанного понятие «персональных данных» в первоначальной редакции Закона о персональных данных представляла собой некий симбиоз между подходом, изложенным в Конвенции 108 Совета Европы о защите прав физических лиц в отношении автоматической обработки персональных данных 1981 года, и Модельным

---

[100] СЗ РФ. 10.03.1997. № 10. Ст. 1127.
[101] Информационный бюллетень Межпарламентской Ассамблеи государств-участников СНГ. 2000. № 23.

законом «О персональных данных», принятым на Межпарламентской ассамблее государств-участников СНГ. Так, под персональными данными понималась любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Как видно из вышеизложенного, отдельная, строго определенная информация о лице на законодательном уровне в императивном порядке была отнесена к категории персональных данных, что следует признать некой попыткой создания перечня персональных данных по большей части смысловой направленности, поскольку данный перечень априори не может быть закрытым. Скорее всего, данная попытка и с точки зрения законодательной целесообразности, и с практической точки зрения себя не оправдала, в связи с чем Федеральным законом от 25 июля 2011 года № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»[102] введено новое, действующее до настоящего времени, понятие «персональных данных», согласно которому персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). При этом целью Закона о персональных данных является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

*Таким образом, начало постсоветского периода ознаменовано прежде всего прочего принятием именно таких законодательных актов, которые являются основополагающими в области регулирования и защиты неприкосновенности частной жизни граждан во всех ее ключевых сферах. В этой связи нельзя не согласиться с мнением Н.А. Богдановой о том, что «Россия исторически следует западной модели прав человека. Пережив социализм, отказавшись от него, она в*

[102] СЗ РФ. 01.08.2011. № 31. Ст. 4701.

*порядке реабилитации, подчеркивает естественно-правовой характер прав человека, характеризует их как неотчуждаемые, прирожденные и включает соответствующее положение в свою Конституцию»*[103]*. Созданный фундамент законодательства в данной области позволил не только продолжить, но и значительно расширить вектор правового регулирования личностных прав граждан, привнося в них различного рода специфику, примером которой может служить выделение информация в отдельный статус персональных данных и формирование самостоятельной области законодательства, которое в своем поступательном развитии демонстрирует тенденцию к упорядочению и отчасти ужесточению мер, связанных с регулированием обработки и защиты персональных данных как наиболее чувствительной информации.*

Одновременно с этим автор не может согласиться с мнением О.Б. Просветовой, согласно которому отечественный правоприменитель не обладает вековой традицией формирования и реализации законодательства через призму обеспечения прав и свобод человека и гражданина[104].

[103] Богданова Н.А. Основные права человека в России: идея, ее конституционное отражение и практика реализации // Конституционные идеалы и ценности в практической демократии: материалы и доклады XII Международной научно-практической конференции (Самара, 29 сентября – 2 октября 2016 г.) / Под ред. В.В. Полянского, В.Э. Волкова. Самара: Изд-во «Самарский университет», 2017. – С. 79–83.

[104] Просветова О.Б. Защита персональных данных. автореф. дис. … канд.юрид.наук. Воронеж, 2005. С.13.

## § 3. Определение информации, относящейся к персональным данным

Базовым нормативным правовым актом в области персональных данных является Закон о персональных данных, в котором сформирован основной понятийный аппарат. Фактически в Законе о персональных данных представлено два определения персональных данных, одно из которых можно признать общим, а второе, касающееся биометрических персональных данных, - специальным. При этом какая-либо формальная определенность относительно взаимного соотношения вышеуказанных понятий в Законе о персональных данных отсутствует, что всегда в подобных ситуациях вызывает затруднения в правоприменительной практике. Так, в общем значении персональные данные – это любая информация, которая относится к прямо определенному или косвенно определяемому физическому лицу, именуемому как субъект персональных данных[105]. Биометрические же персональные данные, исходя из конструкции нормы права[106], — это исключительно сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность.

При этом биометрические персональные данные условно можно разделить на два вида. К первому надлежит отнести те, которые изначально отбираются у субъекта персональных данных для целей установления его личности, что в обязательном порядке требует письменного согласия последнего, а ко второму все иные сведения, обладающие аналогичными характеристиками, но по цели их сбора не предназначенные для установления личности, хотя при определенных условиях и потребностях не исключающие таковой возможности, например проведение портретной экспертизы по видеозаписи, фоноскопической судебной экспертизы по голосу. Согласие на их обработку уже может быть получено любым иным способом,

[105] Статья 3 Закона о персональных данных.
[106] Статья 11 Закона о персональных данных.

а не только в письменном виде. При этом последние обладают специфическим свойством перехода в разряд биометрических персональных данных, используемых для установления личности, в случае возникновения такой необходимости.

Определение биометрических персональных данных, содержащееся в Законе о персональных данных, вряд ли можно признать корректным по причине его двоякого толкования в части того, какие конкретно персональные данные, характеризующие физиологические и биологические особенности человека, можно считать биометрическими персональным данным – только те, которые используются для установления личности человека, или все персональные данные, характеризующие вышеуказанные особенности, на основании которых установление личности возможно. Именно по данному критерию разделились мнения и в научной среде. Так, к примеру Д.Р. Галиуллина[107] и И.А. Терещенко[108] высказывают мнение о том, что к биометрическим персональным данным следует относить только те, целью использования которых является установление личности. Я.В. Кудашкин считает, что биометрические персональные данные – это сведения, необходимые для идентификации субъекта, на основании его физиологических или биологических параметров[109], что также подчеркивает их двойственность, т.е. возможность перехода из общей категории персональных данных в категорию биометрических при наличии соответствующей необходимости. Противоположного мнения придерживаются С.В. Баженов, В.Е. Дивольд, А.А. Морозов, Д.В. Попов, Д.М. Сафронов, А.В. Серов, О.В. Белая, Ю.А. Кицай, согласно которым «биометрические персональные данные – сведения, которые характеризуют физиологические, биологические и поведенческие особенности человека, на основании которых можно установить его личность»[110],

---

[107] Галиуллина Д.Н. Биометрические персональные данные // Документ. Архив. История. Современность. 2015. вып.15. С.268.

[108] Терещенко И.А. Биометрические персональные данные: проблемы перспективы определения понятия // Закон и право. 2024. № 2. С.189.

[109] Кудашкин Я.В. Правовое обеспечение безопасности обработки персональных данных в сети Интернет. дис. … канд.юрид.наук. М., 2019. С.11

[110] Баженов С.В., Дивольд В.Е., Морозов А.А., Попов Д.В., Сафронов Д.М., Серов А.В. Создание Концепции национальной системы биометрической идентификации личности // Труды Академии управления МВД России. 2020. № 2 (54). С. 48.

а «цель использования биометрически данных оператором влияет не на возможность отнесения сведений о лице к соответствующему виду персональных данных, а на порядок и процедуру их обработки, а именно обязательное получение письменного согласия от субъекта соответствующих данных»[111].

Судебная же практика идет по пути признания биометрическими персональными данными только тех сведений, которые используются для установления личности[112], что принципиально неверно, поскольку данный подход существенно меняет основную характеристику понятия, не позволяя относить к биометрическим персональным данным иные сведения, которые также характеризуют физиологические и биологические особенности человека, но не предназначены изначально для установления его личности, при том что сохраняют свое свойство перейти в разряд персональных данных, могущих быть использованных для установления личности. Если следовать оспариваемой в данном исследовании логике, то резонно предположить, что эти сведения надлежит именовать просто персональными данными, что, в свою очередь, вступает в противотечение с понятийным определением, данным в Законе о персональных данных.

Несмотря на вышеуказанные различия персональные данные этого вида обладают и общим свойством. Так, в случае порчи образца (фотографии, видеоизображения, записи голоса) по каким-либо техническим признакам данная информация в силу ее непригодности не может характеризовать физиологические и биологические особенности человека, т.е. быть использованной по назначению, в связи с чем ее нельзя отнести к категории персональных данных. В аналогичном порядке должен быть решен вопрос и в отношении сведений, не соответствующих

---

[111] Белая О.В., Кицай Ю.А. Биометрические данные как средство идентификации и аутентификации человека: Российский и международный опыт // Право и практика. 2020. № 1. С.87.

[112] Так суд в своем решении указал, что «в связи с тем, что граждане не относятся к непосредственным объектам видеонаблюдения, поскольку последними являются только территории и объекты, на основе данных видеоизображений, куда попадают изображения граждан, не проводится мероприятий, направленных на установление личности конкретного гражданина, что не позволяет отнести видеоизображение истицы к биометрическим персональным данным в связи с чем получения письменного согласия на их обработку не требуется» // решение Савеловского районного суда г.Москвы от 06.11.2019 по делу № 2а-577/2019 // https://mos-gorsud.ru/rs/savyolovskij/services/cases/kas/details/988f386e-be51-47b0-b48f-e871043ef1fc?caseNumber=2a-577/2019 (дата обращения: 15.02.2024).

действительности, но при этом указывающими на конкретное физическое лицо. Их также нельзя относить к категории персональных данных, поскольку в действительности эти сведения никакого отношения к последнему не имеют, а значит, не являются его личными персональными данными.

*Представляется, что все вышеуказанные сведения, характеризующие физиологические и биологические особенности человека, вне зависимости от целей их получения и использования относятся к категории биометрических персональных данных и должны именоваться именно так с видовым разделением на биометрические персональные данные, предназначенные для установления личности, и просто биометрические персональные данные.*

Одновременно с этим базовое определение персональных данных позволяет смоделировать две ситуации, связанные с установлением отношения какой-либо информации к конкретному персоналию. Это либо прямо определенное физическое лицо, либо косвенно определяемое. Первична в любом случае информация, т.е. исходя из ее содержания связь с физическим лицом может быть установлена либо безапелляционно - прямо, либо неочевидно - косвенно. Так, по мнению В.И. Солдатовой «косвенная идентификация прямо не указывает на имя или фамилию конкретного лица, но с ее помощью можно отнести к персональным данным информацию, содержащую описание индивидуальных характеристик лица, позволяющих отличить его от других субъектов»[113]. При этом ни на уровне доктринального толкования, ни на уровне законодательного регулирования не определены фактические и достаточные критерии, в соответствии с которыми лицо может быть признано косвенно определяемым, что не способствует единообразию в правоприменении и неминуемо влечет за собой возникновение спорных ситуаций.

Исходя из практики других отраслей права следует констатировать, что косвенное отношение требует дополнительных подтверждений для достоверности установления какого-либо факта. Так, связь информации с конкретным лицом на

[113] Солдатова В.И. Защита персональных данных в условиях применения цифровых технологий // LEX RUSSICA т.73 № 2 (159) февраль 2020. С.39 – 43.

условиях первоначальной неочевидности может быть достигнута в процессе так называемой доказательственной деятельности, например посредством проведения соответствующих экспертиз, установления нотариусом факта тождества[114], предоставления письменных доказательств, показаний свидетелей и тому подобной совокупности. Именно по этому пути придется идти субъекту персональных данных в случае его обращения в контролирующие или судебные органы за защитой своих прав в области обработки персональных данных, поскольку бремя доказывания в рассматриваемом случае возложено на него. Единственное отступление может иметь место, когда оператор персональных данных не оспаривает факта их отношения к конкретному физическому лицу, что позволяет принять данное соглашение в качестве обстоятельства, не требующего доказательства. Что же касается оператора персональных данных, то, исходя из буквального толкования определения персональных данных следует признать, что в случае невозможности установить отношение какой-либо информации, обрабатываемой в организации, к физическому лицу ни прямо, ни косвенно, последняя не может быть отнесена к категории персональных данных со всеми вытекающими отсюда последствиями. Так, по мнению М.В. Бундина для отграничения персональных данных от иных видов информации обосновывается использование в качестве основного признака персональных данных наличие взаимосвязи между субъектом и содержанием соответствующей информации о нем. Такая связь может быть очевидной через прямое указание на субъекта данных с использованием идентифицирующей информации, либо она может быть потенциально установлена[115].

*Таким образом, в целях упорядочения обработки персональных данных, правоприменения и достижения его единообразия необходимо определить критерии и выработать подходы, позволяющие идентифицировать информацию как относящуюся к косвенно определяемому физическому лицу.*

---

[114] Действующем законодательством установлена возможность нотариусов удостоверять тождественность личности гражданина с лицом, изображенным на представленной этим гражданином фотографии // статья 84 Основ законодательства РФ о нотариате.

[115] Бундин М.В. Персональные данные в системе информации ограниченного доступа. автореф. дис. … канд.юрид.наук. М., 2017. С. 9.

Процесс генерации человеком информации о себе является непрерывным, и любое его действие или бездействие в заданном запросе способно быть информативным с той или иной степенью эффективности. Но при этом не всякая информация способна стать персональными данными, поскольку для этого необходимо соблюдение определенных условий. Анализ норм действующего законодательства в области персональных данных позволил сделать вывод о том, что личностная информация о человеке может стать персональными данными только при наличии следующих условий, согласно которым субъект должен добровольно, посредством оформленного надлежащим образом согласия, передать информацию о себе оператору[116], осуществляющему обработку персональных данных исключительно в установленных им целях[117]. При отсутствии вышеуказанной совокупности информация о человеке не может быть признана персональными данными, что делает невозможным применение к рассматриваемым отношениям законодательства о персональных данных.

Условно обработку персональных данных можно разделить на две категории – инициативную и регламентированную, а определение состава информации, относящейся к персональным данным, возможно осуществлять на основании *законодательного установления, локального нормативного акта, судебного вердикта и усмотрения субъекта персональных данных*. При инициативной обработке персональных данных цели обработки перечень персональных данных устанавливаются оператором в его локальных актах, а при регламентированной – в нормах действующего законодательства.

Общим для всех операторов персональных данных является обязанность[118] по разработке политики и издании локальных актов в отношении обработки персональных данных, определение целей обработки, категорий и перечня персональных данных и т.п. При этом государственным и муниципальным органам, которые являются операторами персональных данных, надлежит установить перечень персональных данных, обрабатываемых в данных органах, в связи с

[116] Пункт 1 статьи 9; пункт 1 статьи 11 Закона о персональных данных,
[117] Подпункт 2 пункта 1 статьи 3; статья 5 Закона о персональных данных.
[118] Пункт 2 статьи 18.1 Закона о персональных данных.

реализацией служебных или трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций[119]. Так, в качестве примера можно привести Приказ Министра обороны Российской Федерации от 4 декабря 2019 г. № 707 «О персональных данных в Вооруженных Силах Российской Федерации» (Приложение № 4)[120], в котором содержится перечень категорий персональных данных, подлежащих обработке в Вооруженных Силах Российской Федерации.

Личностная информация о человеке может быть отнесена к категории персональных данных и на основании закона, например, частью 4 статьи 15 Федерального закона «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» от 22 декабря 2008 г. № 262-ФЗ[121] предусмотрено, что персональными данными применительно к судебным актам являются: фамилии, имена и отчества участников судебного процесса, дата и место рождения, место жительства или пребывания, номера телефонов, реквизиты паспорта или иного документа, удостоверяющего личность, идентификационный номер налогоплательщика - физического лица, основной государственный регистрационный номер индивидуального предпринимателя, страховой номер индивидуального лицевого счета, сведения о месте нахождения земельного участка, здания, сооружения, жилого дома, квартиры, транспортного средства, иные сведения об имуществе и о находящихся в банках или иных кредитных организациях денежных средствах участников судебного процесса. Аналогичные перечни персональных данных с учетом специфики общественных отношений

---

[119] Подпункт «б» пункта 1 Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утв. постановлением Правительства РФ от 21.03.2012 № 211 (ред. 15.04.2019) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» // СЗ РФ. 02.04.2012. № 14. Ст. 1626.

[120] Текст приказа опубликован на "Официальном интернет-портале правовой информации" (www.pravo.gov.ru) 18.03.2020 (дата обращения 17.09.2024).

[121] СЗ РФ. 29.12.2008. № 52 (часть I). Ст. 6217.

содержатся и в иных нормативных правовых актах[122]. При этом следует учитывать, что персональные данные, определенные в каждом конкретном нормативном правовом акте, могут применяться только к тем сферам общественных отношений, которые вышеуказанные нормативно правовые акты регулируют.

Что же касается *критерия, связанного с возможностью на основании персональных данных определить субъекта*, то он фактически перестает играть какую-либо роль. Операторы и иные лица, получившие доступ к вышеуказанным персональным данным, будут нести ответственность за любое нарушение обработки этих данных, даже если это касается части из них, по которой определить конкретного человека возможным и не представится. Например, фамилии, имена и отчества физических лиц, которые без дополнительной информации уточняющего характера не могут ни прямо, ни косвенно идентифицировать субъектов. Но при этом в случае утечки вышеуказанных сведений оператор все равно может быть привлечен к ответственности, поскольку данные сведения по воле законодателя поименованы в качестве персональных данных, что априори предполагает их защиту вне зависимости от каких-либо дополнительных факторов, включающих и возможность идентифицировать конкретную личность.

Но вот что касается самих физических лиц, то судебная перспектива требований материального (статья 15 Гражданского Кодекса) и морального (статья 151 Гражданского Кодекса РФ) возмещений в данном случае уже напрямую зависит от возможности идентификации истцов на основании информации, утечка которой произошла. В противном случае право на иск отсутствует, поскольку возможность

---

[122] Указ Президента РФ от 30.05.2005 № 609 (ред. 29.04.2023) «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведения его личного дела» // СЗ РФ. 06.06.2005. № 23. Ст. 2242;

- Постановление Правительства РФ от 30.06.2018 № 772 (с изм. на 12.07.2022) «Об определении состава сведений, размещаемых в Единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства РФ» // СЗ РФ. 09.07.2018. № 28. Ст. 4234;

- Приказ Министерства здравоохранения РФ от 04.03.2019. № 110н «Об обработке персональных данных в Министерстве здравоохранения РФ» // Текст приказа опубликован на "Официальном интернет-портале правовой информации" (www.pravo.gov.ru) (дата обращения 24.12.2024).

получения защиты субъективного права может быть реализована только конкретным лицом и только при доказанности факта нарушения его права.

Таким образом, одним из способов придания информации о человеке статуса персональных данных является *законодательное установление*, распространяющее свое действие на неограниченных круг лиц – как на операторов персональных данных в каждой отдельной сфере общественных отношений, так и на субъектов персональных данных. Но здесь возникает значимый с практической точки зрения вопрос о том, могут ли государственные и муниципальные органы по собственной инициативе расширить установленный для них в нормах действующего законодательства перечень персональных данных и подвергнуть обработке дополнительные персональные данные. Представляется, что не могут. Вопрос же интересен отсутствием не только правового регулирования, но и каких-либо компетентных разъяснений. Так, оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных[123]. При этом обязанности оператора персональных данных по их защите корреспондирует право субъекта персональных данных привлечь последнего к ответственности за нарушение требований законодательства о персональных данных. Устанавливая в нормативном правовом акте перечень персональных данных, подлежащих обработке государственными или муниципальными органами, законодатель тем самым ограничивает рамки их материальной, бюджетной ответственности за нарушение обязанности по защите именно этих персональных данных. Обработка иных персональных данных, не предусмотренных нормативными правовыми актами, следует рассматривать как самовольное расширение границ ответственности государственной и

[123] Статья 19 Закона о персональных данных.

муниципальной структуры, могущее повлечь за собой бюджетный ущерб, не прогнозируемый и не допускаемый при их принятии.

Таким образом, наличие законодательно установленных перечней персональных данных, которые могут обрабатываться в той или иной сфере деятельности, не предусматривает какой-либо инициативы по их расширению со стороны операторов персональных данных, являющихся государственными и муниципальными органами. Одновременно с этим подобные действия следует рассматривать и с точки зрения нарушения императивных требований законодательства, связанных с четким определением перечня персональных данных, которые могут быть подвергнуты обработке.

Поскольку одним из признаков, характеризующих нормативный правовой акт, является наличие в нем правовых норм (правил поведения), обязательных для неопределенного круга лиц[124], следует признать, что *рассматриваемые законодательные установления распространяются и на субъектов персональных данных*, права которых на неприкосновенность частной жизни, личную и семейную тайну гарантируются. Так, статья 23 Конституции РФ гарантирует каждому право на неприкосновенность частной жизни, личной и семейной тайны, защиту своей чести и доброго имени, а ч. 1 ст. 24 Конституции РФ предусматривает, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Также запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами[125]. Исходя из буквального прочтения

---

[124] Признаками, характеризующими нормативный правовой акт, являются: издание его в установленном порядке управомоченным органом государственной власти, органом местного самоуправления, иным органом, уполномоченной организацией или должностным лицом, наличие в нем правовых норм (правил поведения), обязательных для неопределенного круга лиц, рассчитанных на неоднократное применение, направленных на урегулирование общественных отношений либо на изменение или прекращение существующих правоотношений. Пункт 2 Постановления Пленума Верховного Суда Российской Федерации от 25.12.2018 № 50 «О практике рассмотрения судами дел об оспаривании нормативных правовых актов и актов, содержащих разъяснения законодательства и обладающих нормативными свойствами» // Бюллетень Верховного Суда Российской Федерации, февраль 2019. № 2.

[125] Пункт 8 статьи 9 Закона об информации.

данной нормы права, следует признать, что разрешение требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, равно как и запрет на совершение данных действий, может быть дано только в федеральном законе.

При этом понятие «частная жизнь» действующее законодательство не раскрывает, но согласно позиции Конституционного Суда РФ право на неприкосновенность частной жизни, личной и семейной тайны означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера. В понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит непротивоправный характер[126]. Соответственно, лишь само лицо вправе определить, какие именно сведения, имеющие отношение к его частной жизни, должны оставаться в тайне, а потому сбор, хранение, использование и распространение такой информации, не доверенной никому, не допускается без согласия данного лица, как того требует Конституция РФ[127]. Выявленный КС РФ конституционно-правовой смысл нормы приобретает общеобязательный характер для всех субъектов права[128]. Как совершенно верно отметил М.В. Бундин, «определение объекта защиты, т.е. информации, целиком зависит от желаний и интересов частного лица»[129]. Несмотря на то что содержание частной жизни довольно субъективно и, что самое главное, не может быть властно-контролируемо, федеральным законом может быть установлено дозволение истребовать у субъектов персональных данных необходимую информацию вне зависимости от того, относит ли кто-то из них ее к своей частной жизни или нет. Таким образом, только федеральный закон и никакой иной нормативный правовой акт вправе своим

---

[126] Определения Конституционного Суда РФ от 09.06.2005 № 248-О; от 26.01.2010 № 158-О-О // СПС «Консультант Плюс».
[127] Определение Конституционного Суда РФ от 28.06.2012 № 1253-О // СПС «Консультант Плюс».
[128] Брежнев О.В. Конституция 1993 г. и развитие конституционного правосудия в России // Вестник Московского Университета. Серия 11. Право. 2023. Т.64. № 6. С. 75.
[129] Бундин М.В. Система информации ограниченного доступа и конфиденциальность // Вестник Нижегородского университета им. Лобачевского. 2015. №1. С.122.

волеизъявлением исключить определенную информацию персонального характера из сферы частной жизни гражданина посредством предоставления права ее истребования. При этом государственные и муниципальные органы, являющиеся операторами персональных данных, обрабатывают персональные данные как в связи с реализацией служебных или трудовых отношений, так и в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций, что не одно и то же.

Относительно трудовых отношений возможно сослаться на положения абзаца 7 статьи 11 Трудового Кодекса Российской Федерации[130], согласно которому на государственных и муниципальных служащих действие трудового законодательства и иных актов, содержащих нормы трудового права, распространяется с особенностями, предусмотренными федеральными законами и иными нормативными правовыми актами Российской Федерации, законами и иными нормативными правовыми актами субъектов Российской Федерации о государственной и муниципальной службе. Таким образом, установление перечня персональных данных и/или способов их определения в нормативных правовых актах иного уровня, чем федеральный закон в сфере регулирования трудовых и служебных отношений вполне возможно.

Но вот что касается оказания государственных или муниципальных услуг и осуществления одноименных функций, где подчас наличествует недопонимание и недовольство перечнем персональных данных по причине отнесения их субъектом к частной жизни, но без предоставления которых получить, к примеру, государственную или муниципальную услугу возможным не представляется, то рассматриваемое дозволение должно регулироваться либо только федеральным законом, либо иным нормативным правовым актом в случае установления такой возможности федеральным законом. При этом анализ действующего законодательства свидетельствует о тенденции к регламентации особо чувствительных сфер информации персонального характера исключительно на основе федеральных законов.

---

[130] СЗ РФ. 07.01.2002. № 1 (часть I). Ст. 3.

Так, в частности, ограничение доступа к информации возможно только на основании федерального закона[131]. В аналогичном порядке может быть решен вопрос о возможности предоставления разрешений требовать от гражданина информацию о его частной жизни, в том числе информацию, составляющую его личную и семейную тайну[132]; передавать третьим лицам информацию, составляющую профессиональную тайну[133]; не исполнять обязанность по уничтожению либо обезличиванию персональных данных по достижении целей обработки[134]; операторам и иным лицам, получившим доступ к персональным данным, раскрывать третьим лицам и распространять персональные данные без согласия субъекта персональных данных[135]; не прекращать обработку специальных категорий персональных данных, если устранены причины, вследствие которых она осуществлялась[136].

*В этой связи законодательство Российской Федерации в области персональных данных определенно нуждается в проведении взаимосвязанного анализа нормативных правовых актов в различных областях общественных отношений с целью выявления имеющихся противоречий и создания условий для их устранения.*

Сфера частной жизни как таковая вообще способна создавать достаточно интересные коллизии в правоприменении. Так, в качестве иллюстрации можно привести уголовную отрасль права. Согласно положениям части 1 статьи 137 Уголовного кодекса РФ (далее – УК РФ)[137] за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную[138] или семейную тайну, без его согласия, либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или

---

[131] Пункт 1 статьи 9 Закона об информации.
[132] Пункт 8 статьи 9 Закона об информации.
[133] Пункты 5,6 статьи 9 Закона об информации.
[134] Пункт 7 статьи 5 Закона о персональных данных.
[135] Статья 7 Закона о персональных данных.
[136] Пункт 4 статьи 10 Закона о персональных данных.
[137] УК РФ от 13.06.1996 (ред. 08.08.2024) // СПС «КонсультантПлюс».
[138] Сведения, содержащиеся в переписке, фото- и видеоматериалах составляют личную тайну. Обзор судебной практики Верховного Суда РФ № 2, утв. Президиумом Верховного Суда РФ 22.07.2020 // СПС «КонсультантПлюс».

средствах массовой информации предусмотрена ответственность в рамках санкции данной нормы права.

