

а/1
Дат 12.05.26
Под

«Дальневосточный филиал
Федерального государственного бюджетного образовательного учреждения
высшего образования
«Всероссийская академия внешней торговли
Министерства экономического развития Российской Федерации»

ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра юриспруденции

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

по направлению подготовки 40.03.01 «Юриспруденция»
(уровень бакалавриата)
направленность (профиль) «Гражданско-правовой»

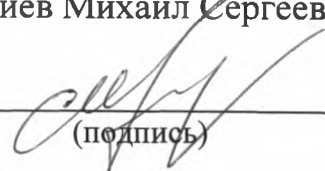
ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ

Научный руководитель:

Студент группы БЮР-2022

доцент кафедры юриспруденции,
канд. юрид. наук
Галиев Михаил Сергеевич

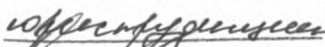
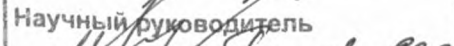
Тупицын Руслан Станиславович


(подпись)
«12» мая 2026 г.


(подпись)
«12» мая 2026 г.

Дата защиты _____

Оценка _____

ПРОВЕРЕНО	
НА УРОВЕНЬ ОРИГИНАЛЬНОСТИ	
Кафедра	
Научный руководитель	
(подпись)	Галиев М.С.
«12»	05 2026 г.

г. Петропавловск-Камчатский
2026 год

ОГЛАВЛЕНИЕ

Введение	3
Глава 1. Теоретико-методологический аспект персональных данных ...	10
1.1. Понятие, сущность и классификация персональных данных	10
1.2. Принципы и методы правового регулирования персональных данных ..	14
1.3. Концепция персональных данных в виртуальном пространстве.....	20
Глава 2. Правоприменительный аспект защиты персональных данных в правовом и виртуальном пространствах.....	26
2.1. Национальное законодательство в области защиты персональных данных и практика его применения.....	26
2.2. Международно-правовые стандарты и зарубежный опыт регулирования защиты персональных данных	34
2.3. Особенности правовой регламентации защиты персональных данных в виртуального пространства.....	41
Глава 3. Правовые дефекты и механизмы совершенствования защиты персональных данных в системе российского законодательства	49
3.1. Основные вызовы и угрозы для защиты персональных данных в виртуальном пространстве	49
3.2. Направления развития и гармонизация национального законодательства в области защиты персональных данных	57
Заключение.....	63
Список использованных источников	66

ВВЕДЕНИЕ

Актуальность выбранной темы обусловлена тем, что на сегодняшний день в условиях цифровизации и стремительного развития информационных технологий, наблюдается ситуация, при которой понимание человеком таких категорий как личное пространство и частная жизнь, серьезно подверглись изменениям и плавно перетекли в новое русло – цифровую среду.

Привычная для каждого человека деятельность, которая ранее проходила в реальной жизни, то есть на физическом уровне, все больше вытесняется цифровой средой, иначе эту цифровую среду, обозначают как «онлайн среда», именно в этом пространстве весомое число российского и мирового общества в целом проводит свою жизнь, поскольку доля ее внедрения в повседневную жизнь любого субъекта права возрастает и становится привычным инструментом для общественных отношений (приобретение товаров; поиск нужных услуг; взаимодействовать с различными ведомствами и организациями; контактировать с нашими друзьями и знакомыми в онлайн пространстве; осуществлять трудовую деятельности с применением цифровых технологий; проходить онлайн обучение и прочее).

На фоне такой роли цифрового пространства в жизни современного человека, неизбежным становится и накопление огромного количества личных данных пользователя этой сети. В мировую сеть попадают персональные данные граждан, которые постоянно собираются и обрабатываются разными ведомствами и организациями при оказании какой-либо услуги.

Из вышеперечисленного вытекает ряд вопросов связанных с регулированием персональных данных субъекта на законодательном уровне и их защищенности. Современная мировая тенденция направлена на цифровизацию, которая всячески упрощает жизнь человека, но каждая

инновационная тенденция носит как положительный, так и отрицательный характер. На сегодняшний день большое количество вопросов, связанных с персональными данными и способами их защиты остаются за рамками правового регулирования, что в свою очередь обуславливает возникновение целого ряда проблем в данной сфере.