Преступление, предусмотренное частью 1 статьи 137 УК РФ является делом частно-публичного обвинения, которое возбуждается не иначе как по заявлению потерпевшего или его законного представителя. Преступления, предусмотренные частями второй (те же деяния, только совершенные лицом с использованием служебного положения) и третьей (касается исключительно несовершеннолетних) вышеозначенной нормы права, являются делами публичного обвинения, поводы для возбуждения которых перечислены в статье 140 Уголовно-процессуального кодекса РФ[139]. Это заявление о совершении преступления, которое может быть подано в правоохранительные органы любым лицом, а не только потерпевшим, явка с повинной, сообщение о совершенном или готовящемся преступлении, полученное из иных источников. Но здесь возникает интересная ситуация, связанная с наличием вышеуказанной позиции Конституционного Суда РФ, согласно которой лишь само лицо, условно потерпевший в рамках уголовного права, вправе определить, какие именно сведения имеют отношение к его частной жизни, а какие нет и хотел ли он держать эти сведения в тайне[140]. Редкий случай, когда дело публичного обвинения не может быть возбуждено, а возбужденное дело подлежит прекращению, если лицо – потерпевший - заявит, что не считает собранные или распространенные в отношении него сведения, относящимися к его частной жизни, которые бы он хотел держать в тайне.

Предлагаемое исследование не может считаться полным без рассмотрения вопроса, связанного с процедурой выражения несогласия лицами, права и обязанности которых затрагиваются теми или иными нормативными правовыми актами. Оспаривание последних осуществляется в соответствии с правилами,

---

[139] Уголовно-процессуальный кодекс РФ от 18.12.2001 № 174-ФЗ (ред. 01.07.2024) // СЗ РФ. 24.12.2001. № 52 (часть I). ст.4921. Далее по тексту – УПК РФ.

[140] При решении вопроса о наличии в действиях лица состава преступления, предусмотренного ч. 1 или ч. 2 ст. 137 УК РФ, суду необходимо устанавливать, охватывалось ли его умыслом, что сведения о частной жизни гражданина хранятся им в тайне (постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138[1], 139, 144[1], 145, 145[1] УК РФ)» // Бюллетень Верховного Суда РФ, февраль 2019. № 2. Далее по тексту - постановление Пленума Верховного Суда РФ от 25.12.2018 № 46.

предусмотренными главой 21 Кодекса административного судопроизводства Российской Федерации[141], и является самостоятельным способом защиты прав и свобод. Такое оспаривание производится посредством подачи административного искового заявления, заявления о признании недействующим нормативного правового акта, как не соответствующего федеральному закону или иному нормативному правовому акту, имеющему большую юридическую силу, и в связи с этим не подлежащим применению для регулирования тех или иных общественных отношений. Последствием признания судом нормативного правового акта недействующим является его исключение из системы правового регулирования полностью или в части[142]. С административным исковым заявлением о признании нормативного правового акта не действующим полностью или в части вправе обратиться лица, в отношении которых применен этот акт, а также лица, которые являются субъектами отношений, регулируемых оспариваемым нормативным правовым актом, если они полагают, что этим актом нарушены или нарушаются их права, свободы и законные интересы.

Административные дела, связанные с оспариванием нормативных правовых актов Президента Российской Федерации, Правительства Российской Федерации, федеральных органов исполнительной власти, Генеральной прокуратуры Российской Федерации, Следственного комитета Российской Федерации, Судебного департамента при Верховном Суде Российской Федерации, Центрального банка Российской Федерации, Центральной избирательной комиссии Российской Федерации, государственных внебюджетных фондов, в том числе Фонда пенсионного и социального страхования Российской Федерации, Федерального фонда обязательного медицинского страхования, а также государственных корпораций, рассматриваются Верховным Судом Российской Федерации в качестве суда первой инстанции[143].

---

[141] СЗ РФ. 09.03.2015. № 10. Ст. 1391.

[142] Постановление Пленума Верховного Суда Российской Федерации от 25.12.2018 № 50 «О практике рассмотрения судами дел об оспаривании нормативных правовых актов и актов, содержащих разъяснения законодательства и обладающих нормативными свойствами» // Бюллетень Верховного Суда РФ, февраль 2019. № 2.

[143] Подп.1 пункта 4 статьи 2 Федерального конституционного закона от 05.02.2014 № 3-КФЗ (ред. 14.07.2022) «О Верховном Суда Российской Федерации» // СЗ РФ. 10.02.2014. № 6. Ст. 550.

Что же касается федеральных законов, то в отношении них могут быть разрешены дела только об их соответствии Конституции Российской Федерации и только в Конституционном Суде Российской Федерации по запросам Президента Российской Федерации, Совета Федерации Федерального Собрания Российской Федерации (далее - Совет Федерации), Государственной Думы Федерального Собрания Российской Федерации (далее - Государственная Дума), одной пятой сенаторов Российской Федерации или депутатов Государственной Думы, Правительства Российской Федерации, Верховного Суда Российской Федерации, органов законодательной и исполнительной власти субъектов Российской Федерации[144]. Конституционность федеральных законов может быть проверена и по жалобам граждан на нарушение их конституционных прав и свобод федеральными законами, применёнными исключительно в конкретном деле и при условии, что исчерпаны все другие внутригосударственные средства судебной защиты[145].

В отношении операторов, которые не относятся к числу государственных и муниципальных органов, правовое регулирование обработки ими персональных данных осуществляется на основе локального нормотворчества, при котором, исходя из установленных целей обработки как в области трудовых отношений, так и в области уставной деятельности, оператор персональных данных самостоятельно определяет перечни персональных данных, подлежащих обработке. При этом вне зависимости от того, определены ли персональные данные в тексте политики обработки персональных данных в виде четкого перечня или имеется понятийная отсылка к Закону о персональных данных, операторы сами, по собственному усмотрению и только в отношении себя придают данной информации статус персональных данных, а также возлагают на себя обязанность и соответствующую ответственность за правомерность их обработки и надлежащую защиту вне зависимости от того, возможно ли на основании этой информации определить конкретное физическое лицо или нет.

---

[144] Подпункт «а» пункта 1 статьи 3 Федерального конституционного закона от 21 июля 1994 г. № 1-ФКЗ (ред. 31.07.2023) «О Конституционном Суде Российской Федерации // СЗ РФ. 25.07.1994. № 13. Ст. 1447.
[145] Там же. Пункт 3 статьи 3.

Данный критерий, как и в предыдущем случае, будет иметь значение исключительно для субъекта персональных данных в случае, если он возымеет намерение обратиться за защитой своих прав, нарушенных обработкой персональных данных или их утечкой. Логика действия абсолютна идентична уже рассмотренному выше способу придания информации статуса персональных данных в нормативных правовых актах. Но вот что касается запрета требовать от гражданина предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, то в рассматриваемом случае соблюдение оператором данного запрета возможным не представляется, в связи с субъективным пониманием каждым лицом того, что относится к данной информации. Так, к примеру, для кого-то сведения о семейном положении – личная тайна, а для кого – то нет. В этой связи возможно возникновение спорных ситуаций с ярко выраженным индивидуальным подтекстом, последствия рассмотрения которых будут касаться исключительно конкретного персоналия.

При этом следует обратить внимание на наличие определенной специфики при оспаривании локального акта, устанавливающего порядок обработки персональных данных сотрудников полностью или в части. Так, требования, связанные с признанием его недействительным или противоречащем закону полностью или в части, не могут быть рассмотрены судами по иску работника, не уполномоченного представлять других работников, поскольку оспариваемый акт также регулирует и их права. В этой связи судебная перспектива подобных дел появляется исключительно в случае, когда все до единого работника подают коллективный иск.

В то же время это не означает, что индивидуальный спор по данной тематике не может быть рассмотрен судебными органами. Для этого нужно лишь воспользоваться иным способом защиты, когда работник обращается в судебные органы за защитой своих нарушенных прав и в процессе рассмотрения дела будет установлен факт несоответствия локального акта, но, как правило, в части, законодательству, что в силу пункта 4 статьи 8 Трудового Кодекса РФ влечет за собой невозможность его применения в этой части.

Таким образом, в отличие от оспаривания нормативного правового акта, что является самостоятельным способом защиты прав и свобод граждан, для локальных актов такой способ защиты действующим законодательством не предусмотрен, в связи с чем проверка последнего на предмет его соответствия законодательству проходит в рамках рассмотрения дел о восстановлении нарушенного права конкретного индивида. При этом требовать признания незаконным включения какой-либо информации в перечень персональных данных работников, подлежащих обработке, на том основании, что последняя относится в частной жизни работника, является его личной или семейной тайной, возможным не представляется, в связи с многообразием индивидуальных характеристик данной информации. В качестве способа защиты своих прав субъект персональных данных может воспользоваться требованием о прекращении обработки его персональных данных и их уничтожении.

Аналогично не может быть оспорен локальный акт, регулирующий порядок обработки персональных данных неограниченного круга лиц, к примеру, в процессе оказания услуг или осуществления оператором персональных данных своей уставной деятельности. Восстановление нарушенных прав субъектов персональных данных также возможно в процессе рассмотрения индивидуального спора с использованием тех же способов защиты.

Еще одним способом отнесения информации к категории персональных данных является *судебное установление*, которое способно носить как общий, в силу определённой специфики применимым ко всем иным отношениям, так и индивидуальный характер, который уже не предполагает такой возможности. Как пример можно привести судебные акты, согласно которым фотография на пропуске, предназначенная для определения личности входящего на территорию какого-либо объекта, является персональными данными[146], а адрес электронной

[146] Решение Арбитражного суда Мурманской области от 03.04.2017 № А42-342/2017 // https://kad.arbitr.ru/Card/f2ba9d7a-13ce-493c-ba04-a14c927a4c7c (дата обращения: 24.12.2024).

почты[147] и ИНН[148], напротив, к персональным данным не причислены. Поскольку в обоих делах Верховный Суд РФ выводы нижестоящих судов поддержал, то следует признать наличие судебного закрепления факта отнесения или не отнесения вышеуказанной информации к категории персональных данных, что подразумевает под собой возможность применения данного подхода ко всем иным отношениям, разумеется, при наличии аналогичных обстоятельств. Так, В.М.Лебедев в своей работе «Судебная власть в современной России: проблемы становления и развития» указывал на то, что решения судов высшей инстанции в любом случае выступают только как вторичные источники права, так как свои решения они основывают на действующих правовых нормах, в связи с чем не могут признаваться первоисточниками. А с учетом того, что такие решения все же являются источниками права, ссылка на них в своих решениях другими судебными органами вполне правомерна[149].

Но существует и иная категория судебных споров, выводы по которым не могут применяться к другим отношениям и с другими субъектами в силу отсутствия значимой по своему масштабу признаковой общности. Например, работник обратился в судебные органы с иском о прекращении обработки и уничтожении некой информации, которую он сгенерировал в период работы и которая в локальном акте в качестве персональных данных конкретно не поименована. Поскольку в данном случае отсутствует факт признания информации персональными данными, как, например, в нормативных и локальных актах, устанавливающих их конкретные виды, то только суд в рассматриваемом случае вправе отнести последнюю к персональным данным. Судебные решения, в свою очередь, можно разделить на те, которые связаны с оспариванием факта отнесения той или иной информации к персональным данным и те, которые, напротив, устанавливают данный факт при наличии спора, т.к. «нормы Закона о

---

[147] Определение Верховного Суда № 305-ЭС23-12160 от 21.07.2023 // https://base.garant.ru/407421338/ (дата обращения: 24.12.2024).
[148] Определение Верховного Суда № 13-В05-13 от 01.03.2006 // https://vsrf.ru/stor_pdf.php?id=137200 (дата обращения: 24.12.2024).
[149] Кузенков К.Г. Судебная практика Верховного Суда РФ как источник права // Юридическая наука. 2021. № 12. С. 9–13.

персональных данных предполагают явную заинтересованность, прежде всего самого субъекта персональных данных, определяющего степень воздействия на его приватную сферу жизни, в отнесении таких сведений к числу конфиденциальных»[150]. На настоящий момент следует отметить, что доля судебного установления принадлежности какой-либо информации к категории персональных данных достаточно велика и не показывает тенденции к снижению.

Возможностью отнесения какой-либо информации к категории персональных данных, вне всякого сомнения, обладают и сами *физические лица*. Данный вывод основан на анализе базового определения персональных данных в совокупности с иными нормами права, правоприменительной практикой и логикой самих общественных отношений в данной области. Так, персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). При этом вопрос критериев определимости физического лица на основании какой-либо информации до конца не разрешен ни в теоретической области, ни в области правоприменения, при том что возможность прямого или косвенного определения субъекта персональных данных является составляющей вышеуказанного понятия.

Иными словами, необходимо рассмотреть вопрос о том, кто может или, напротив, должен иметь возможность определить физическое лицо на основании какой-либо информации, сам субъект, третье лицо или третьи лица. Законом о персональных данных возможность защиты субъектом персональных данных своих прав не поставлена в зависимость от того, для кого и в каком численном составе он может или, напротив, должен быть определяемым, в связи с чем этим лицом может быть как сам субъект персональных данных, к которому данная информация непосредственно относится, так и третьи лица. При этом ни нормы действующего законодательства, ни правоприменительная практика не определяют какого количества третьих лиц для этого достаточно, т.е. по факту рамки соответствия на данном уровне не заданы. Совершенно не исключено, что и среди

[150] Кучеренко А.В. Сравнительный анализ принципов отнесения информации к персональным данным и иным видам сведений конфиденциального характера // Вестник АмГУ. 2009. выпуск 44. С.66.

неограниченного числа людей вполне может быть один или несколько человек, которые на основании, к примеру, того же номера телефона и иной подобной информации способны определить конкретного человека. Одновременно с этим возможность и достаточность установления отношения какой-либо информации к конкретному лицу только и исключительно на основании утверждения субъекта персональных данных на уровне законодательного установления не отрицается.

Актуальность вопроса о возможности отнесения какой-либо информации к категории персональных данных по инициативе самого субъекта связана исключительно с последствиями, которые могут иметь место в результате совершения данных действий. Так, субъект персональных данных, посчитав, что спорная информация имеет к нему отношение, может никак на данный факт не отреагировать, а может предпринять предусмотренные законом меры по защите своих персональных данных, посредством отзыва у оператора согласия на их обработку, заявления требований о прекращении обработки персональных данных и их уничтожении. В случае отказа оператора в удовлетворении заявленных требований субъект персональных данных вправе обратиться за защитой своих прав в компетентные органы, при этом бремя доказывания того факта, что спорная информация имеет отношение именно к нему, лежит на субъекте персональных данных. Если в результате доказательственной деятельности будет установлена несомненная связь между спорной информацией и субъектом персональных данных, требования последнего во всяком случае подлежат удовлетворению, за некоторыми специальными исключениями. Исходя из вышеизложенного, в целях получения лицом безусловной защиты единственным и достаточным условием может являться возможность последнего идентифицировать себя на основании спорной информации без учета аналогичных возможностей для третьих лиц.

***Таким образом, по результатам проведенного исследования можно сделать следующие выводы:***

*1. К персональным данным относится только та информация, которая отвечает совокупности следующих 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;*

*- информация должна быть пригодна для использования по назначению;*

*- передаваемая информация должна либо прямо указывать на субъекта персональных данных, либо косвенно, что требует дополнительных доказательств для установления ее отношения к конкретному лицу;*

*2. Виды персональных данных, обрабатываемых оператором, могут определяться следующим способами посредством:*

*- определения оператором персональных данных;*

*- законодательного закрепления;*

*- судебного установления;*

*- волеизъявления субъекта персональных данных.*

*Одновременно с этим необходимо:*

*1. Внести ясность в понятие биометрических персональных данных, признав, что биометрическими персональными данными являются все сведения, характеризующие физиологические и биологические особенности человека, с разделением на две категории – изначально создаваемые с целью использования для установления личности человека, и, изначально не предназначенные для этой цели, но на основании которых можно установить личность человека.*

*2. Определить критерии и выработать подходы, позволяющие идентифицировать информацию как относящуюся к косвенно определяемому физическому лицу.*

# ГЛАВА II. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБОРОТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ВИРТУАЛЬНОЙ СРЕДЕ ОРГАНИЗАЦИЙ

## § 1. Характеристика и виды персональных данных в виртуальной среде организаций

Технологическое развитие общества повсеместно и неуклонно вносит поистине кардинальные перемены во все области жизни. На этом фоне рынок труда и занятости объективно претерпевает серьезные изменения. «Труд можно считать глобальным ресурсом, поступающим по трем каналам: 1) фирмы могут выбрать свое местоположение в разных местах по всему миру, с тем чтобы найти трудовые ресурсы в зависимости от навыков, издержек или социальных условий; 2) фирмы в любом месте могут привлечь к себе высококвалифицированных работников отовсюду, и они их получат, если предложат хорошую оплату и условия труда; наконец, 3) люди по собственной инициативе могут войти на любой рынок из любой точки мира, гонимые из дома нуждой, войнами или движимые заботой о своих детях»[151].

Привычная для нас форма организации трудовой деятельности, при которой выполнение должностных обязанностей связано с непосредственным нахождением в месте осуществления работодателем своей деятельности, уже перемежается с, так называемой нетрадиционной формой ведения бизнеса, когда коммуникации между территориально удаленными участниками трудового процесса, контроль за их деятельностью и т.п. осуществляются с помощью интернета и иных современных технологий. При этом степень таковой виртуализации может быть совершенно различной, что обусловлено исключительно объективными потребностями хозяйствующего субъекта.

---

[151] Hans Jägers, Wendy Jansen and Wilchard Steenbakkers. Characteristics of Virtual Organizations. Proceedings of the VoNet - Workshop, April 27-28, 1998. Материалы семинара VoNet, 27-28 апреля 1998 г. С.65. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.83.1293&rep=rep1&type=pdf (дата обращения 24.12.2024).

Согласно положениям Закона о персональных данных обработка персональных данных может осуществляться двумя способами - с использованием средств автоматизации или без их использования[152]. Под автоматизированной обработкой персональных данных понимается обработка с помощью средств вычислительной техники, которые, в свою очередь, определяются как совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем[153]. В рамках рассмотрения такого явления, как виртуальная среда, данное определение по своему содержанию остаётся актуальным, поскольку цифровой функционал до сих пор представляет собой совокупность технических и программных элементов.

Виртуальная среда организаций характеризуется не только техническим аспектом, связанным с одноименной инфраструктурой, технологиями, программным обеспечением и другими привычными элементами цифровой действительности, которые не играют основополагающей роли и по своей сути вторичны. Приоритет же отдается описанию модели коммуникаций, видов технологий, предполагаемых к использованию, способов обработки персональных данных и установления их перечня, определения круга субъектов, вовлекаемых в процесс создания информации и претендующих на доступ к информации конфиденциального характера, контура сетей, аппаратной составляющей и других потребностей, 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 запросов. Тем не менее виртуальная среда уже заняла прочное место как в механизме регулирования деятельности отдельно взятой хозяйствующей структуры, так и в экономике в целом.

Осуществление связи между географически удаленными партнерами экономической структуры происходит посредством создания последней своего

---

[152] Пункт 3 статьи 3 Закона о персональных данных.

[153] Государственный стандарт РФ ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» принят постановлением Госстандарта РФ от 09.02.1995 г. № 49 // СПС «КонсультантПлюс».

коммуникативного пространства, входящего в виртуальную среду организации, где возможно создавать, передавать и принимать информацию, вести переписку и общение по всем вопросам. В качестве примеров современных информационно-коммуникационных технологий можно привести корпоративную электронную почту, 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. 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. «Тотальный электронный контроль все шире проникает во все сферы жизни человека, в том числе в трудовые отношения. Так, по данным ряда исследований, проведенных в последние 5 лет, до 80% компаний в той или иной мере осуществляют слежку за своими сотрудниками. 40-60% из них мониторят рабочие компьютеры сотрудников, 30% ограничиваются видеокамерами и системами контроля доступа, до 30% применяют для мониторинга широкий комплекс технических средств»[154]. Таким образом, все то, что ранее в привычной для нас среде проходило или как устное общение, или как визуально контролируемый рабочий процесс, в виртуальной среде оставляет вполне реальный цифровой след, который имеет свойство сохраняться в первоначальном виде без каких-либо изменений на весь период своего существования, определяемый обладателем информации. Одновременно с этим информация о сотруднике, собранная посредством вышеуказанных технологий и подвергнутая соответствующему анализу, может использоваться и при создании его цифрового профиля. «Сегодня формирование и использование цифрового профиля используется и в целях отслеживания эффективности выполнения работником

[154] Пугачев В.П. Глобалистский тоталитаризм: Социальные мутации цифрового капитализма: формирование человека и манипулятивные технологии управления // М.:ЛЕНАНД. 2022. (Будущая России. № 34). С.52.

трудовой функции, и в целях проверки соответствия занимаемой должности, а также в целях поощрения сотрудников за интенсивный труд и т.п.»[155].

Данные технологии, использующиеся широко и повсеместно, имеют обширную базу рекламных предложений и продолжают совершенствоваться, что свидетельствует о наличии стойкого потребительского интереса и порождают тенденцию к их интенсивному развитию. При этом отличительной чертой последних является по сути их двойное назначение, поскольку контроль за сотрудником в виртуальной среде означает и контроль за информационной безопасностью самой организации, что в целях достижения поставленной цели не исключает, а подчас и предполагает его скрытый характер, законность установления которого вызывает ряд вопросов.

Все эти нововведения породили появление достаточно большого множества различной информации в цифровом виде природа которых до настоящего момента принципиально не определена, правовое регулирование отсутствует, а правоприменительная практика не имеет единообразного подхода. Вопрос о том, является ли рассматриваемая информация персональными данными, при каких условиях она может быть отнесена к этой категории и какие это влечет за собой последствия, подлежит тщательному исследованию, поскольку современные реалии актуализировали вопрос о правовом регулировании и защите информации, как генерируемой сотрудниками в рамках виртуального общения в процессе осуществления производственной деятельности, так и иными лицами, которые сотрудниками не являются, но относящаяся к ним информация, включая и информацию на основании которой можно установить их личность, тем не менее обрабатывается хозяйствующим субъектом.

Условно персональные данные, обрабатываемые в виртуальной среде организаций, можно сгруппировать по следующим признакам:

- *информация, получаемая от коммуникационного общения и от осуществления контрольных полномочий;*

[155] Жарова А.К., Елин В.М., Минбалеев А.В. Парадигма цифрового профилирования деятельности человека: риски, угрозы, преступления: монография // М.: РУСАЙНС, 2024. С.10.

Данная группа на настоящий момент является основополагающей, поскольку аккумулирует два основных вида создаваемой информации как главного актива в рассматриваемой области. Коммуникативное общение подразумевает под собой любой обмен информацией посредством каналов связи и с использованием сети Интернет. Например, сотрудник, находящийся на дистанционной работе, отправляет посредством сети Интернет сканированную копию своего паспорта или какого-либо иного документа. В процессе проведения видеосовещания создается его запись, а информация в корпоративном чате хранится в цифровом формате на соответствующих информационных ресурсах.

Что же касается информации, получаемой от осуществления контрольных полномочий, то здесь в качестве примера можно привести программы, фиксирующие активность работников, видеозаписи рабочего процесса и многое другое.

- *источники поступления;*

В данную группу подлежат включению персональные данные, получаемые как в рамках локального контура, так и за его пределами. Например, записи видеоконференции внутреннего потребления только между сотрудниками организации и внешнего при участии третьих лиц, не состоящих с последней в трудовых отношениях, т.к. называемых партнеров.

- *субъектный состав;*

Формируется за счет субъектов персональных данных как сотрудников организации, так и третьих лиц, входящих в коммуникативное виртуальное пространство организаций и:

- оставляющих в нем свои персональные данные в цифровом формате;

- получающих доступ к информации в цифровом формате, включая и персональные данные, как выборочно, так и непрерывно;

- получающих возможность хранить на своем компьютерном устройстве или в иной виртуальной среде (облаке) информацию в цифровом формате, включающую и персональные данные;

- получающих в силу распорядительных полномочий и/или технологического функционала (права администратора) право и/или возможность решать судьбу информации в цифровом формате, включая и персональные данные.

- *обычные персональные данные и биометрические персональные данные как предназначенные для установления личности человека, так и не предназначенные изначально для этих целей;*

При этом означенные группы, формируемые в «чистом» виде, имеют свойство перемежаться между собой, создавая коллаборацию не только со сложным набором прав и обязанностей, но и с осуществлением защиты. Например, запись видеоконференции с участием руководителей разных организаций сохранена в цифровом формате на локальном устройстве и/или в облачной среде организаций, а также на личном компьютерном устройстве каждого из участников - руководителей. При этом определенной части сотрудников предоставлен доступ к этой записи с целью ее использования для более эффективной реализации поставленных задач. Данные исполнители, в свою очередь, для удобства работы скопировали запись на свои электронные устройства.

Как можно видеть из вышеизложенного субъектный состав лиц, получивши доступ к информации конфиденциального характера, характеризуется разнообразием штатной принадлежности, а также техническими возможностями, что усиливает давление на разработанные в организациях нормативные и технологические механизмы защиты и охраны информации конфиденциального характера. В этой связи на первый план выходит нормативное регулирование данных правоотношений как в части внутренней регламентации, так и в части внешних контактов, когда сторонами могут быть разработаны и приняты для исполнения общие регламентирующие документы или стороны принимают к обоюдному исполнению требования контрагента в этой части, зарегламентированные во внутренних нормативных актах и размещенных на сайте организации для ознакомления неограниченного числа лиц, включая и потенциальных партнеров, или передаваемых для руководства при вступлении в переговорный процесс. При этом деловая активность способна самостоятельно, но

безусловно, в рамках законодательства, создавать и иные комбинации превентивных мер нормативного регулирования и защиты персональных данных в виртуальной среде своих организаций. *Предложенная в исследовании признаковая совокупность элементов, связанных с рассматриваемой информацией, направлена на определение прав и обязанностей в части обработки персональных данных и осуществления их защиты, а также оптимизацию сопряженного с этим процесса нормативного регулирования.*

Сведения, исполненные в цифровом формате, могут быть, либо персональными данными в общем значении[156], когда за основу берется сама информация и установлению подлежит наличие или отсутствие ее отношения к конкретному лицу, а не определение последнего, как ошибочно считается в некоторых случаях, либо биометрическими персональными данными, основное и единственное предназначение которых связано с возможностью установить личность человека, т.е. исключить любые сомнения в принадлежности представленных физическим лицом идентификаторов, характеризующих физиологические и биологические особенности, именно этому лицу. При этом для обработки персональных данных в общем понимании необходимо согласие субъекта персональных данных, выраженное в любой форме, позволяющей подтвердить факт его получения, в отличие от обработки биометрических персональных данных, использующихся исключительно для установления личности человека, когда вышеуказанное согласие должно быть в обязательном порядке исполнено в письменной форме или в форме электронного документа, подписанного электронной подписью[157].

По мнению У.М. Стансковой в рамках трудовых и иных непосредственно связанных с ними отношениях информация ограниченного доступа представляет собой совокупность определенных в нормативном порядке сведений, обладающих действительной или потенциальной коммерческой либо социальной ценностью, в

---

[156] При этом сведения, характеризующие физиологические и биологические особенности человека, но не использующиеся для установления его личности, т.е. являющиеся персональными данными в общем понимании, также следует именовать биометрическими.

[157] Пункт 4 статьи 9 Закона о персональных данных.

отношении которых субъектами трудового права установлен режим конфиденциальности с целью ограничения их неправомерного использования и (или) разглашения[158]. При этом трудовым законодательством цели обработки персональных данных строго регламентированы посредством закрытого перечня, согласно которому это исключительно: обеспечение соблюдения законов и иных нормативных правовых актов; содействие работникам в трудоустройстве; получение образования и продвижение по службе; обеспечение личной безопасности работников; контроль количества и качества выполняемой работы и обеспечение сохранности имущества[159]. Указание на исключительность целей обработки персональных данных работников свидетельствует об установлении запрета на их обработку в иных целях.

При этом виртуальная среда организации уже объективно давно пополняется информацией за счет использования специальных технических средств и прикладных программных продуктов, ориентированных как на организацию совместного рабочего процесса в рамках дистанционного доступа с его цифровой фиксацией, так и на современные методы контроля, преследующие различные цели, например отслеживание времени работы сотрудников в режиме удаленного доступа, а также на обеспечение информационной и иной безопасности самой организации. Зачастую цифровая фиксация может являться неотъемлемой частью самой технологии, например чат для онлайн переписки, изначально созданный для сохранения передаваемого текста, или применяться как отдельный инструмент в виде аудио-видео записи совещаний и аналогичных мероприятий массового характера, определяющих или координирующих рабочий процесс.

Формально на настоящий момент законные основания для обработки вышеуказанной информации отсутствуют, поскольку, как указывалось выше, цели обработки персональных данных в Трудовом Кодексе РФ строго определены и рассматриваемые надобности в их перечень не входят. Именно по этой причине не исключено возникновение спорных ситуаций, когда сотрудник посчитает для себя

---

[158] Станскова У.М. Трудоправовые средства обеспечения конфиденциальности информации ограниченного доступа. автореф. дис. … канд.юрид.наук. Екатеринбург, 2014. С. 5.
[159] Часть 1 статьи 86 ТК РФ.

возможным не давать своего согласия на обработку персональных данных в иных целях, чем предусмотрено в вышеуказанной статьей Трудового Кодекса РФ. С одной стороны, правовое обоснование таких действий работника вполне обосновано, а с другой стороны, они вступают в противоречие с заинтересованностью работодателя, что свидетельствует о наличии дисбаланса в соблюдении обоюдных интересов.

*Безусловно, рассматриваемые запросы работодателей в современных условиях вполне оправданны и с экономической, и с организационной точек зрения, в связи с чем представляется целесообразным дополнить перечень целей обработки персональных данных работников за счет включения в него таких целей, как организация совместного рабочего процесса в виртуальной среде организации с возможностью его цифровой фиксации, а также контроль за информационной безопасностью организации.*

Организация рабочего и переговорного процессов в режиме виртуального общения доступна на базе облачных платформенных разработок, предназначенных для коллективной работы. Аудио-, видеозапись совещаний и иных мероприятий с участием как деловых партнеров, являющихся сотрудниками разных организаций, так и с участием сотрудников одной организации требует детального рассмотрения, связанного с выявлением определенных нюансов при получении согласия на обработку персональных данных и ее хранении. Запись конференций в вышеуказанных форматах может осуществляться как в облако, так и на локальный компьютер, где эти файлы и будут сохранены. Что же касается информации, хранящейся в облаке, то любой участник конференции может получить ее по ссылке, которая будет направлена на его электронный адрес после обработки запроса. Полученные файлы можно загрузить на персональный компьютер в режим хранения, при том что владельцем последнего может являться как сама организация, так и физическое лицо, участвовавшее в конференции от имени юридической структуры или от себя лично. В любом случае будет иметь место хранение биометрических персональных данных на локальном компьютере, в связи с чем возникает вопрос о наличии обработки персональных данных, что при

положительном разрешении поставленного вопроса сопряжено с получением соответствующего согласия субъекта. Как правило, функционал программного обеспечения настроен таким образом, что каждый участник при присоединении к конференции, которая записывается, или когда организатор начинает запись, получает запрос на предоставление соответствующего согласия. Если участник своего согласия на запись не дает, он покидает конференцию.

Законодательные определения персональных данных позволяют сделать однозначный вывод о том, что рассматриваемая информация является персональными данными, поскольку имеет отношение к прямо определенным субъектам и характеризует их физиологические и биологические особенности, на основании которых можно установить их личность. При этом отношения, связанные с персональными данными, подразумевают обязательное присутствие оператора персональных данных, в качестве которого могут выступать как юридические, так и физические лица, организующие и (или) осуществляющие обработку персональных данных, определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В этой связи крайне важно правильное понимание статуса лиц, на чьих компьютерах будут храниться персональные данные участников конференций. Поскольку юридические лица создаются для осуществления определенной деятельности, а действие Закона о персональных данных не распространяется на отношения, возникающие при обработке персональных данных физическими лицами исключительно для личных и семейных нужд, последние могут выступать в качестве операторов персональных данных только в том случае, если осуществляют профессиональную или иную предпринимательскую деятельность, сопряженную с извлечением прибыли (индивидуальные предприниматели, самозанятые).

Цели обработки персональных данных должны соответствовать видам деятельности, в противном случае обработка будет являться произвольной, что нарушит задекларированный принцип законности и справедливости[160]. В этой

[160] Пункт 1 статьи 5 Закона о персональных данных.

связи работники организации, на чьих персональных компьютерах, например по причине того, что он является организатором конференции, будут храниться аудио и видеозаписи совещаний и т.п. мероприятий, не должны рассматриваться в качестве самостоятельных операторов, поскольку последними будут выступать работодатели, организовавшие сбор персональных данных, определившие цели их обработки, а сотрудники, в порядке выполнении своей трудовой функции, возможно расценивать как действовавших от имени и в интересах работодателя. Впоследствии данные сведения могут быть переданы на локальный компьютер работодателя, а у сотрудника также может остаться копия записи, равно как и у других участников конференции, которые запросили аудио-, видеозапись с локального компьютера или из облака и скопировали ее на свой персональный компьютер. Данные участники конференции в аналогичном порядке не могут быть признаны операторами персональных данных, а хранение у них на компьютере вышеуказанной информации не будет являться обработкой персональных данных.

Самым распространенным и достаточно давно использующимся источником получения информации в цифровом формате является видеонаблюдение, которое устанавливается в различных местах на территории работодателя, за некоторыми исключениями как по морально-этическим запретам и соображениям, так и в соответствии со сложившейся правоприменительной практикой, и, по сути аккумулирующее информацию, характеризующую физиологические особенности сотрудников. Речь пойдет о таких биометрических персональных данных, которые изначально не собираются для использования в целях установления личности. При этом процедура видеонаблюдения во всем своем практическом многообразии до настоящего времени не имеет четкого регулирования в нормах действующего законодательства, в связи с чем вопрос о том, во всех ли случаях данные видеозаписи сотрудников необходимо относить к категории персональных остается открытым.

По целям видеонаблюдение условно можно разделить на две основные категории, связанные с наблюдением конкретно за сотрудниками, например на их рабочих местах, и не связанные с этой целью, когда видеонаблюдение необходимо

для сохранности какого-то имущества или обеспечения территориальной безопасности. Попадание же сотрудников в «кадр» является неизбежным явлением, но не главной целью.

Возможность установления наблюдения конкретно за сотрудниками предусмотрена частью 1 статьи 214.2 Трудового Кодекса РФ, согласно которой работодателю предоставлено право использовать в целях контроля за безопасностью производства работ приборы, устройства, оборудование и (или) комплексы (системы) приборов, устройств, оборудования, обеспечивающих дистанционную видео-, аудио- или иную фиксацию процессов производства работ и возложена обязанность обеспечивать хранение полученной информации.

Что же касается установления видеонаблюдения в целях территориальной безопасности, при которой неизбежно фиксирование различных сотрудников, то какие-либо четко определенные законодательные запреты на это отсутствуют. И в том и в другом случае работодатель, являющийся оператором персональных данных, будет хранить информацию, характеризующую физиологические и особенности сотрудников, т.е. обрабатывать их биометрические персональные данные.

Исходя из того, что биометрическими персональными данными, согласно данному в Законе определению, являются сведения, характеризующие вышеуказанные особенности человека, вся информация, зафиксированная с помощью приборов, устройств, оборудования и (или) комплекса (системы) приборов, будет во всех случаях являться персональными данными сотрудников, согласие на обработку которых формально можно получить в любой форме, позволяющей подтвердить этот факт, но все же целесообразнее заручиться согласием, исполненным в письменной форме, по причине того, что при наступлении определенных обстоятельств биометрические персональные данные сотрудников могут быть использованы для установления личности, например, в случае повреждения имущества на основании записи видеонаблюдения будет установлено лицо, причинившее ущерб. Данные практические рекомендации связаны с определенным свойством, присущем биометрическим персональным

данным, - переходить при наличии к тому определенных обстоятельств из одной категории, не связанной с установлением личности, в другую, противоположную по своему назначению, при которой согласие на обработку персональных данных должно быть дано исключительно в письменной форме.

Что же касается целей обработки персональных данных работников, то установление камер видеонаблюдения в общественных, производственных и иных местах на территории хозяйствующего субъекта вполне соответствует и обеспечению личной безопасности работников, и сохранности имущества. Исключением из правила является запрет на установление видеонаблюдения в таких помещениях, которые используются для отдыха, переодевания, приема пищи, поскольку последние не используются для производственной деятельности и речь уже идет о праве сотрудников на неприкосновенность частной жизни, т.е. «всего того, что касается человека и не подлежит контролю ни с чьей стороны»[161]. При этом ведение скрытого видеонаблюдения с точки зрения действующего законодательства вряд ли можно признать законным, поскольку все персональные данные работника следует получать у него самого, что подразумевает под собой изначальное уведомление последнего о видеофиксации и, как следствие, получение согласия на обработку персональных данных, решение о чем принимается субъектом персональных данных свободно, своей волей и в своем интересе. В этой связи является крайне сомнительным вывод суда в одном из дел[162], согласно которому действующее трудовое законодательство не содержит обязанности работодателя ставить в известность работника, равно как и получать его согласие на установку системы видеонаблюдения для целей безопасности. Противоречит данный вывод и положениям статьи 21 Трудового Кодекса РФ, согласно которой

---

[161] Определение Конституционного Суда РФ от 09.06.2005 № 248-О "Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом "б" части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации" // СПС Консультант.

[162] Апелляционное определение Свердловского областного суда от 16.11.2016 по делу № 33-20507/2016 https://leninskytag--svd.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=707479&delo_id=1540005&new=0&text_number=1 (дата обращения 24.12.2024).

работник имеет право на получение полной достоверной информации об условиях труда и требованиях охраны труда на рабочем месте.

На настоящий момент существует и практически используется довольно обширный спектр технических решений, которые позволяют осуществлять контроль за работой сотрудников и информационной безопасностью самой организации посредством анализа поведения пользователей, в нашем случае – работников, и которые являются источником накопления персональных данных в каждой конкретной организации. При этом рассматриваемые технологии по своей сути являются методами слежения, в связи с чем необходимо рассмотреть вопросы как о законности их применения, так и о том, возможно ли отнесение получаемой информации пользовательского характера к персональными данными и к какой конкретно категории – общей или все же специальной, характеризующей физиологические и биологические особенности человека.

Осуществление контроля за соблюдением сотрудниками правил внутреннего трудового распорядка, исполнением ими своих трудовых обязанностей, а также за бережным отношением к имуществу является правом работодателя[163]. Одновременно с этим какие-либо законодательно установленные требования или ограничения к методам контроля отсутствуют, в связи с чем спектр предложений достаточно широк и находится в непрерывном развитии. В свете рассматриваемой проблематики работники вне зависимости от того, будет ли информация, полученная в результате осуществления контроля причислена к категории персональных данных или нет, в любом случае должны быть поставлены в известность обо всех формах контроля, в связи с тем, что это значимые условия труда, а работник имеет право на полную и достоверную о них информацию. Если же информация, получаемая в связи с использованием современных технологий контроля, будет являться персональными данными, получение согласия субъектов на их обработку является обязательным, что практически невозможно без уведомления последних о применении технологий контроля.

[163] Статья 22 ТК РФ.

Отдельно следует обратить внимание и на технический аспект рассматриваемой проблемы, связанный с тем, на чьем компьютере предполагается установка программ контроля: на компьютере, принадлежащим работодателю или сотруднику. Если в первом случае данная процедура проходит без участия работника, что предполагает изначально отсутствие его осведомленности, то установка программы на личном компьютере сотрудника вряд ли может пройти без его ведома, в связи с чем последний в любом случае будет проинформирован о предполагаемых методах контроля, а факт установки им соответствующей программы вполне допустимо расценивать как выражение согласие на применение самого контроля.

Таким образом, одним из аспектов при разрешении вопроса о том, относится ли информация, получаемая в результате информационного контроля, к прямо определенному или косвенно определяемому лицу, будет его «привязка» к четко определенному компьютеру. Что же касается самой информации, фиксируемой системами контроля, то условно ее возможно поделить на информацию, просто имеющую отношение к конкретному субъекту – работнику, и информацию, характеризующую физиологические особенности сотрудников. В первом случае получаемые сведения носят по большей части информационно-статистический характер, поскольку связаны с разного рода мониторингом, например, программ, которые использовал работник, и сайтов, которые он посещал; результатов запросов в поисковых системах; социальных сетей, в которых сотрудник был активен; открывавшихся, изменявшихся, удалявшихся и пересылавшихся сотрудником файлов, а также файлах, отправлявшихся на печать; переписки по e-mail и в мессенджерах; скриншотов экрана компьютера, позволяющих фиксировать все действия сотрудника за компьютером; контроля USB-портов и устройств; информации обо всех нажатиях клавиш во всех программах и многое другое.

Сведения, получаемые в результате вышеуказанных методов контроля, относятся к прямо определенным сотрудникам, поскольку целью рассматриваемого мониторинга является деловая активность конкретного сотрудника. Именно на основании этих сведений работодатель получает возможность определить, в

частности, наименее активных и, напротив, наиболее продуктивных сотрудников с целью их поощрения и продвижения по службе, а также установить виновника в нарушении информационной безопасности. При таких обстоятельствах всю вышеуказанную информацию следует отнести к категории персональных данных, поскольку таковой информацией являются любые сведения независимо от формы их представления, и она имеет непосредственное отношение к прямо определенным сотрудникам.

Одновременно с этим в целях контроля работодатель может задействовать и такие программы, которые позволяют осуществлять запись разговоров по микрофону, а также видео с веб-камер, включая и снимки, период обновления которых устанавливается по желанию работодателя. Сведения такого рода уже являются биометрическими персональными данными, поскольку характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

*Поскольку современные технологии существенно изменили и продолжают менять процесс производственный деятельности, привнося в него новые возможности, представляется целесообразным закрепить на законодательном уровне право работодателя использовать в целях контроля за выполнением сотрудниками своих трудовых обязанностей, а также в целях осуществления информационной безопасности помимо приборов, устройств, оборудования и (или) комплексов (систем) приборов, устройств, оборудования, обеспечивающих дистанционную видео-, аудио- или иную фиксацию процессов производства работ, информационные технологии (методы и инструменты) контроля работы сотрудников.*

***Таким образом, по результатам проведенного исследования можно сделать следующие выводы:***

*- виртуальная среда организации характеризуется совокупностью нормативных правовых и локальных актов, иной документацией, которые регламентируют и устанавливают модели коммуникаций, виды используемых технологий, способы обработки персональных данных и их перечень, круг*

*субъектов, вовлекаемых в процесс создания информации и претендующих на доступ к информации конфиденциального характера, контура сетей и многого другого, что формирует основу правоотношений, а также виртуальной инфраструктурой: технологиями, программным обеспечением, вычислительными мощностями и иными технологическими решениями;*

*- в целях совершенствования механизма регулирования и защиты персональных данных в виртуальной среде организаций предлагается использовать группы, сформированные на основе признаковой общности;*

*- виртуальная среда организаций строго индивидуальна и обладает отличительными чертами, что надлежит учитывать в процессе нормотворчества как на законодательном, так и на локальном уровне;*

*- необходимо разработать механизм добровольного принятия прав и возложения обязанностей по защите персональных данных лицами, совместно ими владеющими;*

*- необходимо на законодательном уровне дополнить перечень целей обработки персональных данных работников за счет включения в него совместного рабочего процесса в виртуальной среде организации с возможностью его цифровой фиксации, а также контроль за информационной безопасностью организации;*

*- закрепить на законодательном уровне право работодателя использовать в целях контроля за выполнением сотрудниками своих трудовых обязанностей, а также в целях осуществления информационной безопасности помимо приборов, устройств, оборудования и (или) комплексов (систем) приборов, устройств, оборудования, обеспечивающих дистанционную видео-, аудио- или иную фиксацию процессов производства работ, информационные технологии (методы и инструменты).*

## § 2. Использование и распоряжение персональными данными в виртуальной среде организаций

Деятельность любой хозяйствующей структуры, а особенно в настоящее время, приводит к появлению и накоплению достаточно большого объема информации в цифровом формате. Как верно указано Е.И. Казакевич, отношения между субъектом персональных данных и оператором представляют собой отношения экономической асимметрии, так как оператор имеет значительные экономические преимущества за счет обладания массивами больших данных[164]. При этом рассматриваемая информация, вне всякого сомнения, имеет практическую ценность, а современные технологии позволяют извлекать из нее максимально полезный результат, что уже и происходит повсеместно, к примеру, в области осуществления контрольных функций в совокупности с обеспечением информационной безопасности, построения стратегии экономического развития за счет аналитики внутренней среды и внешнего окружения. По мнению Т.А. Терещенко и А.П. Сергеева предметом коммерческого интереса и, как следствие, оборотоспособным объектом признается не только постоянно видоизменяющийся большой объем самой разнообразной информации с учетом различных источников сбора, но и те новые знания, включая различные прогнозы и алгоритмы оценки тех или иных ситуаций, которые являются следствием специфической и высокоскоростной деятельности по постоянному анализу собираемых сведений с помощью различного специального инструментария[165]. Так, для достижения подобных целей современная действительность активно привлекает технологии искусственного интеллекта, как наиболее эффективное средство анализа информационного потока, порождаемого человеческой деятельностью. Интеграция искусственного интеллекта с иными технологиями позволяет создавать такие сервисные продукты, которые направлены на улучшение продуктивности рабочих

[164]Казакевич Е.И. Защита прав и свобод человека при обработке персональных данных в период цифровой трансформации // Уральский журнал правовых исследований. 2022. № 4. С.40

[165] Сергеев А.П., Терещенко Т.А. Большие данные: в поисках места в системе гражданского права // Закон. 2018. № 11. С. 106–123.

процессов за счет многих показателей, использующихся в формируемой отчетности. Например, искусственный интеллект, встроенный в сервис платформы для проведения совещаний и общения в чатах, способен составлять протокол совещаний с акцентированием внимания на все обстоятельства обсуждения, такие как идеи, доводы и др., повлиявшие на принятие конечного результата. Видеозапись совещаний, как внутренних, так и с внешним элементом, предполагается к доступу всем участникам для возможности повторных просмотров, в связи с чем вся эта информация, содержащая и биометрические персональные данные в том числе, в целях организации производственного процесса может циркулировать внутри предприятия и выходить за пределы его виртуального пространства с иной внешней фиксацией. При этом в нормах действующего законодательства отсутствует прямая регламентация рассматриваемой цифровой действительности, в связи с чем легальность ее уже реального существования может быть подтверждена с помощью правового анализа норм, действующих в области персональных данных и иных областях информационного регулирования.

Правовое регулирование использования персональных данных в виртуальной среде организаций нуждается в установлении соотношения прав субъектов персональных данных и организаций на вышеуказанную информацию. В нормах действующего законодательства отсутствует понятие или какое-либо иное указание на собственника информации. Вместо этого в правовой оборот включено понятие «обладатель информации»[166], которым является лицо[167], самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

При этом цель, которую преследовал федеральный законодатель, вводя понятие «обладатель информации», заключается в описании - по аналогии с гражданско-правовыми категориями «собственник», «титульный владелец», но с

---

[166] Пункт 5 статьи 2 Закона об информации, информационных технологиях и о защите информации.

[167] Гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование (пункт 1 статьи 6 Закона об информации, информационных технологиях и о защите информации).

учетом особенностей информации как нематериального объекта - правового статуса лица, правомочного в отношении конкретной информации решать вопрос о ее получении другими лицами и о способах ее использования как им самим, так и другими лицами[168]. Таким образом, обладатель информации – это правовой статус, возникновение которого обусловлено либо фактом создания информации, либо получением на основании закона или договора права разрешать или ограничивать доступ к ней. Содержание нормы-дефиниции понятия «обладатель информации», раскрытое Г.Г. Камаловой, позволяет выделить первичного обладателя как лицо, создавшее информацию в ходе творческой или иной деятельности, и вторичного обладателя как лицо, правомерно получившее на основе договора или закона сведения, изначально созданные иным лицом. Первый из них имеет полный спектр прав на информацию, включая право интеллектуальной собственности, в предусмотренных законом случаях и право ограничивать доступ к сведениям своей волей и в своем интересе, кроме случаев действия норм-исключений, а второй – правомочия, зафиксированные в договоре или законе, на основании которых получены сведения. Поэтому, по сути, он является пользователем (держателем) информации, обязанным ограничивать доступ к ней в случаях и порядке, предусмотренных договором или законом[169]. Под доступом к информации понимается возможность ее получения и использования[170]. При этом субъект персональных данных может приобрести правовой статус обладателя информации двумя вышеуказанными путями – как посредством самостоятельного создания информации, так и вследствие получения его на основании закона. Так, к примеру, паспортные данные, ИНН, СНИЛС и им подобные идентификаторы присваиваются гражданину органами государственной власти, т.е. создаются непосредственно ими, в связи с чем государство в лице последних является обладателем этой информации. Но одновременно с этим и

---

[168] Постановление Конституционного Суда РФ от 26.10.2017 № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А.И. Сушкова» // СПС «Консультант Плюс».

[169] Камалова Г.Г. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества. дис. … канд. юрид. наук. М., 2020. С. 115.

[170] Пункт 6 статьи 2 Закона об информации, информационных технологиях и о защите информации.

гражданин на основании закона становится ее обладателем, поскольку получает ее на основании законов с правом разрешать или ограничивать доступ к ней. Таким образом, обладателем информации о гражданине, включая и персональные данные, может быть как сам гражданин, так и иные лица в определенных случаях.

Что же касается оператора персональных данных, в рассматриваемом случае работодателя, то последний также может стать обладателем информации о сотруднике, включая и персональные данные, которую он создал сам, например, табельный номер сотрудника, индивидуальный пароль работника для вхождения в локальную сеть или какой-либо иной внутрикорпоративный идентификатор, который после расторжения трудовых отношений остается у работодателя. Вообще это может быть любая информация, которая не только создана работодателем, но и по-иному связана непосредственно с ним, но при этом временно имеющая отношение к прямо определенному или косвенно определяемому физическому лицу. Так, это могут быть данные находящегося в собственности работодателя персонального компьютера, закрепленного исключительно за одним работником, например IP-адрес, пароль для входа, номер и иные данные видеокамеры для съемки процесса осуществления трудовой функции, что, в частности, можно наблюдать у сотрудников, проверяющих билеты в транспорте, телефонного аппарата, также переданного сотруднику в процессе работы, и многое другое. Таким образом, возникает ситуация, при которой информация, обладателем которой является работодатель, становится персональными данными сотрудника, поскольку имеет к нему отношение и на основании этой информации данного сотрудника можно определить прямо или косвенно, при том, что последний статус обладателя информации не приобретает.

Вопрос о принадлежности правового статуса важен с точки зрения распределения прав и обязанностей, поскольку только обладатель информации имеет права, позволяющие решать «судьбу» информации, что в отношении персональных данных выражается в обязательности получения согласия субъекта на обработку персональных данных, а также в осуществлении иных прав, связанных с отзывом согласия на обработку персональных данных, а также с их

уточнением, блокировкой, уничтожением и другими действиями, перечень которых дан в Законе о персональных данных. Таким образом, на обработку персональных данных – информации, обладателем которой является работодатель, согласие субъекта персональных данных не требуется, что тем не менее не исключает возможность предъявления субъектом персональных данных некоторых требований, например связанных с уточнением персональных данных при изменении внутрикорпоративных идентификаторов, присвоенных конкретному лицу. *В этой связи представляется целесообразным отражать в политике обработки персональных данных случаи, при которых работодатель будет являться обладателем информации – персональных данных сотрудника, что, исходя из анализа законодательных норм, не требует получения согласия последнего на обработку этих персональных данных.*

Что же касается персональных данных – информации, созданной непосредственно субъектом персональных данных, - то именно он будет являться ее обладателем. При этом всем обладателям информации, если иное не предусмотрено федеральными законами, предоставляются следующие права[171]:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Одновременно с этим Закон о персональных данных предоставляет субъекту персональных данных дополнительные права, в частности требовать от оператора

[171] Статья 6 Закона об информации, информационных технологиях и о защите информации.

уточнения его персональных данных, их блокирования или уничтожения, в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки[172]. Также субъекту персональных данных предоставлено право отозвать свое согласие на обработку персональных данных и заявить требование о прекращении их обработки, что в итоге влечет за собой уничтожение персональных данных в установленные законодательством сроки[173].

Что же касается норм трудового законодательства, то здесь субъекту персональных данных предоставлено только право требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового Кодекса РФ или иного федерального закона. При этом действующее законодательство не раскрывает понятия «исключение» персональных данных и не определяют последствий от совершения данного действия. Операция «исключение» не входит в понятие обработки персональных данных, поскольку перечень действий (операций) или совокупности действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными не включает в себя такого действия. *Подобная правовая неопределенность требует законодательного уточнения с целью исключения разного рода толкований, которые способны породить возникновение судебных споров.*

Тем не менее это не лишает работника права реализовать любое из тех общих прав, которые предоставлены субъекту персональных данных иными федеральными законами, поскольку согласно пункту 2 статьи 86 Трудового Кодекса РФ при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом РФ и иными федеральными законами. В рамках исследования представляется необходимым рассмотреть вопрос о соотношении

[172] Статья 21 Закона о персональных данных.
[173] Статья 9 Закона о персональных данных.

данных прав и возможных последствиях их реализации при использовании персональных данных в виртуальной среде организаций.