Отсюда следует, что актуальность исследования вопросов правового регулирования и защиты персональных данных в виртуальном пространстве выражается в следующих аспектах:

1. Теоретико-правовой аспект выражается в осмыслении границ приватности, когда виртуальное пространства стирает грань между публичным и частным, а традиционная концепция «тайны частной жизни», гарантированная Конституцией, теряет свою силу. Также возникает необходимость теоретического переосмысления является ли цифровой профиль (аватар, цифровой двойник) просто набором сведений или же это стоит воспринимать, как продолжение личности, которое также нуждается в правовой защите.

2. Государственно-правовой аспект, в котором особое внимание уделяется цифровому суверенитету государства, так Президент Российской Федерации В.В. Путин отметил – «Россия – одна из трёх стран, которая обладает этим цифровым суверенитетом. Это Соединенные Штаты, Китайская Народная Республика и теперь Россия»¹. В данном аспекте видится важность контроля потока персональных данных, во избежание ситуации при которой с помощью этих данных будет дестабилизировано общество. В данном аспекте прослеживается юрисдикционный вызов для государства, ведь виртуальные пространства (например Meta, Telegram Google.) функционируют по собственным правилам, которые часто противоречат национальным законам. Складывается ситуация, при которой

¹ Путин заявил о достижении полного цифрового суверенитета России // ФедералПресс : [официальный сайт] 19 декабря 2025 г. URL: <https://fedpress.ru> (дата обращения: 13.03.2026).

государство вынуждено разрабатывать механизмы принуждения гигантов к соблюдению национального законодательства.

3. Гражданско-правовой аспект заключается в проблеме «информированного согласия» субъекта данных. Не редки случаи, когда в виртуальных пространствах пользователю часто навязывают и принуждают к соглашению на обработку его персональных данных, что ставит под сомнение добровольность и осознанность такого согласия. Рассматривая данный аспект стоит сказать и про имущественный характер данных, так как в современном мире персональные данные стали товаром (цифровым активом), где граждане нуждаются в защите от недобросовестных компаний, которые собирают данные без цели оказания услуги, а для перепродажи рекламодателям. Обосновывая данный аспект, стоит сказать про репутационный вред и цифровой след, заключающийся в распространении ложных или порочащих сведений в виртуальной среде, гражданин должен иметь эффективные механизмы для удаления недостоверной информации и компенсации морального вреда за утечку личных данных.

4. Уголовно-правовой аспект несет в себе тенденцию на увеличение числа киберугроз вызванных систематическими кибератаками и несанкционированным доступом к базам данных, где хранятся персональные данные субъектов. Порождаются новые составы преступлений, деяния, которые сложно, а иногда и невозможно квалифицировать по имеющимся статьям. Необходимо сказать, что преступления, совершенные в виртуальной среде, обладают высочайшей латентностью и уголовно-правовой аспект крайне актуален, поскольку требует совершенствования методов расследования, международного сотрудничества и фиксации цифровых следов как вещественных доказательств.

Таким образом, актуальность темы исследования многогранная, требующая всестороннего осмысления.

Объектом исследования выступают общественные отношения, связанные с правовым регулированием и защитой персональных данных в Российской Федерации.

Предметом выпускной квалификационной работы является российское законодательство и правовые нормы зарубежных стран, затрагивающие вопросы правовой природы института персональных данных, правоприменительная практика и доктринальные положения по теме исследования.

Целью данной работы является исследование теоретико-методологического аспекта персональных данных, анализ правоприменительных инструментов защиты персональных данных в правовом и виртуальном пространствах, выявление правовых дефектов и механизмов совершенствования защиты персональных данных в системе российского законодательства, а также формулирование выводов по теме исследования.

Для достижения поставленной цели необходимо решить следующие задачи:

- исследовать понятие, сущность и классификацию понятию «персональные данные»;
- рассмотреть принципы и методы правового регулирования персональных данных;
- раскрыть концепцию персональных данных в виртуальном пространстве;
- изучить российское законодательство и практику его применения в области защиты персональных данных;
- исследовать международно-правовые стандарты и зарубежный опыт, связанный с защитой персональных данных;
- проанализировать особенности правовой регламентации защиты персональных данных;

- выявить основные вызовы и угрозы для защиты персональных данных в виртуальном пространстве;
- сформировать и проанализировать основные направления и способы гармонизации национального законодательства в области защиты персональных данных.