По общему правилу, любой субъект персональных данных, включая и имеющего статус работника, вправе отозвать свое согласие на их обработку, потребовать прекращения обработки, блокирования и, как итог, уничтожения персональных данных, что может являться не только нецелесообразным по тем или иным причинам, но и откровенно вредным. Данные права предоставлены субъекту персональных данных вне какой-либо зависимости от потребностей работодателя, учета его интересов и самой возможности их исполнения, что вряд ли можно признать правильным. Совершенно очевидно, что в некоторых случаях удовлетворить требование сотрудника о прекращении обработки его персональных данных просто невозможно. Так, объективно не может быть прекращена обработка персональных данных, связанных, к примеру, с начислением и выплатой заработной платы, в связи с тем, что информация подобного рода необходима работодателю и срок ее обязательного хранения установлен законодательством. *В этой связи представляется целесообразным определить на законодательном уровне либо признаки персональных данных, отзыв согласия на обработку которых не повлечет за собой для работодателя обязанности прекратить их обработку, либо предоставить работодателю возможность самостоятельно определять эти виды персональных данных.*

Но имеется и иная категория персональных данных, нуждаемость в которой обусловлена как производственной, так и иной необходимостью, но без обработки которых работодатель вполне способен исполнять все свои обязательства как перед сотрудником, так и перед государством. Например, видеозаписи совещаний, конференций и иных подобных мероприятий, нуждаемость в которой обусловлена исключительно производственной необходимостью, направленной на более эффективное использование имеющихся ресурсов, обеспечением сохранности имущества и иными целями, а также персональные данные, генерируемые программными продуктами, связанными с осуществлением работодателем контрольных функций в совокупности с обеспечением информационной

безопасности. Несмотря на то что обработка работодателем вышеуказанных персональных данных имеет место повсеместно, законодательно установленное дозволение на это фактические отсутствует, поскольку перечень целей обработки персональных данных, содержащийся в Трудовом Кодексе РФ и расширительному толкованию не подлежащий, обработку персональных данных в вышеуказанных целях не предусматривает. В этой связи работники имеют право требовать от работодателя прекращения обработки таких персональных данных и их уничтожения, что не всегда соответствует интересам и потребностям последнего.

На современном этапе одним из путей решения рассматриваемой проблемы, а равно и проблемы использования персональных данных помимо устранения имеющихся пробелов на законодательном уровне является возможность придания работодателю статуса обладателя этой информации, что предоставляет последнему широкий круг полномочий по распоряжению персональными данными, накопляемыми в виртуальной среде организаций. Стать обладателем данной информации работодатель может на основании договора, заключаемого с работником, в соответствии с которым последний наделяет его правом разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Наделение оператора персональных данных правовым статусом обладателя информации позволяет на законных основаниях использовать персональные данные, получаемые в процессе деятельности сотрудника, и в иных целях, не поименованных в Трудовом Кодексе РФ, а также является законным способом предоставления оператору персональных данных таких прав, которые с учетом определенной специфики присущи категориям «собственник» и «титульный владелец». Все это существенно расширяет горизонт возможного использования персональных данных в соответствии с реальными потребностями и обеспечивающим их технологическим развитием. При этом какой-либо специальный регулятивный инструмент для такого рода договоров законом и иными нормативными правовыми актами не разработан, в связи с чем следует руководствоваться общими положениями о договоре, а также правилами об аналогии закона.

В качестве предмета договора следует рассматривать предоставление права разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам, и/или право в отношении конкретной информации решать вопрос о ее получении другими лицами и о способах ее использования. Данное определение предмета договора является общим и дословно основано на формулировках Закона об информации, а также Конституционного Суда РФ, данных в вышеуказанном постановлении от 26.10.2017 № 25-П. При этом ключевым, а равно существенным условием договора следует считать именно информацию, в связи с чем в договоре в обязательном порядке должна указываться либо конкретная информация, либо признаки, по которым она будет определяться, в противном случае договор может быть признан незаключенным. Такими признаками могут быть различные обстоятельства, позволяющие выделить информацию в какую-либо отдельную группу как в широком смысле, например информация, создаваемая в процессе деятельности организации, так и в более усеченном варианте - видеозаписи совещаний, данные иного коммуникативного общения и многое другое.

Поскольку речь идет о договоре, при отсутствии каких-либо специальных императивных предписаний, то стороны договора вправе предусмотреть в нем любые условия, но, разумеется, в рамках действующего законодательства. Так, вполне возможно включить в договор условие, связанное с выплатой работнику вознаграждения за предоставление вышеуказанных прав как в денежном выражении, так и иным способом. При этом, следует заметить, это единственный способ, предоставляющий субъекту персональных данных возможность получения материальной или иного рода выгоды от использования оператором его персональных данных. Как бездоговорную альтернативу можно привести скидочные преференции в торговых предприятиях, предоставляемые в случае передачи субъектом своих персональных данных и оформляемых посредством выдач карт покупателя.

Представляется, что особое внимание в договоре следует уделить правам и обязанностям сторон, где должно быть четко указано какие операции с информацией, права на которые передаются в адрес работодателя, может совершать

последний. Допустимо наряду с перечислением общих прав обладателя информации, содержащихся в статье 6 Закона об информации, информационных технологиях и о защите информации, включение в договор и их более конкретизированных аналогов, а равно наложение запретов на осуществление каких-либо действий с предоставляемой информацией. Как и всякий другой, рассматриваемый договор должен быть заключен на определённый срок, последствия истечения которого должны быть предусмотрены в договоре. Так, например, работодатель утрачивает статус обладателя данной информации и соответствующие права, но может продолжать осуществлять обработку персональных данных или, напротив, должен их уничтожить.

Не менее важным является и условие о расторжении договора в одностороннем порядке и отказа от договора. Несмотря на то что заключение договора исключает для субъекта персональных данных право требовать прекращения обработки последних, отзывать свое согласие на обработку, немотивированный отказ от договора с обязательством уничтожения персональных данных может быть предусмотрен условиями договора. Работодатель также может располагать вышеуказанными правами, например когда необходимость в использовании персональных данных себя исчерпала. При этом следует учитывать, что на период действия договора субъект персональных данных утрачивает либо все, либо какую-то часть прав на эту информацию в зависимости от условий договора, а после прекращения последнего информация в виртуальной среде организации либо перестает существовать, в связи с ее уничтожением, либо может быть передана в адрес субъекта персональных данных, например какие-то видеозаписи, аудиозаписи, данные мониторинга и другое.

По своей природе положение субъекта персональных данных сродни статусу автора произведения, поскольку информация создается именно этим человеком и имеет отношение к нему, но, заключая такого рода договор, субъект передает либо все права, либо их часть в адрес работодателя на весь срок действия договора. Жизненный же цикл персональных данных совпадает со сроком действия договора, либо сроком их последующей обработки, либо длится до момента уничтожения ее

самим субъектом персональных данных в случае, когда информация была передана ему после истечения срока действия договора или его досрочного прекращения.

Использование данной правовой конструкции вполне возможно и в ситуации, когда в качестве цели определен сбор какой-либо информации персонального по своей природе характера, который может иметь место и в виртуальной среде посредством интернет-технологий, что достаточно важно, поскольку такие персональные данные представляют собой еще статистический и научный интерес, целевая обработка которых также способна принести полезный результат.

Так, основой Индустрии 4.0, целью которой является создание полностью автоматизированного цифрового производства, управляемого с помощью программного обеспечения более высокого уровня в режиме реального времени, является повсеместный сбор цифровых данных для их оценки и дальнейшей обработки системам искусственного интеллекта[174]. Предполагается, что с помощью данной технологии использование больших данных позволит повысить эффективность принимаемых стратегических решений, направленных на усовершенствование рабочего процесса, как на уровне одной, отдельно взятой хозяйствующей единицы, так и всей отраслевой экономики.

В дополнение к сказанному, накапливаемые таким образом персональные данные пользовательского и коммуникационного характера, вне всякого сомнения, могут иметь еще и обширное научно-практическое применение, поскольку и технологии искусственного интеллекта, основанные на машинном обучении, и технологии идентификации личности с применением биометрических персональных данных остро нуждаются в огромном количестве информации, как для получения новых результатов, так и для совершенствования уже имеющихся. Уже сейчас имеется множество инновационных проектов в области ML (Machine Learning)-разработок, нуждающихся в большом количестве исходных данных (датасетов) для обучения и формирования обученной модели. Поскольку принцип работы ML предполагает непрерывное обучение, а точность обученной модели

[174] Фомина А.В., Мухин К.Ю. Индустрия 4.0. Основные понятия, преимущества и проблемы // Экономический вектор. 2018. № 3 (14). С. 33.

напрямую зависит от количества и разнообразия базовой информации, потребность в последней будет нарастать в геометрической прогрессии, ведь недаром стала «крылатой» цитата британского математика и эксперта в области анализа данных Клайва Хамби, что «данные – это новая нефть»[175].

Не исключено, что в будущем предоставление обезличенных данных вообще станет обязанностью, аналогичной уплате законно установленных налогов, поскольку для достижения общественных благ и защиты государства последнее нуждается в технологиях искусственного интеллекта, развитие которых напрямую зависит от количественного и качественного состава датасетов. Если налоги – это необходимая плата членов общества для содержания страны и получения общественных благ, то обязанность предоставления данных – можно охарактеризовать как необходимый вклад, без которого невозможно развитие научного и технического потенциала страны, поскольку в современных реалиях жизнеспособным можно считать только такое общество, которое избрало инновационный способ развития. И если ключевой потребностью для такого развития становятся информационные данные, то вполне может возникнуть настоятельная необходимость обязать каждого вносить свой посильный вклад, поскольку: «Индивид центральная фигура происходящего, от которого зависит, насколько возможно станет прогнозируемое будущее, в том числе и в шестом технологическом укладе. Никакая самоуправляемая система просто невозможна без него, так как категория человеческого капитала определяет структуру нашего общества»[176].

Спектр возможного использования накопляемого массива персональных данных в виртуальной среде организаций крайне обширен: например, за денежное вознаграждение предоставлять эти обезличенные данные в пользование коммерческим инвесторам или, напротив, на безвозмездной основе научным организациям с получением каких-либо налоговых преференций, вплоть до использования в собственных научно-практических целях, ведь многие

[175] Алексеев К.Н. Роль больших данных в цифровой экономике // Цифровая экономика. 2019. № 3 (7). С. 93.
[176] Вздорова Л.П. Шестой технологический уклад: новый формат мира // Символ науки. № 9. 2020. С. 60-61.

организации уже располагают обширным штатом IT-специалистов, занимающихся предметными разработками в той или иной области на основе ML-технологий. Так, по мнению Ю.П. Шальновой «монетизация данных – это современный бизнес-процесс, при котором генерируемые организацией и внешние данные используют для получения измеримой экономической выгоды (создание реальной стоимости из данных)»[177]. Вопрос создания легальной площадки или рынка обезличенной персональной информации уже далеко не новый, взять хотя бы «регулятивные песочницы» (Regulatory Sandbox), создаваемые во многих странах, начиная с 2016 года. Данный институт направлен на тестирование новых технологических решений, на который не распространяются рестрикции действующего правового регулирования[178].

В России до принятия 31 июля 2020 года Федерального закона № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»[179] отсутствовало общее регулирование экспериментальных правовых режимов. С введением же в действие данного нормативного правового акта впервые у государства, научного и бизнес-сообщества появился системный механизм тестирования в реальных правоотношениях технологий, которые в силу разных причин (прежде всего – инертность законодательства) использовать сегодня нельзя или затруднительно (искусственный интеллект, блокчейн, большие данные, нейротехнологии, квантовые технологии, виртуальная реальность). В рамках экспериментальных правовых режимов в сфере цифровых инноваций (ЭПР) Правительство может дать ограниченному числу компаний на определенной территории и на определенное время соблюдать действующее законодательство с рядом особенностей. Эти особенности как раз и позволят применять соответствующие технологии[180].

---

[177] Шальнова Ю.П. Монетизация больших данных: технико-экономический анализ драйверов роста и издержек // Экономика. Информатика. 2020. Том 47. № 3. С. 492.

[178] Макаров В.О. Классификация регулятивных песочниц (экспериментальных правовых режимов): Российский и зарубежный опыт//Legal Concept – Правовая парадигма. 2021. Т.20. №3. С. 35–41.

[179] СЗ РФ. 03.08.2020. № 31 (часть I). Ст. 5017.

[180] Economy.gov.ru Министерство экономического развития Российской Федерации. Приоритетные направления / Государственное управление / Нормативное регулирование цифровой среды. Экспериментальные правовые режимы.

Одновременно с этим Федеральным законом от 24 апреля 2020 г. № 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»[181] с 1 июля 2020 года в субъекте Российской Федерации - городе федерального значения Москве проводится эксперимент по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта, а также последующего возможного использования результатов применения искусственного интеллекта. Так, в целях установления экспериментального правового режима, подпунктами 5 и 6 пункта 1 статьи 4 данного Закона предусмотрена возможность передачи собственниками средств и систем фото- и видеонаблюдения изображений, использование которых осуществляется в государственных, общественных или иных публичных интересах, а также изображений гражданина, полученного при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях), за исключением случаев, когда такое изображение является основным объектом использования, а также предоставления доступа к таким средствам и системам фото- и видеонаблюдения органам государственной власти и организациям, осуществляющим публичные функции в соответствии с нормативными правовыми актами Российской Федерации. Что же касается юридических лиц и индивидуальных предпринимателей, то для них предусмотрена возможность обработки персональных данных, полученных в результате обезличивания. 12 октября 2018 года в целях создания условий для развития технологий и продуктов в сфере больших данных в России, а также выработки бизнес-ориентированной стратегии развития рынка больших данных, повышения

[181] СЗ РФ. 27.04.2020. № 17. Ст. 2701.

технической и операционной эффективности взаимодействия участников отрасли,[182] была создана и зарегистрирована саморегулируемая организация Ассоциация Больших Данных (АБД), членами которой являются такие крупные обладатели больших данных, как «Яндекс», VK, «Сбербанк», «Газпромбанк», «Т-Банк», «Россельхозбанк», «МегаФон», «Ростелеком», «Билайн», «МТС», Аналитический центр при Правительстве РФ, «Банк ВТБ», «Авито», Центр стратегических разработок (ЦСР). Деятельность данной организации основана на общих принципах неприкосновенности частной жизни, тайны личной информации, права на анонимность и контроля над использованием персональных данных, а также защиты интересов пользователей, в связи с чем инициировано создание отраслевого акта саморегулирования – Кодекса этики использования данных. Одновременно с этим в АБД создана «песочница» данных для тестирования гипотез и бизнес-моделей. Ассоциация открыта для взаимодействия по следующим форматам: членство, участие и партнерские отношения.

*В соответствии с вышеизложенным представляется целесообразным рассмотреть на уровне законодательного закрепления правовую конструкцию договора о праве субъекта персональных данных разрешать или ограничивать третьему лицу доступ к информации, определяемой по каким-либо признакам.*

***Таким образом, по результатам проведенного исследования можно сделать следующие выводы:***

*- право субъекта персональных данных, предусмотренное в Трудовом Кодексе РФ, требовать исключения персональных данных нуждается в приведении в соответствии с Законом о персональных данных как в части включения его в понятийный аппарат, так и в части определения правовых последствий от совершения данного действия;*

*- необходимо определить на законодательном уровне либо виды персональных данных, либо критерии, отзыв согласия на обработку которых не повлечет за собой для работодателя обязанности прекратить их обработку;*

[182] URL: https://rubda.ru/assocziacziya/ob-assocziaczii/

*- необходимо рассмотреть на уровне законодательного закрепления правовую конструкцию договора о праве субъекта персональных данных разрешать или ограничивать третьему лицу доступ к информации, определяемой по каким-либо признакам, а также определить существенные условия данного договора.*

## § 3. Установление и подтверждение личности в виртуальной среде организаций

Обозначившаяся тенденция технологического развития общества не оставляет сомнения в том, что достоверность установления личности в виртуальном пространстве при вступлении в какие-либо отношения, влекущие правовые последствия, является крайне востребованной. Способы же установления личности, используемые до настоящего времени, не исключают рисков подмены, что может крайне негативно отразиться на экономической и иной безопасности хозяйствующего субъекта, в связи с чем достоверное установление личности и минимизация, а в идеале и полное исключение возможностей ее подмены являются приоритетными при построении отношений в режиме дистанционного доступа.

Сложившаяся практика в области установления личности человека при вступлении в какие-либо правоотношения предлагает, по сути, два способа совершения вышеуказанных действий: по принципу визуального сравнения и автоматическое распознавание[183]. Существует еще и экспертный метод, при котором установление личности происходит на основании заключения специалиста, но это, как правило, событие постфактум, поскольку для инициации правоотношений данный метод не применим. При этом закон не дает четкого определения процедуре установления личности человека. Тем не менее есть все основания согласиться с мнением о том, что это «соотнесение физического лица с юридически значимыми сведениями о личности, идентифицирующими его в общественных отношениях»[184], поскольку оно наилучшим образом отражает суть рассматриваемого явления. Основы законодательства РФ о нотариате, говоря о цели установления личности подразумевают под этим исключение любых сомнений относительно этой самой личности на основании предъявления последним паспорта или иного установленного законодательством документа с

[183] Национальный стандарт РФ. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными ГОСТ Р ИСО/МЭК 19794-1-2008 // СПС «КонсультантПлюс».
[184] Стрельцова Е.Г., Самсонова М.В., Чайкина А.В. Цифровые технологии в гражданском и административном судопроизводстве: практика, аналитика, перспективы. «Инфотропик Медиа», 2022. С. 134.

фотографическими снимками строго установленного образца. В определенных случаях нотариус вправе установить личность гражданина посредством единой биометрической системы (ЕБС), созданной для целей идентификации и (или) аутентификации физических лиц.

*Установление личности посредством предъявления удостоверяющего личность документа*

Основным документом, удостоверяющим личность гражданина, является паспорт, что предусмотрено пунктом 1 Указа Президента РФ от 13.03.1997 № 232 «Об основном документе, удостоверяющем личность гражданина РФ на территории РФ[185]. Перечень сведений, необходимых для установления личности, определен в Положении о паспорте гражданина РФ[186]. Так, в паспорт в обязательном порядке вносятся следующие сведения: фамилия, имя, отчество гражданина, его пол, дата и место рождения. Одновременно с этим в паспорте также в обязательном порядке проставляются отметки о регистрации по месту жительства и снятии с регистрационного учета по месту жительства, об отношении к воинской обязанности в случае достижения гражданином соответствующего возраста. Фотографические снимки должны соответствовать требованиям, установленным Административным регламентом[187] Министерства внутренних дел. Паспорт гражданина РФ является основным, но не единственным документом, удостоверяющим личность. Так, полный перечень таких документов содержится в Классификаторе видов документов, удостоверяющих личность, утвержденном Решением Коллегии Евразийской экономической комиссии от 2 апреля 2019 года № 53[188].

---

[185] СЗ РФ. 1997. № 11. Ст. 1301.

[186] Постановление Правительства РФ от 23.12.2023 г. № 2267 «Об утверждении Положения о паспорте гражданина РФ, образца и описания бланка паспорта гражданина РФ» // СЗ РФ. 2024. № 1 (часть 1). Ст. 163.

[187] Приказ МВД России от 16.11.2020 № 773 «Об утверждении Административного регламента Министерства внутренних дел Российской Федерации по предоставлению государственной услуги по выдаче, замене паспортов гражданина Российской Федерации, удостоверяющих личность гражданина Российской Федерации на территории Российской Федерации» // Текст приказа опубликован на "Официальном интернет-портале правовой информации" (www.pravo.gov.ru) (дата обращения 24.12.2024).

[188] текст решения опубликован на Правовом портале Евразийского экономического союза (https://docs.eaeunion.org) 05.04.2019 (дата обращения 24.12.2024).

При предъявлении вышеуказанных документов удостоверение личности происходит посредством визуального сравнения лица человека с фотографией в документе. На настоящий момент на практике данный метод, к примеру, используется для установления личности при рассмотрении дел в арбитражных судах при проведении судебного заседании в режиме онлайн. Представитель стороны по делу направляет в адрес суда копию своего паспорта в виде PDF-файла, с которым судья сравнивает изображение физического лица на экране монитора. Подобным образом возможно устанавливать личность и в виртуальной среде организаций при различных взаимоотношениях. Это самый простой, но не самый надежный способ.

Одновременно с этим существуют программные продукты и аппаратные средства, например сканер для проверки подлинности вышеуказанных документов[189], который распознает большой спектр признаков фальсификации и предназначен для решения различных бизнес-задач в том числе. Такие сканеры имеют широкое распространение в банковской сфере и во многих государственных структурах, но требует наличия подлинного документа. При этом существуют и сервисные решения[190] проверки паспортов на действительность, что позволяет совершать данные действия удаленно. Так, заинтересованное лицо с помощью API сервиса передает фото или сканы документов, а последний определяет тип документа и распознает все его данные, после чего передает клиенту заполненную структуру всех распознанных данных с выводом о том, является ли представленный документ по своему статусу действующими или нет.

*Установление личности на основании биометрических персональных данных*

На настоящий момент позиционируется, что наиболее совершенной системой идентификации личности, позволяющей практически со стопроцентной гарантией исключить возможность подмены, является биометрия – автоматическое распознавание индивидов, основанное на их биологических и поведенческих

[189] URL: Smart engines // https://smartengines.ru/passport-scanners/.
[190] URL: АДС-СОФТ // https://ads-soft.ru/online-raspoznavanie-dokumentov/#case.

характеристиках[191]. Биометрическое распознавание включает в себя биометрическую верификацию (аутентификацию) – сравнение один к одному с биометрическим шаблоном, когда проверяется тот ли это человек, за кого он себя выдает, и биометрическую идентификацию - сравнение один ко многим, когда в базе данных биометрических характеристик осуществляется поиск с целью найти и возвратить идентификатор, относящийся к одному индивиду.

На настоящий момент, согласно ГОСТу Р 52633.0-2006[192] апробированы или имеют перспективы широкого практического использования следующие биометрические механизмы, основанные на анализе кровеносных сосудов глазного дна; радужной оболочки глаза; двухмерных и трехмерных геометрических особенностей лица в видимом и инфракрасном спектрах света; особенностей геометрии ушных раковин, голоса, папиллярных рисунков пальцев; геометрии ладони, включая рисунки складок кожи ладони и папиллярные рисунки различных фрагментов кожи ладони; рисунка кровеносных сосудов, складок кожи тыльной стороны ладони; рукописного почерка; клавиатурного почерка; геометрических соотношений частей тела; особенностей походки. При этом «список» биометрических данных может постоянно расширяться за счет создания новых, более совершенных алгоритмических инструментов, позволяющих устанавливать личность на основе различных физиологических и биологических особенностей человека, о которых сейчас, например, еще никто и не помышляет.

В Российской Федерации 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. В системе на настоящий момент размещаются только данные изображения человека, полученные с помощью фото-видео

---

[191] Национальный стандарт РФ. Информационные технологии. БИОМЕТРИЯ. Общие положения и примеры применения. ГОСТ Р 54412-2019 (ISO/IEC TR 24741:2018) // СПС «Консультант Плюс».

[192] Национальный стандарт РФ. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. ГОСТ Р 52633.0-2006 // СПС «Консультант Плюс.

устройств, а также голоса[193], что тем не менее не исключает возможности использования в дальнейшем и иных биометрических шаблонов. 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 заседания в режиме видеосвязи, нотариальные услуги.

Возможность же простого 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, на настоящий момент законодательством не предусмотрена, хотя организации и индивидуальные предприниматели наряду с государственными органами, органами местного самоуправления, организациями финансового рынка, нотариусами поименованы в качестве пользователей ЕБС. Закон не запрещает интеграцию коммерческих структур – организаций и индивидуальных предпринимателей с ЕБС, тем более что биометрические персональные данные могут храниться только в ЕБС. Существование коммерческих биометрических систем (КБС) Законом не предусмотрено.

Актуальность использования биометрической системы совершенно очевидна, поскольку биометрия является наиболее эффективной альтернативой иным способам и методам идентификации личности, т.к. речь идет о биологических особенностях человека, присущих только ему. И именно по этой причине рассматриваемому методу идентификации личности предоставлен режим наибольшего благоприятствования и популяризации. Законодательство этой области правового регулирования находится в постоянной динамике, и тем не

---

[193] Постановление Правительства РФ от 30.06.2018 г. № 772 "Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации" (с изменениями и дополнениями) // СЗ РФ. 2018. № 28. Ст. 4234.

менее, в некоторых областях правовых отношений, связанных с данной проблемой, до сих пор имеет место правовой вакуум.

Многие хозяйствующие субъекты, перешедшие на виртуальные (дистанционные) правоотношения, предпочли бы иметь возможность идентифицировать личность с помощью более современных и более достоверных источников, таких как ЕБС. *Возможно, с учетом государственных намерений, связанных с увеличением объема ЕБС, следует упростить и сделать более доступной возможность предоставления организациям и индивидуальным предпринимателям права взаимодействия с данной биометрической системой*, поскольку достоверность в установлении личности в режиме дистанционного сотрудничества во всех случаях является залогом экономической и иной безопасности хозяйствующего субъекта. При этом использование системы предполагает проведение интеграции с ЕБС, посредством установки технологического оборудования, а также программного обеспечения, которые должны соответствовать строго установленным критериям защищенности и информационной безопасности. В некоторых случаях требуется пройти аккредитацию по целому ряду критериев, не самого простого свойства, что довольно серьезно сужает круг лиц, имеющих реальную возможность осуществить подобную интеграцию. Именно по этой причине набирают популярность и пользуются спросом иные технологии, позволяющие устанавливать личности человека иными способами, но уже на свой страх и риск без государственных гарантий.

*Технологические решения подтверждения личности без применения биометрических шаблонов*

Так, разработаны и нашли практическое применение технологии сверки двух лиц без выделения биометрических дескрипторов[194], когда удостоверение личности происходит только по паспорту без обращения к Единой биометрической системе (ЕБС) и без применения биометрических шаблонов. Система сверяет фото в

[194] URL: https://smartengines.ru/face-verification/ (дата обращения 24.12.2024).

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 небиометрической сверкой лиц, что очень верно отражает не только ее существо, но и само направление развития технологий в данной области как некой альтернативы биометрии, применение которой, как указывалось выше, имеет определенные особенности. Интересы бизнеса, отсутствие запретительных или ограничительных мер, востребованность и возможность совершенствования как уже имеющихся технологий подобного рода сверки, так и вновь создаваемых, требует *введения в имеющийся понятийный аппарат соответствующего определения, характеризующего нарождающееся направление в области сверки данных о личности человека в режиме дистанционного доступа без применения биометрических шаблонов, а также законодательной регламентации, легализирующей и вводящей в коммерческий оборот подобного рода технологии, являющиеся по сути альтернативой биометрии, применительно к взаимодействию с Единой биометрической системой (ЕБС).*

Не менее интересной представляется и еще одна отечественная разработка платформы цифрового доверия для подтверждения персональных данных (ПЦД ПД)[195] 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,

[195] URL: https://public.kryptonite.ru/PTsD_PD_presentation.pdf (дата обращения 24.12.2024).

хранящимся у него. Несмотря на то что разработка предназначена для получения сервисов и услуг, технология вполне может быть использована и для подтверждения личности человека посредством индивидуальных идентификаторов в виртуальном пространстве в рамках трудовых и иных взаимодействий.

При этом подобные разработки, потребность в которых является более чем реальной, не могут предоставить каких-либо гарантий безопасности, подкрепленных государственным статусом или осуществлением надзора со стороны властных структур с возможностью применения мер воздействия. Все более стремительная виртуализация общения имеет запрос, а рынок – предложения по установлению связи между данными и субъектом, предоставляя новые методы и возможности идентификации и подтверждения личности. И здесь крайне важна не только законодательная регламентация, но и ее своевременность, поскольку неурегулированность в отношениях порождает неопределенность в правоприменении и, как следствие, трудности в защите нарушенных прав. Выход на рынок разработок подобного рода должен быть обусловлен реальными гарантиями безопасности как аппаратной составляющей, так и программного обеспечения, что определенно нуждается в установлении единых правил и стандартов.