Нормативная основа выпускной квалификационной работы представлена действующими нормативно-правовыми актами, а также актами применения права, а именно: Конституцией Российской Федерации, Федеральным законом «О персональных данных», Федеральным Законом «Об информации, информационных технологиях и о защите информации», Федеральным Законом «О безопасности критической информационной инфраструктуры Российской Федерации», а также различными постановлениями Правительства Российской Федерации и Указами Президента Российской Федерации в области защиты персональных данных.

Эмпирическую основу данного исследования составляет правоприменительная практика Арбитражного суда Республики Башкортостан, решение Красноярского Управление Федеральной антимонопольной службы России, а также дополняется деятельностью Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Теоретическую основу настоящего исследования составляют труды отечественных и зарубежных ученых, посвященные исследованию института персональных данных и его защиты. В рамках данного исследования изучалась специальная литература, научные статьи, материалы научных конференций и монографические работы. Объектом научного исследования в области правового регулирования и защиты персональных данных, отражены в трудах таких ученых и исследователей как Н.Н. Ковалева, Н.А. Жирнова, А.Г. Абрамова, Р.С. Тупицын, М.С. Галиев, Э.В. Талапина, Д.Ю. Южаков, А.Ю. Ястребова, А.И. Савельев.

Методологическая основа составляет комплексное применение общенаучных и частноправовых методов. К общенаучным методам относятся диалектический метод, метод системного анализа, методы анализа и синтеза, метод обобщения. Применимыми частно-правовыми методами будут являться нормативистский метод, сравнительный метод, правосоциологический метод, формально-юридический и другие методы.

Теоретическая и практическая значимость проведенного исследования заключается в том, что сформулированные в работе выводы могут быть использованы в будущих теоретических исследованиях, направленных на развитие категории «персональные данные» и защиты этой категории, в ходе выполнения курсовых работ или же выпускной квалификационной работы, материалом для рукописи научного характера.

Научная новизна выпускной квалификационной работы выражается в правопонимании и правоприменении защиты персональных данных в Российской Федерации, выявлении проблем и различных механизмов направленных на совершенствование защиты персональных данных в цифровом пространстве и в системе российского законодательства, а также в сформулированных выводах и положениях, которые обосновывают правовую природу персональных данных находящихся в виртуальном пространстве.

Апробация результатов научного исследования. Теоретические положения выпускной квалификационной работы нашли свое отражение в двух научных публикациях, в таких как:

1. Галиев М. С., Тупицын Р. С. Защита персональных данных: взгляд от теории к правоприменению / М. С. Галиев, Р. С. Тупицын // Юриспруденция: актуальные вопросы теории и практики: сборник статей XI Международной научно-практической конференции. – Пенза: МЦНС «Наука и Просвещение», 2026. – С. 10-16¹.

¹ Галиев М. С., Тупицын Р. С. Защита персональных данных: взгляд от теории к правоприменению. Пенза, 2026. С. 10-16.

2. Галиев М. С., Тупицын Р. С. Юридическая конструкция «Персональные данные»: теоретико-правовой и уголовно-правовой аспекты / М. С. Галиев, Р. С. Тупицын // Юриспруденция, закон и порядок: актуальны вопросы теории и практики: сборник статей XI Международной научно-практической конференции. – Пенза: МЦНС «Наука и Просвещение», 2026. – С. 12-17.¹

Структура данной выпускной квалификационной работы определяется целями и задачами исследования и состоит из введения, трех глав, объединяющих восемь параграфов, заключения и списка использованных источников.

¹ Галиев М. С., Тупицын Р. С. Юридическая конструкция «Персональные данные»: теоретико-правовой и уголовно-правовой аспекты. Пенза, 2026. С. 12-17.

ГЛАВА 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЙ АСПЕКТ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1. Понятие, сущность и классификация персональных данных

На сегодняшний день очень актуальным и окончательно не решенным остается вопрос, связанный с определением понятия «персональные данные», а также что представляет собой такая категория данные, то есть ее сущность. Сложившаяся ситуация обуславливается динамичностью таких данных, которые могут становятся персональными в зависимости от контекста их применения и обработки. Понятие «персональных данных» представляет собой сложную категорию в современном праве, поскольку оно должно охватывать не только прямые идентификаторы субъекта (например фамилия, имя, отчество, паспортные данные и так далее), но и косвенные сведения, позволяющие установить личность человека не напрямую, а косвенно. В качестве примера здесь можно привести возможность определить человека с помощью комбинации его IP-адреса, геолокации или биометрии.

Институт персональных данных регулируется Федеральным законом от 27.07.2006 года №152-ФЗ «О персональных данных» (Далее – ФЗ «О персональных данных»)¹. Первоначально законодатель закреплял, что к персональным данным можно относить любую информацию, относящуюся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилию, имя, отчество, год, месяц, дату и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессию, доходы,

¹ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025). URL: <http://www.pravo.gov.ru> (дата обращения: 24.06.2025).

другую информацию. Глядя на такое определение, можно понять, что огромный массив данных, который относится к субъекту персональных данных попросту не уточнен и не входит в текст закона, а действовавшая на тот момент редакция носит устаревший характер.

Так 25.07.2011 №261-ФЗ, были внесены изменения в ФЗ «О персональных данных», один из этих изменений стало новое определение понятия «персональные данные», а именно статья 3 признавала персональные данные как любую информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Такое определение, сформированное законодателем, на сегодняшний день охватывает достаточно большой объем персональных данных, хотя прямо и не указывает какие именно данные будут признаваться персональными, но дает понимание, что главным фактором признания данных, персональными, будет являться прямо или косвенное отношение информации к субъекту.

Если обращаться к зарубежным нормативным актам, то стоит обратить внимание на Конвенцию Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» (далее – конвенция № 108), которая была заключена 28.01.1981 в г. Страсбурге¹. Данная конвенция была ратифицирована Российской Федерацией 19 декабря 2005 года, еще до принятия ФЗ «О персональных данных» и ставила важную цель, а именно создание условий которые бы гарантировали уважение прав и основных свобод каждого физического лица, вне зависимости от его гражданства или местожительства при автоматизированной обработке его персональных данных. Упомянутая Конвенция Совета Европы давала свое определение персональным данным, а именно, они означают любую информацию об определенном или поддающемся определению физическом лице («субъект данных»).

¹ О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных : Федеральный закон от 19.12.2005 № 160-ФЗ. URL: <http://www.pravo.gov.ru> (дата обращения: 19.12.2005).

Проводя сравнение данных терминов, можно заметить их схожесть, данная идентичность вызвана стремлением законодателя, приведения ФЗ «О персональных данных» в соответствие с ранее упомянутой Конвенцией 1981 года. Глядя на это механизм возникновения, можно сделать вывод о том, что современное понятие «персональные данные» в отечественном законодательстве сложилось в ходе имплементации в отечественное законодательство некоторых положений зарубежного права, а именно из международной Конвенции 1981 года.

Обращая внимание на мнение ученых теоретиков относительно сущности персональных данных, можно сделать вывод, что сущность заключается в их фундаментальной природе как информации, неразрывно связанной с идентичностью конкретного физического лица, что делает такие данные объектом специального правового режима защиты. Информация будет признаваться персональной при наличии трех ключевых критериев: отношение у субъекту (содержание о человеке), возможность идентификации (прямая или косвенная) и контекст использования, ведущий к потенциальным последствиям для субъекта этих данных¹.

Рассматривая классификацию персональных данных, стоит понимать, что ФЗ «О персональных данных» а именно статьи 10-11 классифицируют персональные данные по степени «чувствительности» и специфике обработки, выделяя общие, специальные, биометрические и иные категории данных.

Первой и категорией данных будут являться – общие персональные данные, они представляют собой базовую информацию, позволяющую идентифицировать субъекта, но не затрагивающие особо чувствительные аспекты жизни человека. К такой категории данных можно отнести ФИО, дату и место рождения, адрес регистрации, контактные данные (телефон ил

¹ Минбалеев А. В. Проблемные вопросы понятия и сущности персональных данных. Челябинск, 2012. С. 4.

адрес электронной почты), сведения о работе, образовании и любые подобные данные.

Вторым видом являются специальные категории персональных данных. Они включают в себя данные связанные с вопросами расы, национальной принадлежности, политических взглядов, религиозной или философских убеждений, состоянием здоровья, интимной жизнь. Данные такого характера носят фактически закрытый характер и соответственно будут иметь особый режим обработки, а именно обработка данных связанная или содержащая в себе перечисленные факты – не допускает, но существуют исключения, содержащиеся в части 2 статьи 10 ФЗ «О персональных данных». Стоит отметить, что сохранение таких данных носит конституционный характер и обеспечение защиты такой информации носит крайне важный характер.