Альтернативой вышеуказанному является Цифровой профиль гражданина (ЦПГ) - совокупность цифровых записей о гражданине, содержащихся в информационных системах государственных органов и организаций, предоставляет 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)[196].

[196] Сценарий использования инфраструктуры Цифрового профиля // URL: https://digital.gov.ru/ru/documents/7554/ (дата обращения 24.12.2024).

Разрешение на получение данных физические лица дают после успешного прохождения авторизации на сайте организации с использованием портала Госуслуг (ЕСИА). Уже существуют и готовые решения для быстрого подключения к цифровому профилю и получению данных о физических лицах для банков, финансовых и страховых компаний, МФО и прочих организаций[197], действующие по следующей схеме[198]. Лицо, имеющее намерение взаимодействовать с какой-либо компанией, заходит на ее сайт или мобильное приложение, где нажимает кнопку «Зайти через Госуслуги». Клиентская система обращается к сервису «Профиль директ» с запросом на проведение идентификации и получения данных. После ввода верного логина и пароля клиенту выводится форма согласия на передачу данных в адрес компании. При запросе указывается цель обработки данных. После ознакомления с перечнем передаваемых данных пользователь предоставляет разрешение. Разрешение содержит также срок, в течение которого оно действует. После согласия сервис «Профиль директ» возвращает клиента на нужную страницу сайта компании (личный кабинет). Одновременно с этим «Профиль директ» передает компании полученные из ЦПГ данные пользователя. Возможно и самостоятельное подключение юридических лиц к ЦПГ, но для этого необходимо согласование доступа к последнему в Министерстве цифрового развития и Центральном Банке РФ.

*Электронный способ идентификации личности*

Несмотря на технологическую активность в данной прикладной области, концепция цифровой идентификации как была, так и остается крайне актуальной. По своей сути 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[199].

---

[197] Для подключения к Цифровому профилю гражданина компания RNDSOFT реализовала готовое решение – сервис «Профиль директ».
[198] URL: https://agredator.ru/dp#func (дата обращения 24.12.2024).
[199] URL: https://ири.рф/news/tsifrovaya-identifikatsiya-polzovateley/ (дата обращения 24.12.2024).

Набор технологий и интеллектуальных устройств для верификации личности по цифровой информации представлен биометрическими персональными данными, цифровыми паспортами или ID, паролями, ПИН-кодами, QR-кодами[200].

На настоящий момент определение индивидуального цифрового идентификатора личности (цифрового аватара) дано в Модельном законе «О цифровых правах»[201], принятом 14 апреля 2023 года, согласно которому это набор символов, изображение или иное условное обозначение, позволяющее идентифицировать в информационной системе субъекта, у которого возникают субъективные гражданские права и обязанности при использовании цифрового аватара в информационной системе. 18 сентября 2023 года издан Указ Президента РФ № 695 «О представлении сведений, содержащихся в документах, удостоверяющих личность гражданина Российской Федерации, с использованием информационных технологий»[202], предоставляющий возможность предъявлять при помощи приложения Единого портала государственных услуг, устанавливаемого на электронные устройства – смартфоны, - удостоверяющие личность данные с портала «Госуслуг» наравне с бумажной версией паспорта.

Данный проект не реализован, но имеет достаточно большой потенциал. Так, в его рамках подразумевается создание единой электронной базы документов, удостоверяющих личность человека, обеспечение безопасности, в том числе и криптозащиту сим-карт при применении программного обеспечения на мобильных устройствах. Одновременно с этим для обеспечения онлайн-доступа к персональной информации, в частности при помощи электронного паспорта, в виде мобильного приложения разрабатывается Государственная система миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность (система «Мир»)[203],

---

[200] Егорова М.А. Проблема цифровой идентификации личности в Российской Федерации и Европейском Союзе // Вестник Университета им.О.Е.Кутафина. 2022. № 1. С. 18–29.

[201] Модельный закон «О цифровых правах» (принят на пятьдесят пятом пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ (постановление от 14 апреля 2023 года № 55–12)) // СПС «КонсультантПлюс».

[202] СЗ РФ. 25.09.2023. № 39. Ст. 7012.

[203] Постановление Правительства РФ от 6 августа 2015 г. № 813 "Об утверждении Положения о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность" // СЗ РФ. 17.08.2015. № 33. Ст. 4843.

одной из основных функций которой является повышение степени защиты документов, удостоверяющих личность, от подделки за счет применения современных методов и средств защиты.

В качестве зарубежных решений в сфере цифровой идентификации в рамках Европейского Союза необходимо рассмотреть так называемый кошелек цифровой идентификации, предназначенный для безопасного хранения гражданами своих персональных данных и для предоставления их в электронной форме в адрес третьих лиц в случае возникновения такой необходимости[204]. Позиционируется, что данный мобильный продукт гарантирует сохранение контроля физических лиц над своими персональными данными, а возможностью доступа к ним третьих лиц будет зависеть от воли самого субъекта. Так, его применение предполагает оптимизацию различных процессов от открытия банковских счетов, поступления в учебные заведения, подачи заявлений о приеме на работу и т.п., до цифровизации государственных услуг. Интеграция в кошелек электронной подписи (eSignature) сделает доступной возможность виртуальной подписи юридически значимых документов. Сам кошелек будет доступен в виде специального приложения, а идентификация лица может проводиться как офлайн, так и полностью виртуально. Одновременно с этим предусматривается обязательная сертификация кошелька.

Что же касается технологий[205], то реализация данного решения может иметь место посредством идентификации через ключи доступа (технология passkeys) или с помощью механизмов блокчейн. И та и другая используют сквозное шифрование. В первом случае усиление системы безопасности достигается за счет встраиваемых в устройство пользователей таким опций, как Touch-ID, Face-ID или приложений-менеджеров паролей, которые привязаны исключительно к пользовательскому устройству. При регистрации пользователя на сайте или в мобильном приложении сторонних сервисов автоматически генерируется уникальный цифровой ключ, который в дальнейшем будет использоваться для входа в учетную запись. Этот идентификатор за счет открытого и закрытого ключей шифрования не доступен

[204] URL: https://cryptoarm.ru/news/eidas-new-horizon-for-the-electronic-identification/ (дата обращения 24.12.2024).
[205] URL: https://ири.рф/news/tsifrovaya-identifikatsiya-polzovateley/ (дата обращения 24.12.2024).

третьим лицам, так как даже при взломе сервера злоумышленник получит доступ лишь к открытому ключу, который не отображает информации об учетной записи или иных данных для входа. Идентификация с помощью блокчейна позволяет хранить информацию о личности в виде идентификаторов-токенов[206] внутри виртуального кошелька. Для такого кошелька не требуется одно- или многофакторная идентификация (логины, пароли и т.д.), так как проверка информации происходит автоматически внутри блокчейна.

Исходя из вышеизложенного невозможно не согласиться с мнением Л.К. Терещенко относительного того, что необходимость расширения возможностей и способов идентификации, особенно дистанционных, не вызывает сомнения. Однако они должны соответствовать характеру и юридической значимости совершаемых действий[207].

*Как можно видеть из вышеизложенного на настоящий момент основным трендом в области установления и подтверждения личности в виртуальном пространстве являются цифровые идентификаторы и их аккумулирование в «руках» субъекта персональных денных, которые по своему усмотрению будут предоставлять доступ к ним третьим лицам. В случае реализации рассматриваемого подхода вопрос идентификации личности в виртуальной среде организаций может быть значительно упрощен.*

***Таким образом, по результатам проведенного исследования можно сделать следующие выводы:***

*- вопрос о возможности предоставления организациям и индивидуальным предпринимателям права взаимодействия с ЕБС требует дополнительной разработки в целях определения порядка его реализации;*

*- необходимо законодательно регламентировать применение технологических решений подтверждения личности в виртуальной среде с учетом обязательного или добровольного прохождения сертификационных процедур, гарантирующих безопасность использования предлагаемой технологии;*

---

[206] Токен – единица учета, запись в блокчейне.

[207] Терещенко Л.К. Научные концепции развития российского законодательства. Коллективная монография. Институт законодательства и сравнительного правоведения при Правительстве РФ. М.: 2024. С.403.

- *организовать обязательную или добровольную сертификацию на базе саморегулирования – самостоятельной и инициативной деятельности, которая осуществляется субъектами предпринимательской или профессиональной деятельности и содержание которой является разработка и установление стандартов и правил указанной деятельности, а также контроль за соблюдением требований указанных стандартов и правил*[208].

[208] Федеральный закон от 01.12.2007 г. № 315-ФЗ «О саморегулируемых организациях» // СЗ РФ. 2007. № 49. Ст. 6076.

# ГЛАВА 3. МЕХАНИЗМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ВИРТУАЛЬНОЙ СРЕДЕ ОРГАНИЗАЦИЙ

## § 1. Правовой режим обработки персональных данных в виртуальной среде организаций

Правовой режим – это совокупность правил, регулирующих ту или иную сферу деятельности[209]. Правила обработки персональных данных устанавливаются как на законодательном, так и на локальном уровне с учетом индивидуальной специфики каждого оператора персональных данных. Сопутствующие деловой активности технологии в сфере осуществления контрольных функций, коммуникаций и иных решений породили запрос на совершенствование правового режима обработки персональных данных в новых условиях, в том числе и в виртуальной среде организаций. Возможности информации к мгновенному распространению, масштабированию и хранению в цифровой среде без использования привычных материальных носителей на фоне все большего вовлечения в рабочий процесс личных компьютерных и иных устройств сотрудников и деловых партнеров с циркуляцией в информационной среде организации как личной, так и корпоративной информации уже можно признать по истине революционными изменениями, системно изменившими корпоративное мировоззрение в части обработки персональных данных. Вне всякого сомнения, 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, поскольку «в 2006 году при разработке Закона о персональных данных данное направление было малоизученным, количество персональных данных,

[209] Пушкин А. Правовой режим иностранных инвестиций в Российской Федерации. М.: Альпина Паблишер, 2012. С.32.

предоставляемых гражданами, незначительным и составляло небольшой поток данных»[210]. В этой связи ключевой задачей является осознание произошедших изменений и разработка с их учетом правового режима обработки персональных данных на основе научного подхода в совокупности с анализом норм действующего законодательства. При этом основополагающая роль в правовом режиме обработки персональных данных в виртуальной среде организаций отводится локальному нормотворчеству, «устанавливающему режим защиты конфиденциальной информации и обращения с ней в каждой отдельной организации»[211], по своей природе более мобильному средству правового реагирования на различные ситуационные изменения.

В настоящее время виртуальная среда организации представлена в различных ипостасях. Это технологии, связанные с созданием в данной среде новой, ранее не известной информации, ее использованием и хранением, технологии телекоммуникационного пространства для взаимодействия пользователей друг с другом как во внутренней информационной среде организации, так и с внешним миром посредством удаленного сетевого доступа, электронной почты, мессенджеров, социальных сетей и т.п., а также совокупность организационно-правовых мер, направленных на регулирование рассматриваемых отношений. При этом в каждой организационной структуре в зависимости от целей создается своя виртуальная среда, которая, как правило, не является стабильной и постоянно пополняется за счет новых технологий. Безусловно, технологическая реальность всегда опережает правовое реагирование, что, однако, не исключает каких-либо послаблений, связанных с исполнением оператором персональных данных обязанностей, возложенных на него законодательством в области персональных данных. В этой связи необходимо рассмотреть вышеуказанные и им подобные технологии на предмет выработки практических рекомендаций по регулированию

---

[210] Поликанина О.А., Поликанин А.Н., Шабурова А.В. Организация защиты персональных данных в государственных и муниципальных системах // Интерэкспо ГЕО-Сибирь 2022. Том 6. С. 198.

[211] Майстренко Г.А., Майстренко А.Г. Источники правового регулирования защиты персональных данных работника в России // Legal Bulletin. 2020. Т.5 (1). С. 25.

обработки информации, получаемой в результате их использования, в рамках виртуальной среды организации.

В соответствии с положениями Закона о персональных данных оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных вышеуказанным Законом и принятыми в соответствии с ним нормативными правовыми актами[212]. Минимально достаточный объем мер[213], определенный Законом о персональных данных и обязательный для применения, включает в себя издание оператором персональных данных:

- документа, определяющего политику оператора в отношении обработки персональных данных;
- локальных актов по вопросам обработки персональных данных, определяющих:

  - цели обработки персональных данных;
  - категории и перечень обрабатываемых персональных данных;
  - категории субъектов, персональные данные которых обрабатываются;
  - способы, сроки их обработки и хранения;
  - порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований;

- локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

Таким образом, в случае использования оператором персональных данных каких-либо технологических решений, способных генерировать создание и хранение персональной информации, последнему надлежит предусмотреть данный факт в локальном акте, с указанием всех технологий, подлежащих применению. Одновременно с этим должны быть определены цели обработки персональных данных, получаемых в результате их использования, а также сами персональные

[212] Пункт 1 статьи18.1 Закона о персональных данных.
[213] Подпункт 2 пункта 1 статьи 18.1 Закона о персональных данных.

данные, которые целесообразно разбить по категориям в зависимости от применяемой технологии, например, персональные данные, создаваемые в процессе производственных видеоконференций, осуществления контроля работодателя за исполнением сотрудником своих обязанностей и другое. Представляется целесообразным указать сведения персонального характера, которые не могут быть уничтожены раньше установленного законодательством времени и в отношении которых не может быть отозвано согласие на их обработку, поскольку это сделает невозможным исполнение оператором персональных данных каких-либо установленных законом обязанностей. Также в целях определения границ прав субъекта персональных данных следует перечислить информацию, априори могущую стать персональной, но создателем и обладателем которой будет организация – оператор персональных данных, к примеру корпоративный номер телефона, аппаратное телефонное устройство.

Что же касается субъектов персональных данных, то помимо сотрудников организации в их число надлежит включить и иных лиц, которыми могут быть деловые партнёры или сотрудники контрагента в рамках взаимоотношений по исполнению договорных обязательств. Относительно способов, сроков обработки и хранения персональных необходимо указать какие конкретно действия могут быть совершены с персональными данными, получаемыми в результате использования технологий, а также сколько времени и где конкретно в виртуальной среде они будут храниться, например на локальном сервере организации или в облаке. Здесь же крайне важно указать на потенциальную возможность хранения персональных данных на личных компьютерных средствах и иных гаджетах сотрудников и третьих лиц, поскольку и многие технологии это предполагают, и процесс деловой активности это исключить не может. При этом складывается интересная ситуация, которая Законом о персональных данных никак не урегулирована и связана с тем, что все права субъекта персональных данных корреспондируют с обязанностями оператора персональных данных, но никак не с другими сотрудниками как самой организации, так и ее контрагентами. Если субъект персональных данных вправе обратиться к оператору с требованием о

предоставлении информации о том, какие персональные данные он обрабатывает, то его обращение к другим сотрудникам организации или третьим лицам, хранящими на своих компьютерных устройства его персональную информацию, обязанностью последних предоставить эту информацию не подкреплено. В этой связи рассматриваемые сведения будут просто считаться информацией о частной жизни гражданина. В аналогичном порядке требования субъекта персональных данных, адресованные вышеуказанных лицам, об уничтожении информации о нем в рамках законодательства о персональных данных разрешено быть не может. Подлежит детальному рассмотрению и порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, с указанием, каким способом и на каких носителях будет произведено данное действие, а также документ административного уровня, подтверждающий совершение данного действия.

Представляет интерес и вопрос о разделении зон ответственности по защите информации между теми, кто предоставляет определенного рода информационные технологии и теми, кто их использует. Рассмотрим данный тезис на примере мессенджера, который представляет собой программу для мгновенного обмена текстовыми сообщениями и мультимедиа между зарегистрированными пользователями через интернет, которыми зачастую пользуются в каждой организации, создавая корпоративные чаты. На настоящий момент мессенджеры предоставляют возможность общения через текстовые сообщения, а также отправлять фото, видео и другие файлы; пользоваться и общаться голосом, не звоня друг другу; осуществлять видеозвонки и видеоконференции[214].

Именно создатели технологий декларируют определенные условия безопасности использования предлагаемого коммуникативного продукта в части защищенности информации, включая и персональные данные, такие как, например, сквозное шифрование, при котором все сообщения, звонки и иные функции общения доступны только для официальных участников данного процесса и никто другой, даже сам мессенджер не сможет их расшифровать. Использование

[214] URL: https://getcompass.ru/blog/posts/chto-takoe-messendzher (дата обращения 24.12.2024).

мессенджера возможно и на смартфоне, и в планшете, и на компьютере, которые в своем большинстве являются собственностью пользователя – работника или партнера работодателя. При этом существуют определенные технологии, позволяющие записывать аудио- и видеозвонки с использованием мессенджера на компьютерное устройство при условии, что мессенджер установлен на компьютер. Одновременно с этим любой пользователь чата в мессенджере может провести архивацию всей информации, содержащейся в переписке, и сохранить ее в своем компьютерном устройстве, а также сделать снимок экрана с чатами или сообщениями и распорядиться ими по своему усмотрению. Что же касается текстовых сообщений, фотографий, файлов, то они хранятся в резервных копиях, если таковая функция настроена пользователем (в облаке на сервере дата центра) и локально на устройстве в зашифрованном виде.

Владельцы мессенджеров в своей политике конфиденциальности[215] позиционируют, что они не хранят сообщения пользователей в ходе предоставления услуг, поскольку последние удаляются с их серверов после доставки. Исключениями являются случаи, когда сообщение не удалось доставить, тогда его хранение осуществляется на их серверах определенное количество дней, после чего удаляется, а также при пересылке медиафайлов, которые также некоторое время хранятся в целях облегчения повторной пересылки. Владелец мессенджера декларирует и несет ответственность за безопасность, защищенность и целостность информации методами и способами, указанными в его политике конфиденциальности, доступной для всех, и находящейся в зависимости от технических возможностей самого владельца коммуникативного сервиса. При этом, принимая предлагаемые условия, пользователь на эффективность таковой защиты повлиять никак не может.

Итогом использования вышеуказанной и иных подобных технологий, позволяющих не только существенно расширить круг лиц, имеющих доступ к информации, зачастую носящей конфиденциальный характер, но и предоставляющих определенный функционал, является практически полная утрата

[215] URL: https://www.whatsapp.com/legal/privacy-policy?lang=ru_RU (дата обращения 24.12.2024).

работодателем – оператором персональных данных или их обладателем - контроля за информацией и, соответственно, ослабления возможностей для ее защиты. Добросовестность пользователей, получивших не только доступ к информации, но и обладающие техническими возможностями для ее копирования, хранения и совершению иных действий на своем личном компьютерном устройстве, уже не поддается контролю со стороны работодателя. Цель повышения конкурентоспособности хозяйствующего субъекта не позволяет отказаться от вышеуказанных и подобных им технологий в пользу соблюдения защиты информации, поскольку создание всех документов в одном экземпляре текста на печатной машинке с их дальнейшим хранением в сейфе, безусловно, в целях защиты информации более предпочтительно, но невозможно и нецелесообразно уже фактически.

В этой связи на первый план в обеспечении безопасности и защите информации выходит ответственное отношение субъектов к правилам поведения в информационной среде, установленным нормативными правовыми и локальными актами, во избежание наступления неблагоприятных последствий, таких как привлечение к дисциплинарной ответственности вплоть до расторжения трудового договора по инициативе работодателя за разглашение персональных данных другого работника[216], возмещение материального и морального вреда, причиненного субъекту разглашением его персональных данных, возмещение материального вреда, причиненного работодателю утечкой информации по вине лица, получившего доступ через личное сетевое устройство к охраняемой информации. При этом вышеуказанная ответственность работника ограничена средним месячным заработком, в отличие от иных лиц, которые возмещают причиненный ущерб в полном размере. *В этой связи имеется настоятельная необходимость введения в круг лиц, обязанных обеспечивать защиту персональных данных, еще одного субъекта со статусом пользователя информацией с выработкой мер и способов обеспечения безопасности информации именно этим*

[216] Подпункт «в» пункта 6 статьи 81 ТК РФ.

*субъектом, а также установления ответственности, что возможно реализовать в локальном акте.*

Прежде всего необходимо установить момент, с наступлением которого субъект будет считаться приобретшим вышеуказанный статус, а также связанные с ним права и обязанности. Представляется, что таким будет являться момент фактического допуска данного лица к информации, включающей и персональные данные. Одновременно с этим в политике безопасности необходимо указать принцип, по которому сотрудникам или третьим лицам может быть предоставлен доступ к подобного рода информации, чтобы изначально исключить возможность несанкционированного получения информации неограниченным кругом лиц. Необходимо предусмотреть возможность создания аккаунтов или совершения иных действий, требуемых для активации виртуального общения, строго определенными лицами с установлением запретительных мер для иных лиц. Возможно предусмотреть создание исключительно секретных чатов, установить запрет на копирование информации на свое личное электронное устройство, определить круг лиц, ответственных за проведение видеоконференций и ее фиксации на строго определенном локальном носителе, предусмотреть условия сетевого допуска в корпоративное информационное пространство, посредством выдачи паролей, установкой на личные компьютерные средства определенных антивирусных программ. Перечень подобных методов и способов обеспечения безопасности информации и ее защиты пользователями информации может быть крайне различным, в зависимости от потребностей самой организации, масштабов ее деятельности, а также информационных ресурсов и применяемых технологий. Исходя из положений части пункта 10 статьи 86 ТК РФ, согласно которым работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников, совместное локальное нормотворчество в рамках хозяйствующего субъекта вполне способно удовлетворить потребности последнего в регулировании защиты персональных данных от вредоносных действий согласно возникающим потребностям.

При этом нормами действующего законодательства круг лиц, на которых возложена обязанность принятия мер по обеспечению безопасности и защите информации, включая и персональные данные, ограничен оператором и обладателем информации, обеспечение которых достигается за счет принятия последними правовых, организационных и технически мер. В случае с персональными данными оператор должен принимать необходимые меры для защита персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных[217]. *Как можно видеть из вышеизложенного данный перечень не является закрытым, что предполагает возможность указания в локальном акте и иных неправомерных операций с персональными данными, например использование в целях, отличных от предусмотренных в организации.*

Что же касается обладателя информацией - персональными данными, то помимо вышеуказанных целей, которые, к слову сказать, полностью совпадают с требованиями к оператору персональных данных, цели, на которые направлена защита информации дополнены соблюдением конфиденциальности информации ограниченного доступа и реализацией права на доступ к информации[218]. Коллаборация понятий конфиденциальности информации, данных в Законе о персональных данных и Законе об информации, информационных технологиях и о защите информации позволяет охарактеризовать данное правовое явление как обязанность обладателя информации, оператора персональных данных и иных лиц, получивших доступ к персональным данным, не передавать такую информацию третьим лицам без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, и обладателя информации (в отношении данного субъекта без каких-либо оговорок). Таким образом, иные лица, получившие доступ к персональным данным, поименованы как субъекты

[217] Статья 19 Закона о персональных данных.
[218] Статья 16 Закона об информации, информационных технологиях и о защите информации.

определенных обязательств только в отношениях, связанных с соблюдением конфиденциальности информации.

В отношении осуществления защиты информации, доступ к которой они получили, и носителя информации, находящегося в его владении, нормы действующего законодательства не предусматривают для них каких-либо обязанностей по соблюдению соответствующих мер, как то предусмотрено для оператора персональных данных и обладателя информации, при том, что сотрудники работодателя и его партнеры фактически используют, хранят и совершают иные действия с информацией, включающей и персональные данные, на своих электронных устройствах, т.е. за периметром корпоративной информационной среды организации. *В свете рассматриваемых обстоятельств следует признать все возрастающую роль локальных актов хозяйствующих субъектов в деле обеспечения безопасности и защиты информации – персональных данных в виртуальной среде организации, которые способны адаптировать различные технологии под необходимые правила поведения,* например обязательное изучение функционала информационного продукта, предполагаемого к внедрению, как силами сотрудников организации, так и третьими лицами, обладающими специальными познаниями в данной области, разработка порядка и установление ответственных за лиц с целью расследования возникающих инцидентов и подозрительных действий, разработка подробного механизма обеспечения информационной безопасности и защиты информации силами сотрудников, получившими доступ к ней доступ, а также третьими лицами – бизнес-партнерами. Нормы действующего законодательства не ограничивают хозяйствующий субъект какими – либо рамками в части установления перечня вышеуказанных документов, но при этом определяют их необходимый минимум, обязательность наличия которого контролируется соответствующими органами.

Реализация правовых мер для обеспечения безопасности и защиты персональных данных в организации осуществляется посредством исполнения оператором обязанности по разработке ранее указанного комплекта документов, а также положения о защите персональных данных, которое должно содержать

сведения о реализуемых требованиях к защите персональных данных и устанавливать процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, а также на устранение последствий таких нарушений. Что же касается обладателя информации, то в отношении него такого четкого перечня обязательных документов не предусмотрено, но в случае, когда речь заходит о персональных данных, являющихся частью информации, обязательность наличия вышеуказанных документов предполагается. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности, представляет собой политику безопасности (информации в организации)[219]. При этом какие-либо требования к обязательным условиям такого документа законодательством не предусмотрены, в связи с чем его содержание, как правило, представляет собой продукт собирательной деятельности выявляемых правовых норм, регламентирующих защиту персональных данных, что тем не менее не исключает возможности внесения в него и иных положений, основанных на специфике деятельности организации.

Высокоуровневая структура подобного рода документа представлена в Национальном стандарте РФ[220], согласно которому высшее руководство организации должно установить политику информационной безопасности, которая:

a) соответствует целям деятельности организации;

b) содержит цели информационной безопасности или обеспечивает основу для их установления;

c) содержит обязательство соответствовать применимым требованиям, относящимся к информационной безопасности;

---

[219] Пункт 2.4.4 Национального стандарта РФ. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» // СПС «КонсультантПлюс».

[220] ГОСТ Р ИСО/МЭК 27001-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» // СПС «КонсультантПлюс».

d) содержит обязательство постоянно улучшать систему менеджмента информационной безопасности.

Политика информационной безопасности должна быть:

e) доступна в виде документированной информации;

f) доведена до сведения работников организации;

g) доступна заинтересованным сторонам.

Перечень средств, которые необходимы для обеспечения безопасности персональных данных и которые должны найти свое отражение в локальном акте, находится в зависимости от того, происходит ли обработка персональных в данных в информационных системах персональных данных или имеет место просто автоматизированная обработка персональных данных с помощью средств вычислительной техники, что не одно и тоже. Понимание сути данных явлений является залогом правильной организации системы безопасности информации в виртуальной среде организации, включая и персональные данные. Так, пункт 2 статьи 19 Закона о персональных данных содержит перечень действий, за счет совершения которых достигается обеспечение безопасности персональных данных. К таковым относятся:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных[221], исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

---

[221] Требования к защите персональных данных представляют собой систему защиты персональных данных, включающую средства защиты информации, актуальные угрозы, а также уровни защищенности персональных данных. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" // СЗ РФ. 2012. № 45. Ст. 6257.

- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- учет машинных носителей персональных данных;

- обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

Данный перечень в полном объеме применим к случаям, когда обработка персональных данных происходит в информационных системах персональных данных. В случае же, когда речь идет просто об автоматизированной обработке персональных данных с помощью средств вычислительной техники, то из вышеуказанных способов обеспечения безопасности персональных данных следует вычленить следующие:

- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- учет машинных носителей персональных данных;

- обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

В связи с тем, что набор мер, необходимых для осуществления защиты и обеспечения безопасности персональных данных не является одинаковым для всех, следует выявить соответствующие различия при обработке просто персональных данных и персональных данных в информационных системах. Так, информационная система персональных данных – это совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств[222]. Основой данной правовой конструкции является такое понятие как база данных, определение которой дано в Гражданском Кодексе РФ. Базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины[223]. База данных признается составным произведением, у которого в обязательном порядке должен быть изготовитель – лицо, организовавшее создание базы данных и работу по сбору, обработке и расположению составляющих ее материалов[224]. Одновременно с этим возможна и государственная регистрация баз данных, подтверждающая авторские права.

Исходя из вышеизложенного, база данных — это не просто набор информации, пусть расположенный и даже систематизированный в некотором порядке, это некое произведение, которое именно так и задумывается, со своей определенной тематикой, предназначением, сбором и хранением строго определенной информации, например база данных стандартных образцов России, правовые базы данных, база данных дактилоскопических карт и многие другие. Ю.С. Телина, к примеру, считает необходимым ведение реестра баз персональных данных[225]. Таким образом, совокупность персональных данных, подвергающихся автоматизированной обработке в виртуальной среде организации в рамках осуществления хозяйствующим субъектом своей уставной деятельности, но без

---

[222] Пункт 10 статьи 3 Закона о персональных данных.
[223] Пункт 2 статьи 1260 Гражданского Кодекса РФ.
[224] Пункт 1 статьи 1333 Гражданского Кодекса РФ.
[225] Телина Ю.С. автореф. дис. … канд.юрид.наук. М, 2016. С.16

какой-либо строго определённой тематической цели, не может быть причислена к базе данных. В случае обработки просто персональных данных технические меры защиты будут иными, чем те, которые применяются при обработке персональных данных в информационных системах, к которым предъявляются повышенные меры безопасности.

*Из всего вышесказанного следует, что правовые акты хозяйствующего субъекта способны играть значительную регулятивную роль в деле обеспечения безопасности и защиты персональных данных в виртуальной среде организации и должны активно использоваться с целью закрепления обязательных для исполнения локальных механизмов, методов и способов достижения вышеуказанной цели. Одновременно с этим использование современных технологий влечет за собой перманентное увеличение числа лиц, получающих доступ к персональным данным, что требует усиления превентивных мер, направленных на снижение риска нарушения безопасности персональных данных за счет усиления мер самоконтроля и ответственного отношения каждого пользователя персональными данным под страхом наступления ответственности.*

***Таким образом, по результатам проведенного исследования можно сделать следующие выводы:***

*- необходимо ввести в круг лиц, обязанных осуществлять защиту персональных данных, еще одного субъекта со статусом пользователя информацией.*

## § 2. Разрешительная система доступа к персональным данным в виртуальной среде организации

Общим принципам построения разрешительной системы доступа к какой-либо конфиденциальной информации посвящено достаточно много исследований, и процесс ее практической реализации особенных трудностей не вызывает. Так, последняя является составной частью системы правовых, организационных и технических мер в части обеспечения безопасности и осуществления защиты информации конфиденциального характера. По общему правилу организации, имеющей в своем активе информацию подобного рода, надлежит разработать и принять локальные нормативные положения, направленные на обеспечение обоснованного и правомерного доступа пользователей к вышеуказанной информации. При этом под обоснованностью следует понимать исключительно необходимость, связанную с выполнением служебных обязанностей. Правомерность доступа достигается за счет реализации следующей последовательности действий. Прежде всего на уровне руководящего состава организации определяется лицо или лица, имеющие право давать разрешение на доступ к информации конфиденциального характера. Далее выявляется круг пользователей, потенциальная возможность обращения которого к данной информации предполагается, а также разрабатывается порядок оформления разрешений на доступ к данной информации. Право работать с информацией конфиденциального характера предоставляется только тем лицам, которые либо в соответствии с приказом руководителя, либо на основании трудового договора получили такой доступ. Предлагаемое в этой части исследование ориентировано на выявление особенностей в регулировании порядка доступа к информации конфиденциального характера именно в виртуальной среде организаций.

Статьей 7 Закона о персональных данных предусматривается конфиденциальность персональных данных, т.е. операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта

персональных данных, если иной не предусмотрено федеральным законом. Таким образом, доступ к персональным данным является ограниченным, что предполагает установление разрешительной системы в этой части. Прежде всего необходимо определить цели создания такой системы, которые условно можно разделить на три направления. Первое – это *соблюдение оператором и иными лицами, получившими доступ к персональным данным, требований конфиденциальности*, что по своей природе представляет собой совершение вышеуказанными лицами обязательных к исполнению действий в пользу защиты интересов других лиц - субъектов персональных данных. Иными словами, состояние конфиденциальности данной информации сохраняется до тех пор, пока субъект персональных данных своим волевым решением не прекратит ее существование, дав согласие на ее раскрытие и распространение, т.е. конфиденциальность персональных данных полностью зависит от желаний и предпочтений субъекта персональных данных. В этой связи имеется потенциальная возможность получения от субъекта персональных данных 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. Наличие подобного согласия на предоставление и раскрытие данной информации в целом существенно облегчит правовую регламентацию возможности ее использования всеми сотрудниками, а не только теми, кто имеет специально установленный доступ, что в условиях настоящей действительности способно существенно ускорить процесс реализации поставленной задачи от ее возникновения до ее воплощения. *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 разрешительной системы доступа к персональным данным организации с определением формы согласия, срока его предоставления, порядка отзыва и т.п. критериев.*

Статьей 7 Закона о персональных данных предусмотрено, что операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать

третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. При этом как было рассмотрено выше и применительно к теме исследования, обладателем персональных данных не всегда будет являться только субъект персональных данных, поскольку при определенных условиях им может стать и оператор персональных данных – юридическое лицо, в то время как субъектом персональных данных может быть только лицо физическое. *Сужение круга лиц, за которыми закреплено право предоставления вышеуказанного согласия исключительно до субъекта персональных данных, не соответствует иным правам, предоставленным субъектам данных правоотношений, в связи с чем имеется настоятельная необходимость в корректировке законодательства о персональных данных в части расширения круга лиц, у которых полежит истребованию согласие на раскрытие персональных данных за счет включения в него обладателя информации.*

Вторым направлением, в отношении которого необходима целевая разработка разрешительной системы доступа к персональным данным, является причисление персональных данных к *активам организации, имеющим ценность в интересах достижения целей деятельности и находящимся в ее распоряжении*[226]. Как верно отмечено В.А. Севериным «основой развития современных предприятий является новая техническая, технологическая и деловая информация, введенная в оборот как коммерчески значимая информация, которая признается ценным ресурсом, овеществляется во всех факторах производства и составляет необходимый элемент деятельности по производству и реализации инновационных товаров (работ и услуг). В условиях конкуренции защита такой информации от неправомерного использования требует разработки и соблюдения установленных мер информационной безопасности»[227]. Так, в качестве примера можно привести

[226] Информационные активы, в том числе различные виды информации, циркулирующие в информационной системе (служебная, управляющая, аналитическая, деловая и т.д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение) (п.3.1.4 и 3.1.6) Национального стандарта РФ. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения // СПС «КонсультантПлюс».

[227] Северин В.А. Правовые аспекты обеспечения информационной безопасности цифровой экономики // Пробелы в российском законодательстве. 2023. Том 16. № 8. С. 49.

конфиденциальное корпоративное видео по обсуждению условий предполагаемой сделки. Биометрические персональные данные, на основании которых можно установить личности переговорщиков и, соответственно, представляемые ими структуры, не должны подлежать распространению, в частности и в целях сохранения тайны проведении самих переговоров. Видеоматериалы, содержащие помимо биометрических персональных данных еще и иную значимую информацию, могут быть причислены к коммерческой тайне в соответствии с Законом «О коммерческой тайне»[228]. При этом персональные данные в силу своей универсальности способны вступать в коллаборацию и с иными тайнами, например государственной, защитой свидетелей, когда и личность человека, и его внешние данные, являющиеся биометрическими персональными данными, и иные сведения должны быть недоступны для третьих лиц. Как очень точно отметил А.В. Минбалеев «персональные данные могут охраняться как самостоятельным режимом защиты, так и в режиме государственной тайны или определенного вида информации ограниченного доступа, например, коммерческой тайны или профессиональной тайны. В этом случае персональные данные подобны хамелеону и в зависимости от ситуации «меняют окраску» и охраняются в режиме определенного вида информации ограниченного доступа или при помощи собственных мер, или в режиме совместной охраны. Подобная практика позволяет режиму персональных данных быть очень «гибким» и подстраиваться под те или иные отношения. Обусловливается это тем, что персональными данными могут стать любые сведения, если по ним даже есть косвенная возможность определить физическое лицо»[229]. Разрешительная система доступа в каждом конкретном случае должна учитывать требования законодательных норм, регулирующих конкретные отношения. Так, статья 10 Закона о коммерческой тайне предусматривает меры охраны конфиденциальности информации, принимаемые ее обладателем:

- определение перечня информации, составляющей коммерческую тайну;

---

[228] СЗ РФ. 09.08.2004. № 32. Ст.3283

[229] Минбалеев А.В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2012. № 2 (4). С. 8.

- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

- нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

В виртуальной среде организаций информация о принадлежности какой-либо информации к коммерческой тайне также должна иметь место, хотя совершенно очевидно, что вышеуказанные способы в данном случае неисполнимы. В качестве предложений по техническому решению данной ситуации возможно использовать группировку информации по папкам с указанием на ее принадлежность к коммерческой тайне, применение технологии сокрытия папок или файлов, шифрование видео с помощью специальных протоколов, когда доступ к нему предоставляется по усмотрению его обладателя с гарантией от скачивания и распространения, шифрование электронной почты, доступ к содержанию которой могут получить только предполагаемые лица.

Закон о персональных данных никаких конкретных требований, связанных с соблюдением режима конфиденциальности последних, не содержит. При этом в императивном порядке предусматривает обязанность для оператора, являющегося юридическим лицом[230], назначить сотрудника, ответственного за организацию

[230] Статья 22.1 Закона о персональных данных.

обработки персональных данных, который получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему. В обязанности данного лица, в частности, входит осуществление внутреннего контроля за соблюдением оператором и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных, а также доведение до сведения работников оператора положения законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных. Соблюдение конфиденциальности персональных данных является требованием Закона о персональных данных и направлено на недопущение несанкционированного или случайного доступа и, соответственно, на защиту персональных данных, в связи с чем это может быть одно и тоже лицо, одновременно ответственное как за обработку персональных данных, так и за соблюдение режима их конфиденциальности. Но при этом совершенно не исключено возложение этих обязанностей и на отдельного сотрудника. *Все остальные вопросы, не входящие в совокупность законно установленных требований к обеспечению режима конфиденциальности персональных данных, а также требований к охране какой-либо тайны или тому подобной сущности, включающей персональные данные, подлежат регулированию посредством локальных актов.*

Третьим целевым направлением создания разрешительной системы допуска является *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[231]. Обеспечение безопасности персональных данных достигается, в частности, за счет обнаружения фактов несанкционированного доступа к персональным данным и принятием соответствующих мер[232], а также установления правил доступа к персональным

[231] Пункт 1 статьи 19 Закона о персональных данных.
[232] Подпункт 6 пункта 2 статьи 19 Закона о персональных данных.

данным, обрабатываемым в информационной системе персональных данных, обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных[233]. При этом следует иметь в виду, что обработка персональных данных может быть обычной, т.е. применяемой в каждой хозяйствующей структуре, а может быть специализированной, когда персональные данные размещаются и хранятся именно в информационной системе персональных данных, что ни одно и тоже. *В этой связи обязательное установление правил доступа к персональным данным и обеспечение регистрации всех действий с ними применимо только в случае специализированной обработки персональных данных в различных информационных системах*, что тем не менее не отрицает создание подобного документа и при обычной обработке персональных данных. Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного[234], в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных[235]. А.А.Тедеев обращает внимание на то, что «неправомерным (несанкционированным) считается доступ к информации, нарушающий установленные правила разграничения доступа[236].

*Таким образом, вышеозначенные нормы права, направленные на обеспечение безопасности персональных данных, должны в обязательном порядке учитываться при создании разрешительной системы доступа к ним в виртуальной среде организаций.*

---

[233] Подпункт 8 пункта 2 статьи 19 Закона о персональных данных.

[234] Несанкционированный доступ: Доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа. П.3.3.6 Национального стандарта РФ. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения // СПС «КонсультантПлюс».

[235] Пункт 11 статьи 19 Закона о персональных данных.

[236] Тедеев А.А. Инфомационное право: Учебник. М., 2005. С. 172.

В части законодательного установления порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных[237]. При этом последний не содержит определения «доступ», но в рамках основных понятий, использующихся в данном Законе, оно непосредственно связано с термином «передача», согласно которому это распространение, предоставление, доступ[238]. Под распространением персональных данных понимаются действия, направленные на раскрытие персональных данных неопределенному кругу лиц, а предоставление – это раскрытие персональных данных определенному лицу или определенному кругу лиц[239]. Одновременно с этим раскрытие персональных данных (распространение и предоставление) может иметь место двумя способами: из внутренней среды во внешнюю, когда персональные данные, хранящиеся у оператора, масштабируются и копии «покидают» место хранения, например, фотоизображение выкладывается в интернет, и диаметрально противоположным способом, когда при определенных условиях третьи лица могут войти в информационное пространство и ознакомиться с персональными данными, хранящимися там, т.е. раскрытие происходит во внутренней информационной среде. В качестве определенных условий можно привести в пример получение кодов и паролей доступа к месту хранения персональных данных и т.п. технологических решений. Таким образом, в рамках основного понятия «доступ» — это передача персональных данных. Тем не менее не совсем понятно как этот термин должен пониматься в рамках пункта 9 статьи 10.1 Закона о персональных данных, согласно которому «в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц». Как видно из вышеизложенного действия, связанные с предоставлением

[237] Пункт 9 статьи 9 Закона об информации, информационных технологиях и о защите информации.
[238] Пункт 3 статьи 3 Закона о персональных данных.
[239] Пункты 5 и 6 статьи 3 Закона о персональных данных.

«доступа», а также получением «доступа» к персональным данным, являются исключением из правил, установленных данной нормой права. При этом *отсутствие определения рассматриваемого понятия крайне затрудняет применение означенной нормы права по ее назначению, в том числе и в целях создания разрешительной системы доступа к персональным данным в виртуальной среде организаций, что требует уточнения или иной корректировки в рамках Закона о персональных данных.*

Одновременно с этим термин «доступ» к информации закреплен в Законе об информации, информационных технологиях и защите информации, что при определенных условиях дает возможность применения аналогии закона. Так, доступ к информации – это возможность ее получения и использования[240]. Данное определение полностью соответствует положениям статьи 14 «Право субъекта персональных данных на доступ к его персональных данным», согласно которой субъект персональных данных имеет право на получение сведений, указанных в части 7 данной нормы права. Это право является безусловным за некоторыми исключениями, предусмотренными законом, например когда доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц. Особенностью здесь является факт предоставления права доступа субъекта персональных данных к своим персональным данным на уровне законодательного установления, что отрицает существование каких-либо разрешительных процедур в этой части на локальном уровне. Единственное, что может и должно быть зарегламентировано, – это последовательность фактических действий, в результате которой субъект персональных данных получает искомую информацию. *Таким образом, в рамках Закона о персональных данных доступ к персональным данным - это как их передача, так и получение, что надлежит учитывать при создании разрешительной системы допуска к персональным данным в виртуальной среде организации.*

По мнению В.А. Северина при обработке персональных данных оператором решаются две основные задачи, связанные с обеспечением «допуска» и «доступа»

[240] Пункт 6 статьи 2 Закона об информации, информационных технологиях и о защите информации.

к персональным данным субъектов работников оператора и других субъектов в соответствии с целями обработки персональных данных. Поскольку в законодательстве эти процедуры не прописаны, в каждой организации принимаются свои корпоративные акты о порядке обработки и обеспечения режима защиты персональных данных работников. Под «допуском к обработке персональных данных» понимается «процедура оформления права на доступ к персональным данным». Под «доступом» - наличие условий правовых, технических и иных для обработки персональных данных в организации. Представители сторонних организаций могут быть допущены к процессу обработки персональных данных на основании договора и совместных документов, где прописаны меры обеспечения безопасности персональных данных при их обработке[241]. Исходя из вышеизложенного, условно доступ к персональным данным можно разделить на юридический и фактический, но при этом только их совокупность гарантирует получение и использование персональных данных. В первом случае посредством разрешительной системы доступа к персональным данным в виртуальной среде организации устанавливается весь спектр правил, регулирующий данный порядок. Что же касается фактического доступа к персональным данным, то это непосредственная реализация вышеозначенного права на их получение и использование, и если по какой-то причине, например технической неисправности получение персональных данных становится невозможным, доступ к последним следует считать отсутствующим. Фактический доступ осуществляется как посредством вхождения в виртуальное пространство организации, так и посредством подключения к нему через мессенджеры, ссылки на приглашение в видеоконференцию и иных подобных действий.

Орган юридического лица, имеющий компетенцию на утверждение локальных нормативных актов, входящих в разрешительную систему доступа к персональным данным, определяется в соответствии с его учредительными документами. Это может быть и исполнительный орган хозяйствующей структуры,

[241] Северин В.А. Правовой институт персональных данных в системе российского права // Коммерческое право. 2020. № 4 (Том 39). С. 48–49.

и общее собрание участников, и иное лицо. В случае нарушения порядка принятия и компетенции вышеозначенные акты не приобретают обязательную для исполнения силу.

В данном аспекте не менее важен и факт надлежащего ознакомления лиц, получающих доступ к персональным данным в виртуальной среде организаций, с вышеозначенными правилами, поскольку последние применительно с ним получат обязательную для исполнения силу только после такого ознакомления и принятия этими лицами всех предусмотренных в них условий. Специфическая особенность среды хранения персональных данных предполагает и необходимость размещения вышеозначенных документов именно в виртуальной среде либо на сайте организации для неограниченного доступа, либо посредством предоставления возможности для ознакомления и принятия условий отдельным лицам по усмотрению организации. И в том и в другом случае необходимо предусмотреть техническую возможность подтверждения лицами, получающими доступ к персональным данным в виртуальной среде организаций, факта ознакомления и принятия условий доступа, что может быть реализовано с помощью электронной подписи, нажатия кнопки «принять» или «отклонить» на сайте организации.

При этом в рамках конфиденциальности информации обязанность лиц, получивших доступ к персональным данным, не разглашать их без согласия субъекта персональных данных, а равно их обладателя, уже предусмотрена нормами действующего законодательства. В этой связи факт ознакомления с правилами получения доступа к персональным данным и принятия всех условий такого доступа будет являться достаточным подтверждением добровольного возложения на себя лицами, получающими доступ к персональным данным, обязанности не раскрывать третьим лицам и не распространять эти данные без согласия субъекта персональных данных и их обладателя. При получении доступа к персональным данным, являющихся активом общества и имеющих экономическую, государственную и т.п. ценность за счет их неизвестности третьим лицам, обязанность по охране их конфиденциальности наравне в соблюдением прав субъектов персональных данных обусловлена еще и иными целями, например

получением коммерческой выгоды в зависимости от того, какую иную тайну представляют собой персональные данные. Таким образом, на лицо, получающее доступ к такого рода персональным данным, возлагается обязанность по охране ее конфиденциальности в соответствии с законом, регулирующим режим конкретной тайны, в связи с чем требуется получение подтверждения об ознакомлении лица с перечнем информации, составляющей какую-либо тайну, например, коммерческую, а также с перечнем действий, которые лицо вправе совершать с данной информацией: чтение, хранение, изменение, копирование, уничтожение и принятия им обязанности не разглашать данные сведения. Одновременно с этим в зависимости от вида охраняемой тайны будет разниться и ответственность за ее нарушение, при том что не исключается одновременное привлечение к ответственности как за разглашение персональных данных, так и иной тайны, содержанием которой или составляющей являются персональные данные. *Таким образом, разрешительная система доступа к персональным данным должна содержать четкие критерии персональных данных, конфиденциальность которых подлежит охране, – относящиеся к прямо определенному или косвенно определяемому лицу, или к активу организации в силу ценности информации, выраженной в виде или с посредством персональных данных.*

За основу определения круга лиц, имеющих доступ к персональным данным, возможно брать как их четкий перечень, так и некие категории, принадлежность к которым по оговоренным признакам также предоставляет вышеуказанное право, например лица, состоящие в корпоративном чате или принимающие участие в видеоконференциях. Характерной особенностью, которой подвержен рассматриваемый круг лиц при доступе к персональным данным в виртуальной среде организаций по сравнению с более стабильными средами, является его постоянная динамика, связанная как с использованием технологий, так и с простотой самого физического доступа, когда, к примеру, буквально за одну секунду в чат или видеоконференцию может быть добавлен новый участник без предварительного прохождения длительных бюрократических процедур.

*В этой связи представляется, что при формировании разрешительной системы доступа к персональным данным именно в виртуальной среде организаций необходима вся полнота охвата как использующихся в организации технологий, так и всех категорий лиц, получающих одновременно с доступом к технологиям и доступ к персональным данным, будь то сотрудники организации или третьи лица. При определении категорий вышеуказанных лиц целесообразно основываться на целях доступа, поскольку они абсолютно стабильны.*

***Таким образом, по результатам проведенного исследования можно сделать следующие выводы:***

*- разрешительной системы доступа к персональным данным в виртуальной среде организаций должна учитывать следующие цели:*

*1. соблюдение оператором и иными лицами, получившими доступ к персональным данным, требований конфиденциальности в соответствии с Законом о персональных данных, т.е. в пользу защиты прав субъекта персональных данных;*

*2. соблюдение лицами, получившими доступ к персональным данным, требований конфиденциальности в соответствии с иными законами, регулирующими охрану какой-либо тайны, которой непосредственно являются сами персональные данные или в состав которой они входят, т.е. в пользу защиты прав оператора персональных данных и иных обладателей информации;*

*3. соблюдение оператором персональных данных требований Закона о персональных данных, связанных с защитой персональных данных от неправомерного или случайного доступа к ним.*

*- представляется целесообразным предусмотреть возможность субъекта персональных данных отказаться от конфиденциального статуса своих персональных данных с установлением формы такого согласия, срока его действия, порядка отзыва и иных подобных критериев;*

*- расширить круг лиц, получение согласия которых для раскрытия третьим лицам и распространения персональных данных является обязательным за счет включения в него обладателя данной информацией;*

*- предусмотреть в Законе о персональных данных определение «доступа» к персональным данным;*

*- разрешительная система доступа к персональным данным в виртуальной среде организации, наряду с общепринятыми правилами, должна содержать следующие обязательные условия:*

*1. указание на цели создания разрешительной системы доступа к персональным данным в зависимости от того, в чьих интересах подлежит соблюдению режим конфиденциальности персональных данных;*

*2. классификацию персональных данных в зависимости от целей обеспечения конфиденциальности;*

*3. порядок определения лиц, получающих доступ к персональным данным, посредством четкого перечня и/или какой-либо иной общности - категории;*

*4. порядок размещения в виртуальной среде организации документов разрешительной системы допуска к персональным данным;*

*5. порядок ознакомления лиц, получающих доступ к персональным данным, с документами разрешительной системы, размещенными в виртуальной среде организации, с описанием технических возможностей подтверждения факта ознакомления;*

*6. перечень технологических решений, применяемых в организации для обеспечения уставной деятельности (мессенджеры для мгновенного обмена сообщениями, облачные платформы для проведения онлайн-видеоконференций, программные продукты для сбора персональной аналитики качества и количества выполняемой работы, записи видеонаблюдения и др.);*

*7. порядок осуществления доступа в виртуальное пространство организации как посредством паролей, ключей и атрибутов доступа, идентификации, аутентификации, так и через мессенджеры, ссылки-приглашения и др.;*

*8. порядок определения лиц, в обязанности которых входит создание вышеуказанных технологических средств доступа, а также осуществление контроля за их использованием;*

*9. порядок фиксации грифа конфиденциальности персональных данных в зависимости от целей ее соблюдения;*

*10. порядок использования в работе личных компьютерных средств и их учета;*

*11. порядок хранения в тайне паролей и иных подобных технологических средств доступа в виртуальную среду организации и к персональным данным;*

*12. виды ответственности за нарушение режима конфиденциальности персональных данных.*

## § 3. Меры организационно – правового и технического характера по обеспечению безопасности персональных данных в виртуальной среде организаций

Если еще относительно недавно основа информационной безопасности строилась на том, чтобы не допустить несанкционированный физический доступ к материальным носителям информации, то в современных реалиях, когда основной массив информации хранится в виртуальной среде без использования материальных носителей[242], на первый план обеспечения информационной безопасности выходят меры технического характера, призванные не допустить утечки защищаемой информации по техническим каналам[243], ее перехвата[244], а также предотвратить несанкционированный доступ[245] во избежание ее уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также совершения иных неправомерных действий в отношении персональных данных[246].

Обязанность оператора при обработке персональных данных принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования,

---

[242] В качестве материального носителя следует рассматривать компьютерное средство, съемный накопитель, планшет, смартфон и т.п. и только в том случае, если информация хранится именно в этом компьютерном средстве или гаджете. Если информация хранится в облаке, то вышеуказанные материальные активы уже нельзя признать носителями информации. В этом случае они представляют собой средство доступа к информации, посредством паролей и иных технических возможностей.

[243] Утечка (информации) по техническому каналу представляет собой неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации (п.3.2.4 Рекомендации по стандартизации. Р 50.1.056-2005. «Техническая защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 29.12.2005 г. № 479-ст)) (далее по тексту – Рекомендации) // СПС «КонсультантПлюс».

[244] Перехват (информации) – это неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов, которое может иметь место посредством подключения устройства перехвата к незащищенному каналу передачи данных или в его разрыв (п.3.2.5 Рекомендаций).

[245] Несанкционированный доступ к информации - доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа с применением штатных средств информационной системы или средств аналогичных им по своему функциональному предназначению и техническим характеристикам и может иметь место посредством (п.3.2.6 Рекомендаций).

[246] Пункт 1 статьи 19 Закона о персональных данных.

предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных предусмотрена положениями Закона о персональных данных[247]. Одновременно с этим данной нормой права предусмотрен перечень мероприятий, направленных на обеспечение безопасности персональных данных. При этом данный перечень не является единым для всех, в связи с разнообразием деловой активности.