Третий вид – биометрические персональные данные. В эту группу данных входят все сведения человека касаясь его уникальных физиологических и биологических особенностей, которые в последующем позволяют установить личность человека. Так же этими сведениями пользуются лица, обрабатывающие те или иные данные человека, устанавливая личность человека по этим самым данным. Такая категория данных может обрабатываться только при наличии со стороны субъекта обработки этих данных волеизъявления, а именно письменного согласия. Законом так же предусмотрены исключения, согласия человека не будет требоваться в случае осуществления правосудия или при исполнении Российской Федерацией международного договора.

Здесь важно подчеркнуть, что в законе не указывается конкретный перечень данных, которые можно считать биометрическими, но его можно найти в Постановлении Правительства Российской Федерации от 30 июня 2018 г. № 772¹. Данное постановление определило виды биометрических персональных данных физического лица:

¹ Об определении состава сведений, размещаемых в единой биометрической системе, в том числе в ее региональных сегментах, а также о внесении изменений в некоторые акты Правительства Российской

1) Данные изображения человека, которые были получены с помощью фото или же видео устройств;

2) Данные голоса человека, записанные на звукозаписывающие устройства.

Четвертый вид, а именно, иные персональные данные включают в себя все остальные сведения, которые не вошли в предыдущие три категории персональных данных. К данному виду будет относиться информация, связанная с доходом, социальным статусом, стажем работы, данные о семье человека. Такие данные подлежат стандартной защите, но при определенных обстоятельствах могут переходить в специальные категории в зависимости от конкретной ситуации и контекста их использования.

Данная классификация, указанная в законе, является понятной и позволяет достаточно эффективно производить обработку персональных данных, оптимизировав ресурсы и минимизировать риск утечки данных при их обработке.

Подводя итог вышеперечисленному, можно сказать, с одной стороны о достаточной разработанности и законодательной регламентации института персональных данных, а с другой о возникающей проблеме актуальности этой законодательной регламентации, ведь в рамках постоянно развивающегося цифрового пространства возникают новые массивы и виды данных, которые не успевают охватываться нормами права.

1.2 Принципы и методы правового регулирования персональных данных

Правовое регулирование оборота, обработки и иных операций, связанных с персональными данными в современном цифровом обществе, представляет собой сложный, динамичный и многоуровневый правовой институт. Его формирование и развитие является прямым ответом на вызовы информационной эпохи, где личная информация превратилась в ключевой экономический актив и, одновременно, в объект, представляющий повышенную опасность для индивида.

Основу этого правового регулирования составляют фундаментальные принципы – устойчивые идеи и начала, определяющие его философию и цели, а практическую реализацию этих принципов обеспечивает система правовых методов, а именно приемов, способов и механизмов воздействия права на общественные отношения в этой сфере. Их комплексное взаимодействие создает правовое поле, предназначенное для достижения сложного баланса: защиты неприкосновенности частной жизни и базовых прав личности, с одной стороны, и обеспечения свободного потока информации, необходимого для экономического развития, инноваций и государственного управления – с другой.

Система принципов правового регулирования персональных данных носит универсальный характер, будучи закрепленной в ключевых международных актах, таких как Общий регламент по защите данных Европейского союза (GDPR), Конвенция Совета Европы 108+. Те или иные положения данных международных актов транслированы в национальные законодательства¹. Но все же основополагающий нормативно-правовой акт регулирующий этот вопрос, содержится во внутреннем законодательстве, в частности в ФЗ «О персональных данных». Принципы, которые содержатся в данных нормативно-правовых актах формируют фундамент, на котором базируются все конкретные нормы права, связанные с защитой, обработкой и

¹ Чурилов А. Ю. Принципы Общего регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации. Томск, 2019. С. 29-35.

иных манипуляций с персональными данными. Видится необходимым перечислить такие принципы и раскрыть их сущность.

Первый принцип, это принцип законности, справедливости и прозрачности. Законность в данном случае означает, что обработка персональных данных должна иметь четкое правовое основание: добровольное, информированное и конкретное согласие субъекта; необходимость для исполнения договора, стороной которого является субъект; соблюдение правовых обязанностей оператора; защиту интересов субъекта, которые ему гарантированы законом; выполнение задачи, осуществляемой в общественных интересах или осуществление оператором публичных полномочий; наличие законных интересов оператора, не противоречащих правам субъекта. Справедливость запрещает вводящие в заблуждение или противоправные действия, например, скрытый сбор данных. Прозрачность обязывает оператора доступным языком информировать субъекта о том, кто, зачем, на каком основании и как обрабатывает его данные, а также о правах субъекта.

Второй принцип – принцип ограничения целей (целевого использования). Он означает, что данные должны собираться для заранее определенных, явно выраженных и законных целей и не обрабатываться в дальнейшем способом, несовместимым с этими целями. Это препятствует «миссии дрейфа» – незаметному расширению использования данных за пределы тех ожиданий, которые были у человека при их предоставлении. Например, номер телефона, оставленный для доставки товара, не может быть использован для рассылки рекламных предложений без отдельного согласия¹.

Третьим принципом является, принцип минимизации данных. Его суть заключается в том, что должны обрабатываться только те данные, которые являются адекватными, релевантными и необходимыми для заявленных целей их обработки. Этот принцип направлен против избыточного сбора

¹ Абрамова А. Г. Современные проблемы осуществления защиты персональных данных в сети: основополагающие принципы защиты персональных данных. Ереван, 2020. С. 21-25.

информации «про запас» и требует от оператора критически оценивать объем запрашиваемых сведений. Примером, иллюстрирующим такие ситуации, здесь может выступить тот факт, что для онлайн-викторины не требуются данные паспорта, а для подписки на новости – дата рождения.

Четвертым по счету становится, принцип точности (достоверности) и актуальности. Оператор обязан принимать разумные меры для обеспечения того, что неточные или неактуальные данные либо незамедлительно удаляются, либо исправляются. Это право субъекта на возможность исправление данных, является его прямой гарантией против принятия решений на основе устаревшей или ошибочной информации, например, изменение в кредитной истории клиента банка.

Пятый, принцип ограничения хранения. Персональные данные должны храниться в форме, позволяющей идентификацию субъекта, не дольше, чем этого требуют цели их обработки. После достижения целей данные подлежат уничтожению или обезличиванию. Этот принцип призван противостоять созданию вечных, неконтролируемых «цифровых досье» на каждого субъекта персональных данных.

Шестой принцип, это принципы целостности и конфиденциальности (безопасности). Здесь важно понимать, что обработка должна осуществляться с обеспечением соответствующей безопасности, включая защиту от несанкционированной или незаконной обработки, случайной утраты, уничтожения или возможной кражи данных. Такая ситуация требует от операторов применения технических (шифрование, псевдонимизация) и организационных мер (политики доступа, своевременное обучение сотрудников) соразмерно рискам для прав и свобод субъектов, которые могут быть нарушены.

Окончательным седьмым, связующим все ранее перечисленные принципы, является принцип подотчетности. Он означает, что оператор не просто обязан соблюдать закон, но и должен быть способен продемонстрировать это соблюдение регулятору и субъектам данных. Это

реализуется через ведение документации по обработке, проведение оценок влияния на защиту данных, назначение ответственных лиц и реализацию принципа «защиты по умолчанию и по проектированию».

Обращая внимание на методы правового регулирования, с помощью которых данные принципы воплощаются в жизнь, представляют собой сочетание императивного (публично-правового) и диспозитивного (частноправового) воздействия, что свидетельствует о комплексной природе этого института.

Императивные (предписывающие) методы доминируют в сфере правового регулирования в сфере персональных данных, установления гарантий и обеспечения прав. Они проявляются в виде:

Установлении прямых законодательных запретов и обязывания: запрет на обработку специальных категорий данных (о здоровье, расе, убеждениях) без исключительных оснований; обязанность оператора получить предварительное согласие субъекта в ясной форме; обязанность уведомить надзорный орган (в РФ таким компетентным органом является Роскомнадзор) о начале обработки; обязанность сообщать о нарушениях безопасности данных субъектам и регулятору¹.

Создания института независимого надзора: наделение специальных органов, таких как Роскомнадзор, широкими контрольными, разрешительными и корректирующими полномочиями. Они проводят проверки, выдают предписания, налагают значительные административные штрафы, что является мощным превентивным инструментом.

Установленная юридическая ответственность: административная, гражданско-правовая и даже уголовная за нарушения законодательства в области персональных данных. Это метод правового принуждения, обеспечивающий неотвратимость последствия и наказания для нарушителей.

¹ Могунова М. М. Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг). Саратов, 2020. С. 137.

Диспозитивные методы в сфере правового регулирования персональных данных, предоставляют субъектам отношений, пространство для автономии и саморегулирования. К таим методам относятся:

Метод согласования воли (дозволения): ключевым здесь является институт согласия субъекта данных как самое распространенное правовое основание обработки. Закон определяет рамки (требования к форме и содержанию согласия на обработку персональных данных), но само решение предоставить или отозвать его остается за индивидом.