Так, если персональные данные обрабатываются в информационных системах персональных данных, то оператору надлежит совершить следующие действия:

- определить угрозы безопасности персональных данных[248];

- применить организационные и технические меры по обеспечению безопасности персональных данных при их обработке, необходимые для выполнения требований к защите персональных данных, которые в итоге должны обеспечить установленные Правительством Российской Федерации уровни защищенности персональных данных[249];

- провести оценку эффективности принимаемых мер по:

А) обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных[250];

Б) обнаружению фактов несанкционированного доступа к персональным данным;

В) обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них[251];

Г) установлению правил доступа к персональным данным;

Д) обеспечению регистрации и учета всех действий, совершаемых с персональными данными[252].

---

[247] Статья 19 Закона о персональных данных.
[248] Подпункт 1 пункта 2 статьи 19 Закона о персональных данных.
[249] Подпункт 2 пункта 2 статьи 19 Закона о персональных данных.
[250] Подпункт 4 пункта 2 статьи 19 Закона о персональных данных.
[251] Подпункт 6 пункта 2 статьи 19 Закона о персональных данных.
[252] Подпункт 8 пункта 2 статьи 19 Закона о персональных данных.

А также установить контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности[253]. Во всех остальных случаях операторам надлежит применять прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации[254], применять для уничтожения персональных данных прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации, в составе которых реализована функция уничтожения информации[255]; вести учет машинных носителей персональных данных[256], восстанавливать персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним[257]. Данные требования, наравне с вышеуказанными относятся также и к операторам, осуществляющим обработку персональных данных в информационных системах персональных данных.

Одновременно с этим для информационных систем персональных данных помимо требований к защите персональных данных, включающих средства защиты информации, актуальные угрозы, а также уровни защищенности персональных данных, отдельно утверждены состав и содержание организационных и технических мер по обеспечению безопасности персональных данных в рассматриваемых системах[258]. Что же касается автоматизированной обработки персональных данных вне информационных систем, то с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных Правительством РФ[259] установлены только требования к

---

[253] Подпункт 9 пункта 2 статьи 19 Закона о персональных данных.
[254] Подпункт 3 пункта 2 статьи 19 Закона о персональных данных.
[255] Подпункт 3.1 пункта 2 статьи 19 Закона о персональных данных.
[256] Подпункт 5 пункта 2 статьи 19 Закона о персональных данных.
[257] Подпункт 7 пункта 2 статьи 19 Закона о персональных данных.
[258] Приказ ФСТЭК России от 18.02.2013 № 21 (ред. 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 № 28375) // СПС «КонсультантПлюс».
[259] Постановление Правительства РФ от 06.07.2008 г. № 512 «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» // СЗ РФ. 2008. № 28. Ст. 3384.

материальным носителям биометрических персональных данных и технологиям хранения таких данных вне вышеуказанных информационных систем. В части обработки иных видов персональных данных вне информационных систем персональных данных и при условии, что конкретные требования законодательством не предусмотрены, операторам предоставлены права самостоятельного принятия решений о превентивных мерах для обеспечения безопасности информации, а также о том, каким образом будут пресекаться незаконные действия с персональными данными.

Под безопасностью информации (данных) понимается состояние защищенности информации (данных), при котором обеспечиваются ее (их) конфиденциальность, доступность и целостность[260]. Иными словами, информация должна находиться в таком состоянии, когда отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право, а субъекты, имеющие права доступа[261], могут реализовывать их беспрепятственно. Таким образом, нарушение хотя бы одного свойства из вышеуказанной триады, приводит к нарушению безопасности, выстраиваемой в отношении информации – персональных данных.

Под организационно-техническими мероприятиями по обеспечению защиты информации надлежит понимать совокупность действий, направленных на применение организационных мер и программно-технических способов защиты информации на объекте информатизации, которые должны осуществляться на всех этапах жизненного цикла объекта информатизации[262]. Исходя из содержания данного понятия, а также природы персональных данных, следует признать, что жизненный цикл последних начинается с момента сбора персональных данных и заканчивается моментом их уничтожения, включая и иные действия, такие как хранение, и использование, уточнение персональных данных. При этом оператор

---

[260] Рекомендации по стандартизации Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения» (п.3.1.3) // СПС «КонсультантПлюс».

[261] К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также право на изменение, использование, уничтожение ресурсов. Там же. Пункт 3.1.8.

[262] Рекомендации по стандартизации Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения» (п.3.5.1) // СПС «КонсультантПлюс».

персональных данных и обладатель данной информации должны обеспечивать безопасность каждой операции, которая совершается в вышеуказанных период, для чего целесообразно определить, какие конкретно требования должны предъявляться к каждому действию, поскольку технические методы защиты могут разниться.

С учетом вышеизложенного 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 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 иные меры);

- 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.

Безусловно, данный перечень является исключительно приблизительным, но тем не менее в нем учтены основные направления, присущие обработке персональных данных в виртуальной среде организаций.

Сложно не согласиться с мнением В.А. Северина о том, что «с развитием новейших технологий изменился сам подход к вопросам обеспечения информационной безопасности организаций в силу использования информационных и цифровых технологий»[263]. В рамках данных изменений основным и главным последствием является снижение степени защиты персональных данных в виртуальной среде организаций за счет увеличения, порой неконтролируемого со стороны организации, числа лиц, получающих доступ к использованию и хранению персональных данных; количества личных компьютерных средств и иных гаджетов сотрудников и третьих лиц, принимающих участие в деловой активности; сервисных решений и иных инструментов, сопутствующих организации деятельности хозяйствующей структуры по разным направлениям, и т.п.

Одновременно с этим *целесообразно провести условное разграничение 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.* Основу данного разграничения составляют принадлежность технологических средств, информационные технологии, сервисы и т.п., используемые в процессе деятельности, а также волеизъявление участников вышеозначенного процесса. При этом чем выше степень концентрации надзорной функции, тем выше и контроль со стороны организации. Примером могут служить любые персональные данные в

[263] Северин В.А. Правовые аспекты обеспечения информационной безопасности цифровой экономики // Пробелы в российском законодательстве. Том 16. № 8. С. 46–51.

виртуальной среде организации, которые традиционно используются строго определенными лицами или службами – бухгалтерией, отделом кадров и т.п. Ответственность за соблюдением конфиденциального характера персональных данных, аккумулированных в подобных структурах, несут или их сотрудники, или иные лица, назначаемые в установленном порядке. Обработка информации происходит с применением строго определенных технических средств и программного обеспечения. 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, и переложения данного бремени на разработчика используемой технологии.

Меры технического характера по обеспечению безопасности персональных данных в виртуальной среде организаций напрямую зависят от вышеуказанной градации. Условно их можно *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. Традиционно средства технической защиты информации делятся на группы: физические, направленные на создание осязаемых препятствий к проникновению и/или доступу

к материальному носителю информации конфиденциального характера; аппаратные – устройства, способные пресекать несанкционированный доступ к информации и ее утечку; программные средства в виде специальных программных обеспечений, предназначенных для защиты информации в информационном пространстве; криптографические, основанные на возможности преобразования информации[264]. Обеспечение информационной безопасности физическими лицами на своих информационных устройствах может быть осуществлено с помощью паролей, двухфакторной аутентификации, программ – антивирусов. Одновременно с этим поведенческая грамотность также является залогом безопасности, для чего необходимо использовать только сертифицированное программное обеспечение, проводить его своевременное обновление, не переходить на подозрительные информационные ресурсы и не вводить на них свои идентификаторы и т.п[265].

Использование современных технологий сделало возможным рассмотрение вопроса *об отнесении к техническим мерам защиты информации условия безопасности, предоставляемые в отношении услуг разработчиками различных технологических решений и сервисов*. Так, к примеру мессенджеры WhatsApp и Telegram используют сквозное шифрование в сообщениях и звонках, что означает возможность прочтения сообщений только собеседниками. Одновременно с этим сервис позволяет скрывать персональную информацию и настраивать двухфакторную аутентификацию и т.п., что по своей природе вполне относимо к техническим мерам обеспечения безопасности информации, включая и персональные данные.

***Таким образом, по результатам проведенного исследования можно сделать следующие выводы:***

- *перечень мер организационного и технического характера, обязательный для исполнения операторами персональных данных в соответствии с Законом о персональных данных, разнится в зависимости от того, обрабатываются ли*

[264] Аль-Амори А., Дяченко П.В., Клочан А.Е., Бакун Е.В., Козелецкая И.К. Методы и средства защиты информации // The scientific heritage. 2020. № 51. С. 38–40.
[265] Босова Е.Д., Селищев В.А. Информационная безопасность: современные реалии // Известия ТулГУ. Технические науки. 2019. Вып.9. С. 298.

*персональные данные именно в информационной системе персональных данных или без создания такой системы;*

*- персональные данные в виртуальной среде организации подразделяются на две категории – поддающихся контролю со стороны оператора персональных данных, не поддающихся данному контролю или со сниженной степенью контроля;*

*- меры технического характера по обеспечению безопасности персональных данных надлежит разделить на две категории – обязательные к исполнению и рекомендательные, что находится в зависимости от субъекта, в чьи обязанности входит обеспечение защиты персональных данных в виртуальной среде организаций;*

*- необходимо отнести к техническим мерам защиты информации условия безопасности, предоставляемые в отношении услуг разработчиками различных технологических решений и сервисов.*

# Заключение

Результат проведенного исследования позволил сформировать вывод о том, что персональные данные, наряду со сведениями о частной жизни гражданина и т.п., являются составной частью более широкого и емкого явления – информации о человеке. Отнесение какой – либо информации к категории персональных данных возможно только в случае, когда отношения между субъектом персональных данных и оператором персональных данных складываются исключительно в связи с обработкой персональных данных в целях, устанавливаемых оператором, а информация, относящаяся к прямо определенному и косвенно определяемому физическому лицу, передается последним в адрес оператора в добровольном порядке. Только наличие вышеуказанной совокупности позволяет выделить из общей информации о человеке именно персональные данные, что может иметь место посредством судебного установления, закрепления в нормах права и локальных нормативных актах, а также в соответствии с волеизъявлением самого субъекта персональных данных.

Персональные данные — это и просто информация, относящаяся к физическому лицу, и сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных. В отношении данного понятия не только возможно, но и имеет место двоякое толкование, поскольку не совсем очевидно какие все-таки сведения о человеке стоит именовать биометрическими персональными данными, только те, которые используются для установления личности человека или все сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность. Подобные разночтения затрудняют правоприменение и не способствуют его единообразию, в связи с чем представляется целесообразным все сведения, характеризующие физиологические и биологические особенности человека, вне зависимости от целей их получения и

использования именовать биометрическими персональными данными с той лишь разницей, что одни предназначены для установления личности человека, а другие являются просто биометрическими персональными данными.

Технологическое развитие предлагает не только новые жизненные концепции как, например, виртуальная среда существования персональных данных, но и значительно расширяет их видовой и содержательный объем. В результате использования современных технологий появляется и фиксируется в цифровой формате совершенно новая, ранее не известная информация, например, поведенческие биометрические характеристики, такие как клавиатурный почерк, «когнитивный след», который еще называют цифровым почерком, характеризующим поведение пользователя при взаимодействии с различными технологичными устройствами, и т.п. Создание подобного рода технологий, способных не только уловить, но и что самое главное - зафиксировать всевозможную информацию о человеке, дает широкие возможности для ее дальнейшего использования и является основной отличительной чертой нашего времени.

Именно по этой причине, связанной с широким внедрением современных технологических решений, в результате деятельности любой хозяйствующей структуры появляется и накапливается достаточно большой объем информации, включая и персональные данные в цифровом формате, которая, вне всякого сомнения, имеет практическую и научную ценность. Так, и коммерческие инвесторы, и научные организации остро нуждаются в подобного рода информации как для построения более эффективных экономических моделей, так и для достижения научного прогресса. При этом нормы действующего законодательства правила использования вышеуказанной информации не устанавливают, а правовое регулирование в данном вопросе на настоящий момент носит экспериментальный характер, посредством предоставления ограниченному числу компаний на определенной территории и на определенное время права соблюдать действующее законодательство с рядом особенностей, позволяющих использовать различные технологии, включая и большие данные, в реальных правоотношениях.

Все эти изменения и нововведения неминуемо влекут за собой переосмысление прав и обязанностей как тех, кто эту информацию непосредственно создает – субъектов персональных данных, так и тех, кто ей владеет на законных основаниях – операторов персональных данных, на предмет установления их соотношения, а также соблюдения баланса частных и государственных интересов стратегического и научного назначения.

Вопрос права собственности на персональные данные и триады правомочий никак в законодательстве не решен. В правовой оборот включено понятие «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. Одновременно с этим обладателям информации предоставляются права использовать информацию, в том числе распространять ее, по своему усмотрению, передавать информацию другим лицам по договору или на ином установленном законом основании, а также осуществлять иные действия или разрешать осуществление таких действий. Приобретение оператором персональных данных правового статуса обладателя информации на основании договора с субъектом персональных данных позволит ему на законных основаниях как использовать персональные данные, так и распоряжаться ими по своему усмотрению. Поскольку какой-либо специальный регулятивный инструмент для такого рода договоров законом и иными нормативными правовыми актами не разработан представляется целесообразным рассмотреть на уровне законодательного закрепления правовую конструкцию договора о праве субъекта персональных данных разрешать или ограничивать третьему лицу доступ к информации, определяемой по каким-либо признакам.

Одним из аспектов, характеризующих виртуальную среду организаций, является ее техническая составляющая, представленная инфраструктурой, технологиями, программным обеспечением и т.п. привычными элементами цифровой действительности, которые осуществляют фиксацию персональных данных сотрудников и иных лиц в виртуальной среде организаций как в различных

производственных целях, так и в связи с тем, последняя является неотъемлемой частью самой технологии, например чат для онлайн переписки, изначально созданный для сохранения передаваемого текста, и т.п.

При этом в рамках трудового законодательства цели обработки персональных данных представлены в виде закрытого перечня, что формально должно расцениваться как запрет на их обработку в иных целях. В современных же реалиях повсеместно происходит использование специальных технических средств и прикладных программных продуктов, ориентированных как на организацию совместного рабочего процесса в рамках дистанционного доступа с его цифровой фиксацией, так и на современные методы контроля, преследующие различные цели, например отслеживание времени работы сотрудников в режиме удаленного доступа, а также на обеспечение информационной и иной безопасности самой организации. Все это активно пополняет персональными данными виртуальную среду организаций, где они хранятся в связи с наличием производственной и иной подобной необходимости.

В этой связи перечень целей обработки персональных данных работников, приведенный в Трудовом Кодексе РФ, нуждается в дополнении за счет включения к него таких целей обработки персональных данных как совместный рабочий процесс в виртуальной среде организации, а также контроль за информационной безопасностью организации. Одновременно с этим необходимо закрепить на законодательном уровне право работодателя использовать в целях контроля за выполнением сотрудниками своих трудовых обязанностей, а также в целях осуществления информационной безопасности наряду с приборами, устройствами, оборудованием и (или) комплексами (системами) приборов, устройств, оборудования, обеспечивающих дистанционную видео-, аудио- или иную фиксацию процессов производства работ, информационные технологии (методы и инструменты).

Существование виртуальной среды породило актуальную на настоящий момент проблему, связанную с достоверностью установления в ней личности человека. При этом позиционируется, что именно биометрия является наиболее

совершенной системой идентификации личности, которая позволяет практически со стопроцентной гарантией исключить возможность подмены. В Российской Федерации создана и действует Единая биометрическая система (ЕБС), которой придан статус государственной информационной системы (ГИС) с гарантией наивысшей степени защищенности данных. Организации и индивидуальные предприниматели наряду с государственными органами, органами местного самоуправления, организациями финансового рынка, нотариусами поименованы в качестве пользователей ЕБС, но тем не менее для них возможность установления личности физического лица, например при проведении собеседования с претендентом на занятие вакантной должности или предполагаемым партнером при вступлении в гражданско-правовые отношения с использованием ЕБС на настоящий момент законодательством не предусмотрена. В этой связи вопрос о возможности предоставления организациям и индивидуальным предпринимателям права взаимодействия с ЕБС требует дополнительной разработки в целях определения порядка его реализации. Что же касается иных технологических решений подтверждения личности в виртуальной среде организаций, но уже без применения биометрических шаблонов, то их введение в информационный оборот целесообразно сопровождать прохождением сертификационных процедур на добровольной или обязательной основе, которую возможно организовать на базе саморегулирования.

В условиях все ускоряющегося технологического развития и изменяющейся действительности совершенно очевидно проявилась некоторого рода инертность правового регулирования, не позволяющая оперативно реагировать на все вызовы и проблемы, возникающие в процессе информатизации общественных отношений. В этой связи значительную роль в регулировании обработки персональных данных и их защите способны играть локальные нормативные акты хозяйствующих субъектов, призванные активно использоваться с целью закрепления обязательных для исполнения локальных механизмов, методов и способов достижения вышеуказанных целей. В этой связи востребованным является исследование с целью определения состава нормативных актов локального характера, принятие

которых обусловлено переходом деловой активности в виртуальную среду. К таким документам, частично не имевших хождение ранее, следует отнести:

- концепцию информационной безопасности;

- политику информационной безопасности;

- методы и способы защиты информации от несанкционированного доступа;

- политику работы в корпоративной сети, а также с такими инструментами как мессенджеры, онлайн-платформы различного назначения и т.п.;

- политику работы в условиях удаленного доступа, а также с сетью Интернет;

- политику использования паролей и иных средств доступа в виртуальную среду организации;

- политику безопасности ИТ-инфраструктуры, включая и личные компьютерные устройства, мобильные телефоны и иные гаджеты, используемые сотрудниками в виртуальной среде организации;

- политику защиты конфиденциальной информации;

- политику использования программного обеспечения и антивирусной защиты, включая и личные компьютерные средства, мобильные телефоны и иные гаджеты сотрудников и иных лиц, получающих доступ в виртуальную среду организации;

- политику проведения аудита информационной безопасности;

- политику принятия решений об использовании новых технологий с учетом правил их тестирования или подтверждения иным способом соответствия их функционала заявленным критериям;

- политику обеспечения и защиты критически значимой информации при взаимодействии с третьими лицами в виртуальной среде организации;

- политику хранения критически значимой информации в виртуальной среде организации;

- и др., необходимость принятия которых обусловлена индивидуальными потребностями организации.

Актуальность темы диссертации обусловлена слабой разработанностью в науке правового регулирования и защиты персональных данных в виртуальной

среде организаций. Изначально в диссертационном исследовании проведен комплексный анализ правовой природы персональных данных, который позволил определить необходимую совокупность признаков информации подобного рода. В дальнейшем, на примере используемых технологий были выявлены новые виды создаваемой ими информации, а также проведен анализ на предмет возможного отнесения последней к персональным данным. Одновременно с этим выявлены те области законодательства, которые нуждаются в приведение в соответствие с фактическими обстоятельствами использования информационных технологий, порождающих появление и фиксацию новой информации в цифровом формате. Предложены способы решения актуальных проблем, связанных с использованием вышеуказанной информации, а также с установлением и подтверждением личности человека в виртуальной среде организаций.

В рамках исследования выявлены сопутствующие рассматриваемой теме вопросы, подлежащие отдельному рассмотрению, что является почвой для проведения дальнейших исследований в данной области. Научный и культурный прогресс остро нуждается в огромном количестве персональных данных, характеризующих, например, поведенческие стереотипы людей, а имеющиеся технологии, основное значение среди которых в последнее время придается искусственному интеллекту, позволяет извлекать из этой информации полезный результат в заданной части. Возможность успешного развития технологий на базе больших данных в настоящий момент объективно имеют только те организации, которые этими данными владеют, такие как банки, медицинские, образовательные и т.п. учреждения. При этом в рамках равных прав на проведение научных исследований и создания информационных технологий иные организации, не располагающие вышеуказанной информацией в нужном объеме по объективным причинам, ставятся в неравное положение, в связи с чем в будущем не исключено введение ограничений на монопольное владение информацией с обязательством передавать имеющиеся персональные данные в обезличенном виде для использования иными организациями в научных и иных общественно-полезных целях.

# БИБЛИОГРАФИЧЕСКИЙ СПИСОК

## I. Нормативные правовые акты

1. Конституция Российской Федерации. Принята на всенародном голосовании 12.12.1993 (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30 декабря 2008 года № 6-ФКЗ, от 30 декабря 2008 года № 7-ФКЗ, от 5 февраля 2014 года № 2-ФКЗ, от 21 июля 2014 года № 11-ФКЗ, от 14 марта 2020 года № 1-ФКЗ) и Федеральных конституционных законов от 4 октября 2022 года № 5-ФКЗ, от 4 октября 2022 года № 6-ФКЗ, от 4 октября 2022 года № 7-ФКЗ, от 4 октября 2022 года № 8-ФКЗ.) // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru.

2. Федеральный конституционный закон от 05.02.2014 № 3-КФЗ (ред. от 14.07.2022) «О Верховном Суда Российской Федерации» // СЗ РФ. 2014. № 6. Ст. 550.

3. Федеральный конституционный закон от 21.07.1994 № 1-ФКЗ «О Конституционном Суде Российской Федерации» (ред. от 31.07.2023) // СЗ РФ. 25.07.1994. № 13. Ст. 1447.

4. Гражданский Кодекс РФ. Часть I от 30.11.1994 № 51-ФЗ (ред. от 08.08.2024) // СЗ РФ. 1994. № 32. Ст. 3301.

5. Уголовный Кодекс РФ от 13.06.1996 № 63-ФЗ (ред. 08.08.2024) // СЗ РФ.1996. № 25. Ст. 2954.

6. Трудовой Кодекс РФ от 30.12.2001 № 197-ФЗ (ред. от 08.08.2024) // СЗ РФ.2002. № 1 (ч. I). Ст. 3.

7. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 01.07.2024) // СЗ РФ. 24.12.2001. № 52 (ч. I). Ст. 4921.

8. Кодекс административного судопроизводства Российской Федерации» от 08.03.2015 № 21-ФЗ (ред. от 08.03.2024) // СЗ РФ. 2015. № 10. Ст.1391.

9. Декларация прав и свобод человека и гражданина // Ведомости СНД и ВС СССР. 1991. № 37. Ст. 1083.

10. Закон от 11.03.1992 № 2487–1 (ред. от 25.12.2023) «О частной детективной и охранной деятельности в РФ» // Ведомости СНД и ВС СССР. 1992. № 17. Ст. 888.

11. Закон РФ от 27.12.1991 № 2124-I (ред. от 11.03.2024) «О средствах массовой информации» // Российская газета от 08.02.1992. № 32.

12. Федеральный закон от 19 декабря 2005 года № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» // СЗ РФ. 2005. № 52 (ч.I). Ст. 5573.

13. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 08.08.2024) «Об информации, информатизации и защите информации» // СЗ РФ. 2006 г. № 31 (ч. I). Ст. 3448.

14. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) «О персональных данных» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.

15. Федеральный закон от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» // СЗ РФ. 2011. № 31. Ст. 4701.

16. Федеральный закон от 29.12.2022 № 572-ФЗ (ред. от 08.08.2024) «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» // СЗ РФ. 2023. № 1 (ч. I). Ст. 19.

17. Федеральный закон «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» от 22.12.2008 г. № 262-ФЗ (ред. от 14.07.2022) // СЗ РФ. 2008. № 52 (ч. I). Ст. 6217.

18. Федеральный закон от 31.07.2020 № 258-ФЗ (ред. от 08.08.2024) «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // СЗ РФ. 2020. № 31 (часть I). Ст. 5017.

19. Федеральный закон от 24.04.2020 № 123-ФЗ (ред. от 08.08.2024) «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» // СЗ РФ. 2020. № 17. Ст.2701.

20. Федеральный закон от 01.12.2007 № 315-ФЗ «О саморегулируемых организациях» (ред. от 02.07.2021) // СЗ РФ. 2007. № 49. Ст. 6076.

21. Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 08.08.2024) «О Коммерческой тайне» // СЗ РФ. 2004. № 32. Ст.3283.

22. Основы законодательства РФ о нотариате от 11.02.1993 № 4462-I (ред. от 08.08.2024) // «Российская газета» от 13.03.1993.

23. Указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении перечня сведений конфиденциального характера» // СЗ РФ. 1997. № 10. Ст. 1127.

24. Указ Президента РФ от 30.05.2005 № 609 (ред. от 29.04.2023) «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведения его личного дела» // СЗ РФ. 2005. № 23. Ст. 2242.

25. Указ Президента РФ от 13.03.1997 № 232 «Об основном документе, удостоверяющем личность гражданина РФ на территории РФ // СЗ РФ. 1997. № 11. Ст.1301.

26. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

27. Указ Президиума ВС СССР от 18.09.1973 № 4812-VIII «О ратификации Международного пакта об экономических, социальных и культурных правах и Международного пакта о гражданских и политических правах» // Ведомости Верховного Совета СССР. 1973. № 40. Ст. 564.

28. Указ Президента РФ от 18.09.2023 № 695 «О представлении сведений, содержащихся в документах, удостоверяющих личность гражданина Российской Федерации, с использованием информационных технологий» // СЗ РФ. 25.09.2023. № 39. Ст. 7012.

29. Постановление Правительства Российской Федерации от 15.06.2022 № 1067 (в ред. от 31.05.2023 № 893) «О случаях и сроках использования биометрических персональных данных, размещенных физическим лицом в единой биометрической системе с использованием мобильного приложения единой биометрической системы, в том числе при отсутствии сведений о физическом лице в единой системе идентификации и аутентификации утверждены» // СЗ РФ. 2022. № 25. Ст. 4337.

30. Постановление Правительства РФ от 21.03.2012 г. № 211 (ред. от 15.04.2019) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» // СЗ РФ. 2012. № 14. Ст. 1626.

31. Постановление Правительства РФ от 30.06.2018 г. № 772 (ред. от 23.03.2024) «Об определении состава сведений, размещаемых в Единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства РФ» // СЗ РФ. 2018. № 28. Ст. 4234.

32. Постановление Правительства РФ от 23.12.2023 г. № 2267 «Об утверждении Положения о паспорте гражданина РФ, образца и описания бланка паспорта гражданина РФ» // СЗ РФ. 2024. № 1 (часть 1). Ст. 163.

33. Постановление Правительства РФ от 06.08.2015 № 813 (ред. от 29.08.2024) «Об утверждении Положения о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность» // СЗ РФ. 17.08.2015. № 33. Ст. 4843.

34. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" // СЗ РФ. 2012. № 45. Ст.6257.

35. Постановление Правительства РФ от 06.07.2008 г. № 512 (ред. от 27.12.2012) «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» // СЗ РФ. 2008. № 28. Ст.3384.

36. Приказ Министра обороны Российской Федерации от 04.12.2019 № 707 (ред. от 06.06.2024) «О персональных данных в Вооруженных Силах Российской Федерации» // СПС «КонсультантПлюс».

37. Приказ Министерства здравоохранения РФ от 04.03.2019 № 110н (ред. от 28.09.2020) «Об обработке персональных данных в Министерстве здравоохранения РФ» // СПС «КонсультантПлюс».

38. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 12.05.2023 г. № 453 "О порядке обработки биометрических персональных данных и векторов единой биометрической системы в единой биометрической системе и в информационных системах аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации, организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц" (вместе с "Порядком обработки, включая сбор, хранение, биометрических персональных данных, в том числе требованиями к параметрам биометрических персональных данных", "Порядком размещения и обновления биометрических персональных данных в единой биометрической системе, а также случаями и сроками использования биометрических персональных данных при их размещении в единой биометрической системе в соответствии с частью 14 статьи 4 Федерального закона от 29 декабря 2022 г. № 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", "Порядком обработки, включая сбор, хранения и уничтожения биометрических персональных данных, векторов единой биометрической системы в информационных системах аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации, организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц", "Порядком создания и передачи векторов единой биометрической системы в целях осуществления аутентификации", "Требованиями к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных, векторов единой биометрической системы в целях проведения идентификации и (или) аутентификации, а также порядком подтверждения соответствия информационных технологий и технических средств указанным требованиям") // СПС «КонсультантПлюс».

39. Приказ МВД России от 16.11.2020 № 773 (ред. 26.07.2022) «Об утверждении Административного регламента Министерства внутренних дел Российской Федерации по предоставлению государственной услуги по выдаче, замене паспортов гражданина Российской Федерации, удостоверяющих личность гражданина Российской Федерации на территории Российской Федерации» // СПС «КонсультантПлюс».

40. Рекомендации по стандартизации Р50.1.053-2005. «Информационные технологии. Основные термины и определения в области технической защиты информации». Утв. приказом Федерального агентства по техническому регулированию и метрологии от 06.04.2005 г. № 77-ст // СПС «КонсультантПлюс».

41. Национальный стандарт РФ. Информационные технологии. БИОМЕТРИЯ. Общие положения и примеры применения. ГОСТ Р 54412-2019 (ISO/IEC TR 24741:2018) // СПС «КонсультантПлюс».

42. Национальный стандарт РФ. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. ГОСТ Р 52633.0-2006 // СПС «КонсультантПлюс».

43. Государственный стандарт РФ ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» принят постановлением Госстандарта РФ от 09.02.1995 г. № 49 // СПС «КонсультантПлюс».

44. Национальный стандарт РФ ГОСТР 57721 —2017 Информационно-коммуникационные технологии в образовании. Эксперимент виртуальный. Общие положения // СПС «КонсультантПлюс».

45. Национальный стандарт РФ. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными ГОСТ Р ИСО/МЭК 19794-1-2008 // СПС «КонсультантПлюс».

46. Национальный стандарт РФ. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» // СПС «КонсультантПлюс».

47. ГОСТ Р ИСО/МЭК 27001-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» // СПС «КонсультантПлюс».

48. Национальный стандарт РФ. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения // СПС «КонсультантПлюс».

49. ГОСТ Р 52292-2004. Национальный стандарт РФ. Информационная технология. Электронный обмен информацией. Термины и определения // М.: ИПК Издательство стандартов. 2005.

50. Рекомендации по стандартизации. Р 50.1.056-2005. «Техническая защита информации. Основные термины и определения». Утв. приказом Федерального агентства по техническому регулированию и метрологии от 29.12.2005 г. № 479-ст // СПС «КонсультантПлюс».

51. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // СПС «КонсультантПлюс.

## II. Международные правовые акты

1. Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеей ООН резолюцией 217 А (III) от 10 декабря 1948 г.) // Российская газета. 1995. № 67.

2. Конвенции 108 Совета Европы о защите прав физических лиц в отношении автоматической обработки персональных данных 1981 года // СПС «КонсультантПлюс».

3. Модельный закон «О персональных данных», принят 16 октября 1999 года на Межпарламентской ассамблее государств-участников СНГ // Информационный бюллетень Межпарламентской Ассамблеи государств-участников СНГ. 2000. № 23.

4. Международный пакт о гражданских и политических правах от 16 декабря 1966 года // Ведомости Верховного Совета СССР. 1976. № 17, ст. 291.

5. Классификатор видов документов, удостоверяющих личность, утвержденном Решением Коллегии Евразийской экономической комиссии от 2 апреля 2019 года № 53 // текст решения опубликован на Правовом портале Евразийского экономического союза. URL: https://docs.eaeunion.org.

6. Решение Коллегии Евразийской экономической комиссии от 2 апреля 2019 года № 53 // текст решения опубликован на Правовом портале Евразийского экономического союза URL: https://docs.eaeunion.org.

7. Модельный закон «О цифровых правах» (принят на пятьдесят пятом пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ (постановление от 14 апреля 2023 года № 55–12)) // СПС «КонсультантПлюс».

## III. Судебная практика

1. Постановление Пленума Верховного Суда Российской Федерации от 25 декабря 2018 г. № 50 «О практике рассмотрения судами дел об оспаривании нормативных правовых актов и актов, содержащих разъяснения законодательства

и обладающих нормативными свойствами» // Бюллетень Верховного Суда Российской Федерации. 2019. № 2.

2. Определение Конституционного Суда РФ от 29.09.2011 г. № 1063-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Багадурова Магомеда Магомедовича на нарушение его конституционных прав подпунктом 1 пункта 3 статьи 6 Федерального закона "Об адвокатской деятельности и адвокатуре в Российской Федерации", статьей 10 Федерального закона "О персональных данных" и частью второй статьи 57 Гражданского процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс».

3. Определения Конституционного Суда РФ от 9 июня 2005 г. № 248-О «Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом "б" части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации» // СПС «КонсультантПлюс».

4. Определения Конституционного Суда РФ от 26 января 2010 г. № 158-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Усенко Дмитрия Николаевича на нарушение его конституционных прав положениями статьи 8 Федерального закона «Об оперативно-розыскной деятельности» // СПС «КонсультантПлюс».

5. Определение Конституционного Суда РФ от 28 июня 2012 г. № 1253-О «Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации» // СПС «КонсультантПлюс».

6. Постановление Конституционного Суда РФ от 26.10.2017 № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А.И. Сушкова» // СПС «КонсультантПлюс».

7. Обзор судебной практики Верховного Суда РФ № 2, утв. Президиумом Верховного Суда РФ от 22 июля 2020 года // СПС «КонсультантПлюс».

8. Постановление Пленума Верховного Суда РФ от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138[1], 139, 144[1], 145, 145[1] УК РФ)» // СПС «КонсультантПлюс».

9. Решение Арбитражного суда Мурманской области от 3 апреля 2017 г. № А42-342/2017 // URL: https://kad.arbitr.ru/Card/f2ba9d7a-13ce-493c-ba04-a14c927a4c7c (дата обращения: 17.09.2024).

10. Определение Верховного Суда № 305-ЭС23-12160 от 21.07.2023 // URL: https://base.garant.ru/407421338/ (дата обращения: 17.09.2024).

11. Определение Верховного Суда № 13-В05-13 от 01.03.2006 // URL: https://vsrf.ru/stor_pdf.php?id=137200 (дата обращения: 17.09.2024).

12. Решение Савеловского районного суда г.Москвы от 06.11.2019 по делу № 2а-577/2019 // URL: https://mos-gorsud.ru/rs/savyolovskij/services/cases/kas/details/988f386e-be51-47b0-b48f-e871043ef1fc?caseNumber=2a-577/2019 (дата обращения: 17.09.2024).

13. Апелляционное определение Свердловского областного суда от 16 ноября 2016 года по делу № 33-20507/2016 // URL: https://leninskytag--svd.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=707479&delo_id=1540005&new=0&text_number=1 (дата обращения: 17.09.2024).

## IV. Специальная научная и монографическая литература

1. Авакьян С.А. Конституционное право России. Учебный курс. В 2-х томах. 5-е изд., перераб. и доп. Том 1. М.: Норма, 2014.

2. Антонов, Д.Н., Антонова, И.А. Метрические книги России XVIII - начала XX в. М.: РГГУ, 2006.

3. Байбурин, А.К. К антропологии документа: паспортная «личность» в России Антропология социальных перемен. Сборник статей к 70-летию В.А.Тишкова. М.: РОССПЭН, 2011.

4. Бачило И.Л. Информационное право. М.: Издательство Юрайт, 2013.

5. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник / Под редакцией акад. Б.Н. Топорнина Спб.: Юрид.центр Пресс, 2001. С. 151.

6. Богданова Н.А. Основные права человека в России: идея, ее конституционное отражение и практика реализации // Конституционные идеалы и ценности в практической демократии: материалы и доклады XII Международной научно-практической конференции (Самара, 29 сентября – 2 октября 2016 г.) / Под ред. В.В. Полянского, В.Э. Волкова. Самара: Изд-во «Самарский университет», 2017.

7. Борисов М. А., Будник Р.А., Войниканис Е. А., Дейнеко А.Г., Елин В.М., Ерофеева Е.В., Жарова А.К., Монахов В. Н., Околёснова О. А., Перепелица Е. В., Петрин И. В., Примакова А.В., Серго А. Г., Тедеев А. А., Федотов М.А., Шаблинский И. Г., Якимовская Н. Л. Информационное право: Учебник для вузов / Под общей редакцией Федотова М.А. М.: Юрайт, 2023.

8. Безверхов А.Г., Коростелев В.С. «Проект уголовного уложения Российской Империи 1813 года», утв. редакционно-издательским советом Самарского государственного Университета в качестве монографии. Самарский университет, 2013.

9. Важорова М. А. История возникновения и становления института персональных данных. Государство и право: теория и практика: материалы I Междунар. науч. конф. (г. Челябинск, апрель 2011 г.). Челябинск: Два комсомольца, 2011. URL: https://moluch.ru/conf/law/archive/37/365/ (дата обращения: 17.09.2024).

10. Жарова А.К., Елин В.М., Минбалеев А.В. Парадигма цифрового профилирования деятельности человека: риски, угрозы, преступления: монография / М.: РУСАЙНС, 2024. - 240с.

11. Копылов В.А. Информационное право: Учебник. М.: Юристъ, 2002.

12. Маньков А.Г. Российское законодательство X-XX вв.: в 9-ти томах. Т.4. Законодательство периода становления абсолютизма. М.: Юридическая литература, 1986.

13. Нуркаева Т.Н. Уголовно-правовая охрана личности, ее прав и свобод: вопросы теории и практики. ООО «Проспект», 2017.

14. Полякова Т.А., Стрельцов А.А. Организационное и правовое обеспечение информационной безопасности: Учебник и практикум для бакалавриата и магистратуры. М.: Юрайт, 2016.

15. Пушкин А. Правовой режим иностранных инвестиций в Российской Федерации. М.: Альпина Паблишер, 2012.

16. Пугачев В.П. Глобалистский тоталитаризм: Социальные мутации цифрового капитализма: формирование человека и манипулятивные технологии управления // М.:ЛЕНАНД. 2022. (Будущая России. № 34).

17. Савченко Е.А. Право и виртуальное пространство: коллективная монография; отв. ред. Ю.А. Тихомиров // Москва: Проспект, 2025.

18. Стрельцова, Е.Г., Самсонова, М.В., Чайкина, А.В. Цифровые технологии в гражданском и административном судопроизводстве: практика, аналитика, перспективы. «Инфотропик Медиа», 2022.

19. Тедеев А.А. Инфомационное право: Учебник. М., 2005.

20. Терещенко Л.К. Научные концепции развития российского законодательства: коллективная монография. Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. М. 2024. 656 с.

21. Федотов М.А. Информационное право: учебник для бакалавриата, специалитета и магистратуры. М.: Юрайт, 2019.

22. Черкасов К.В. Трансформация прав и обязанностей человека и гражданина в условиях цифрового общества и государства // Сборник материалов Всероссийской научно-практической конференции «Защита прав человека: теория и региональная практика». Хакасский государственный университет им. Н.Ф. Катанова. 2021. 200 с.

23. Чистяков О.И. Конституция СССР 1924 года. Учебное пособие. М.: Зерцало-М, 2004.

24. Шугай А.А. Защита персональных данных: формирование и развитие научных взглядов. Научные стремления. Научные стремления. ООО «Лаборатория интеллекта» и Центр молодежных инноваций. Минск: «Энциклопедикс», 2013. Выпуск 7.

## V. Публикации в периодических изданиях

1. Алексеев К.Н. Роль больших данных в цифровой экономике // Цифровая экономика. 2019. № 3 (7).

2. Аль-Амори А., Дяченко П.В., Клочан А.Е., Бакун Е.В., Козелецкая И.К. Методы и средства защиты информации // The scientific heritage. 2020. № 51.

3. Баженов С.В., Дивольд В.Е., Морозов А.А., Попов Д.В., Сафронов Д.М., Серов А.В. Создание Концепции национальной системы биометрической идентификации личности // Труды Академии управления МВД России. 2020. № 2.

4. Белая О.В., Кицай Ю.А. Биометрические данные как средство идентификации и аутентификации человека: Российский и международный опыт // Право и практика. 2020. № 1.

5. Борисов М.А., Северин В.А. Проблемы допуска и доступа субъектов к коммерческой и служебной тайне в условиях цифровой экономики // Пробелы в российском законодательстве. 2019. № 6.

6. Босова Е.Д., Селищев В.А. Информационная безопасность: современные реалии // Известия ТулГУ. Технические науки. 2019. Вып.9.

7. Брежнев О.В. Конституция 1993 г. и развитие конституционного правосудия в России // Вестник Московского Университета. Серия 11. Право. 2023. Т.64. № 6. С. 75.

8. Бундин М.В. Система информации ограниченного доступа и конфиденциальность // Вестник Нижегородского университета им. Лобачевского. 2015. №1.

9. Вздорова Л.П. Шестой технологический уклад: новый формат мира // Символ науки № 9/2020.

10. Галиуллина Д.Р. История развития биометрических документов в России // Вестник науки и образования. 2015. № 9 (11).

11. Галиуллина Д.Р. Биометрические персональные данные // Документ. Архив. История. Современность. 2015. вып.15.

12. Егорова М.А. Проблема цифровой идентификации личности в Российской Федерации и Европейском Союзе // Вестник Университета им. О.Е. Кутафина. 2022. № 1.

13. Кадников Б.Н. О становлении и развитии законодательства об охране частной жизни // Общество и право. 2016. № 2 (56).

14. Казакевич Е.И. Защита прав и свобод человека при обработке персональных данных в период цифровой трансформации // Уральский журнал правовых исследований. 2022. № 4.

15. Камалова Г.Г. История охраны конфиденциальности сведений в России // Диалог со временем. 2019. выпуск 66.

16. Крохина Ю.А. Проблемы правового регулирования цифровых технологий, применяемых Центральным банком РФ и финансовыми институтами // Мониторинг правоприменения. 2022. № 4 (45). С. 33.

17. Кузенков К.Г. Судебная практика Верховного Суда РФ как источник права // Юридическая наука. 2021. № 12.

18. Кутейников Л.Д., Ижаев О.А., Лебедев В.А., Зенин С.С. Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности // LEX RUSSICA. 2022. Том 75 № 2 (183). С. 121-131.

19. Кучеренко А.В. Сравнительный анализ принципов отнесения информации к персональным данным и иным видам сведений конфиденциального характера // Вестник АмГУ. 2009. выпуск 44.

20. Майоров А.В., Поперина, Е.Н. Формирование и развитие права на неприкосновенность частной жизни // Юридическая наука и правоохранительная практика. 2012. № 3 (21).

21. Макаров В.О. Классификация регулятивных песочниц (экспериментальных правовых режимов): Российский и зарубежный опыт // Legal Concept – Правовая парадигма. 2021. Т.20. №3.

22. Материалы Народного комиссариата юстиции. Народный суд. М., 1918. Вып. 11. 56-57 с. из статьи Ульянченко А.М. «История развития уголовного законодательства России об ответственности за преступления против неприкосновенности частной жизни» // Известия Вузов. Северо-Кавказский регион. Общественные науки. 2006. № 2.

23. Малеина М.Н. Право на тайну и неприкосновенность персональных данных // Журнал российского права. 2010. № 11.

24. Майстренко Г.А., Майстренко А.Г. Источники правового регулирования защиты персональных данных работника в России // Legal Bulletin. 2020. Т.5 (1).

25. Минбалеев А.В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2012. № 2 (4).

26. Минбалеев А.В., Полякова Т.А., Троян Н.А. Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. 2023. № 5. С.131-144.

27. Немыкина О.И. Понятие виртуальности в филосовском контексте // Известия высших учебных заведений. Поволжский регион. Гуманитарные науки. Философия. 2011. № 1 (17). С. 53–62.

28. Поликанина О.А., Поликанин А.Н., Шабурова А.В. Организация защиты персональных данных в государственных и муниципальных системах // Интерэкспо ГЕО-Сибирь. 2022. Том 6.

29. Проскурякова М.И. Конституционно-правовые рамки защиты персональных данных в России // Вестник СПбГУ. 2016. Сер.14. вып.2.

30. Саушкин С.О., Синцов Г.В. К вопросу о соотношения институтов защиты персональных данных и защиты неприкосновенности частной жизни // Гуманитарный научный вестник. 2020. №2.

31. Савченко Е.А. Культурные права человека в условиях цифровизации // Вестник Томского государственного университета. Право. 2023. № 49. С. 151-164.

32. Солдатова В.И. Защита персональных данных в условиях применения цифровых технологий // LEX RUSSICA. 2020. т.73. № 2 (159).

33. Северин В.А. Правовые аспекты обеспечения информационной безопасности цифровой экономики // Пробелы в российском законодательстве. 2023. Том 16. № 8.

34. Северин В.А. Правовой институт персональных данных в системе российского права // Коммерческое право. Научно-практический журнал. 2020. № 4 (Том 39).

35. Сергеев А.П., Терещенко Т.А. Большие данные: в поисках места в системе гражданского права // Закон. 2018. № 11. С. 106–123.

36. Терещенко Л.К., Тиунов О.И. Правовой режим персональных данных // Журнал российского права. 2014. № 12.

37. Терещенко Л.К. О соблюдении баланса интересов при установлении мер защиты персональных данных // Журнал российского права. 2011. № 5.

38. Терещенко И.А. Биометрические персональные данные: проблемы перспективы определения понятия // Закон и право. 2024. № 2.

39. Троицкая А.А. Основные права: происхождение, юридическая природа и пределы защиты // Сравнительное конституционное обозрение, 2013. № 1 (92). С. 67

40. Фомина А.В., Мухин К.Ю. Индустрия 4.0. Основные понятия, преимущества и проблемы // Экономический вектор. 2018. № 3.

41. Шальнова Ю.П. Монетизация больших данных: технико-экономический анализ драйверов роста и издержек // Экономика. Информатика. 2020. Том 47. № 3. С.492

## VI. Диссертации

1. Абаев Ф.А. Правовое регулирование отношений по защите персональных данных работника в трудовом праве: автореф. дис. … канд.юрид.наук. Москва, 2014.

2. Бундин М.В. Персональные данные в системе информации ограниченного доступа: автореф. дис. … канд.юрид.наук. М., 2017.

3. Камалова Г.Г. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества: автореф. дис. … канд. юрид. наук. М., 2020.

4. Кудашкин Я.В. Правовое обеспечение безопасности обработки персональных данных в сети Интернет: автореф. дис. … канд.юрид.наук. М., 2019.

5. Просветова О.Б. Защита персональных данных: автореф. дис. … канд.юрид.наук. Воронеж, 2005.

6. Станскова У.М. Трудоправовые средства обеспечения конфиденциальности информации ограниченного доступа: автореф. дис. … канд.юрид.наук. Екатеринбург, 2014.

7. Телина Ю.С. Конституционное право гражданина на неприкосновенность частной жизни, личную и семейную тайну при обработке персональных данных в России и зарубежных странах: дис. … кандидата юрид. наук. М., 2016.

8. Терещенко Л.К. Правовой режим информации: дис. ... доктора юрид. наук. М., 2011.

## VII. Иные источники

1. Полное собрание законов Российской империи (ПСЗ- I). Т. IV. № 1908 // СПС «КонсультантПлюс».

2. Полное собрание законов Российской империи (ПСЗ-1). Т. XX. № 14948 // СПС «КонсультантПлюс».

3. Полное собрание законов Российской империи ПСЗ I. Т. XL. Общее приложение к собранию. К Т. XXVII. № 20266а // СПС «КонсультантПлюс».

4. Аптекарский Устав. Раздел Б. «История фармацевтического сословия». Стр. XXXIII. Извлеченный из Свода законов полных собраний законов, распубликованных циркуляров Министерства внутренних дел, постановлений Медицинского совета и разъясняемый историей законодательства / [соч.] Н. Варадинова, д-ра прав и философии, чл. С.-Петерб. и Венского фармацевтического и других ученых обществ. - С.-Петербург: Тип. М-ва вн. дел, 1880. - 12, LXX. Место хранения оригинала: РГБ. URL: htpps://www.prlib.ru> item (дата обращения 17.09.2024).

5. Аптекарский Устав. Раздел А. «Права и обязанности фармацевтов». С. 13. Свод законов. Т.III. Устав врачебный. Раздел Ф. «Ученые степени и звания». Извлеченный из Свода законов полных собраний законов, распубликованных циркуляров Министерства внутренних дел, постановлений Медицинского совета и разъясняемый историей законодательства / [соч.] Н. Варадинова, д-ра прав и философии, чл. С.-Петерб. И Венского фармацевтического и других ученых обществ. – С.-Петербург: Тип. М-ва вн. Дел, 1880. – 12, LXX. Место хранения оригинала: РГБ. URL: htpps://www.prlib.ru> item (дата обращения 17.09.2024).

6. Гоголь Н.В. Мертвые души. М.: Азбука. 2024. 352 с.

7. Проект уголовного уложения Российской Империи // РГИА Ф. 1251 Оп. 1, часть 1 Д. 10.

8. Уложение о наказаниях уголовных и исправительных. Санкт-Петербург: Тип. 2 отделения собств. е. и. в. канцелярии, 1845. - [4], IV, 898, XVII. URL: https://viewer.rsl.ru/ru/rsl01002889696?page=1&rotate=0&theme=white

9. Энциклопедический словарь Брокгауза и Ефрона. т.VII (1892). URL: https://runivers.ru/lib/book3182/10144/.

10. Свод законов Российской Империи, издание 1857 года, т.12, часть 1, тетрадь 3, ст. 11, Типография Второго Отделения Собственной Е.И.В. Канцелярии // СПС «КонсультантПлюс».

11. Судебные Уставы 20 ноября 1864 года, с изложением рассуждений, на коих они основаны. Часть первая, стр. III-IV // СПб, 1866.

12. Уложение о наказаниях уголовных и исправительных 1885 года // издано проф. Ипм.Училища правоведения… Н.С. Таганцевым. 5-е изд., доп. Санкт-Петербург: тип. М.Стасюлевича, 1886. – [4].

13. Новое Уголовное Уложение, высочайше утвержденное 22 марта 1903 года // СПб.: Изд. В.П.Анисимова.1903.

14. Временное положение о военной цензуре // Собрание узаконений и распоряжений Правительства. Отдел I. № 192. 20.07.1914 // СПС «КонсультантПлюс».

15. Работа профессора церковного права Петербургского университета и священнослужителя Русской православной церкви Михаила Горчакова «О тайне супружества» // Санкт-Петербург: тип. В.С. Балашева, 1880. -[4], IV, 384, 55 с.

16. Декреты Советской власти. Т. 1. М., 1957.

17. Собрание узаконений и распоряжений рабочего и крестьянского Правительства. 1919. № 66.

18. Декларация прав трудящегося и эксплуатируемого народа. 3 (16) января 1918 г. // Декреты Советской власти. Т. 1. М., 1957.

19. Хрестоматия по истории отечественного государства и права 1917-1991 годов // М.: Зерцало, 1997.

20. Конституция РСФСР 1925. Известия ЦИК СССР и ВЦИК, 26.05.1925, № 118 // Собрание узаконений и распоряжений Рабоче-крестьянского Правительства РСФСР. 1925. № 30. Ст. 218.

21. Устав почтовый, телеграфный, телефонный и радиосвязи СССР // СЗ СССР. 1929. № 22. Ст.ст.193, 194.

22. Конституции СССР 1936 года Известия ЦИК СССР и ВЦИК. 1936. № 283.

23. Уголовный Кодекс 1961 года // Ведомости Верховного Совета РСФСР. 1960. № 40. Ст.591.

24. Конституция СССР от 7 октября 1977 года/ Ведомости Верховного Совета СССР. 1977. № 41. Ст. 617.

25. Конституции РСФСР от 12 апреля 1978 года/ Ведомости Верховного Совета РСФСР. 1978. № 15. Ст. 407.

26. Economy.gov.ru Министерство экономического развития Российской Федерации. Приоритетные направления / Государственное управление // Нормативное регулирование цифровой среды. Экспериментальные правовые режимы.

27. Smart engines. Аналитический отчет: «Исследование актуальных угроз мошенничества с использованием поддельных документов» // URL: https://smartengines.ru/passport-scanners/ (дата обращения 17.09.2024).

28. АДС-СОФТ // URL: https://ads-soft.ru/online-raspoznavanie-dokumentov/#case (дата обращения 17.09.2024).

29. Smart engines. Аналитический отчет: «Исследование актуальных угроз мошенничества с использованием поддельных документов» // URL: https://smartengines.ru/face-verification/ (дата обращения 17.09.2024).

30. Платформы цифрового доверия для подтверждения персональных данных (ПЦД ПД) // URL: https://public.kryptonite.ru/PTsD_PD_presentation.pdf (дата обращения 17.09.2024).

31. Hans Jägers, Wendy Jansen and Wilchard Steenbakkers. Characteristics of Virtual Organizations. Proceedings of the VoNet - Workshop, April 27-28, 1998. Материалы семинара VoNet, 27-28 апреля 1998 г. Стр.65

32. АО «НПК «КРИПТОНИТ» // URL: https://public.kryptonite.ru/PTsD_PD_presentation.pdf (дата обращения 17.09.2024).

33. Сценарий использования инфраструктуры Цифрового профиля // URL: https://digital.gov.ru/ru/documents/7554/

34. Цифровой профиль гражданина // URL: https://agredator.ru/dp#func (дата обращения 17.09.2024).

35. ИРИ «Цифровая идентификация пользователей» // URL: https://ири.рф/news/tsifrovaya-identifikatsiya-polzovateley/ (дата обращения 17.09.2024).

36. КриптоАРМ. eIDAS: новые горизонты электронной идентификации // URL: https://cryptoarm.ru/news/eidas-new-horizon-for-the-electronic-identification/ (дата обращения 17.09.2024).

37. Мессенджеры: что это такое и зачем они нужны бизнесу // URL: https://getcompass.ru/blog/posts/chto-takoe-messendzher (дата обращения 17.09.2024).

38. Политика конфиденциальности WhatsApp // URL: https://www.whatsapp.com/legal/privacy-policy?lang=ru_RU (дата обращения 17.09.2024).

39. сервис «Профиль директ» // URL: https://agredator.ru/dp.

40. Ассоциация Больших Данных // URL: https://rubda.ru/assocziacziya/ob-assocziaczii/.

41. Яндекс.Телемос https://www.google.com/search?client=safari&rls=en&q=яндекс.Телемост&ie=UTF-8&oe=UTF-8.

42. Контур. Толк https://kontur.ru/talk.