Реализация субъективных прав: право на доступ, исправление, удаление («право на забвение»), ограничение обработки, переносимость данных и возражение против обработки данных. Активное использование этих прав субъектами формирует обратную связь для операторов.

Гибкость в выборе мер исполнения: законодательство часто ставит цель (например, обеспечение безопасности данных), но при этом позволяет операторам самостоятельно выбирать конкретные технические и организационные средства для достижения этой цели, соразмерно характеру данных и рискам. Это стимулирует разработку инновационных решений в области процедуры обработки персональных данных.

Корпоративное саморегулирование и стандарты: возможность использования утвержденных правил поведения, сертификации механизмов защиты, а также стандартных корпоративных правил, для трансграничных передач тех, или иных данных, связанных с субъектом. Это метод делегирования части нормативной функции профессиональному сообществу.

Взаимодействие принципов и методов носит диалектический характер. Принципы наполняют методы правового регулирования смыслом и задают вектор их развития. Например, принцип подотчетности трансформирует императивный метод надзора, делая акцент не только на карательной, но и на консультационной функции регулятора. В свою очередь, конкретные методы делают принципы реализуемыми на практике. Принцип минимизации

данных из декларации превращается в конкретное требование методам формы сбора данных на сайте и оценивается регулятором в ходе проверок.

В современных условиях система принципов и методов сталкивается с новыми вызовами, такими как проблема больших данных (Big Data), искусственный интеллект, интернет вещей, где традиционные подходы к согласию и минимизации подвергаются нагрузке¹. Ответом становится развитие таких концепций, как «контекстуальная целостность» и «управление данными», а также адаптация методов – внедрение обязательных оценок воздействия для технологий с высоким уровнем риска и усиление роли принципа «защиты по проектированию». Таким образом, система принципов и методов правового регулирования персональных данных не является застывшей; она эволюционирует, стремясь сохранить свою фундаментальную цель – защиту достоинства и автономии личности, а также разработку действенных механизмов направленных на защиту персональных данных при любых манипуляциях с ними.

1.3. Концепция персональных данных в виртуальном пространстве

Наиболее рациональным и логически правильным видится рассмотрение концепции персональных данных в виртуальном пространстве, затрагивая ее эволюцию, природу и те современные вызовы, которые стоят перед концепцией на сегодняшнем этапе развития.

Так, концепция персональных данных в виртуальном пространстве представляет собой динамичную и сложную систему взглядов, определяющую природу, границы, правовой режим и социально-экономическую ценность информации о личности в цифровой среде. Данная

¹ Савельев А. И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data). М., 2015. С. 49.

концепция возникла на стыке юриспруденции, информационных технологий, социологии и этики, эволюционируя от простого понимания данных как формализованных сведений до признания их ключевым активом и цифровым двойником человека в сетевой реальности. Виртуальное пространство, понимаемое как глобальная, децентрализованная среда, образуемая компьютерными системами и сетями (в данном случае прежде всего, речь идет о сети Интернет), радикально трансформировало традиционные представления о приватности, конфиденциальности и самом субъекте данных¹.

Исторически понятие «персональные данные» уходит корнями в право на приватность, сформулированное в конце XIX века. Однако в доцифровую эпоху их сбор, хранение и обработка были пространственно и технически ограничены, что делало контроль со стороны субъекта более осуществимым. С наступлением в мире цифровой революции и становлением виртуального пространства как основной арены социальных, экономических и политических взаимодействий произошла фундаментальная трансформация. Сложилась ситуация, где данные перестали быть статичными записями в картотеках, они стали динамичными, машиночитаемыми, легко копируемыми, агрегируемыми и передаваемыми на глобальные расстояния мгновенно и за минимальную стоимость. Это породило ключевую особенность концепции в виртуальной среде: диссоциацию данных от физического носителя и их постоянную процессуальность. Данные непрерывно обрабатываются – собираются, анализируются, профилируются, продаются и используются для прогнозирования поведения, часто в реальном времени и без явного ведома человека.

Сущность концепции персональных данных в виртуальном пространстве сегодня раскрывается через несколько взаимосвязанных аспектов:

¹ Голоскоков Л. В. Сетевое законодательство: концепция развития. М., 2006. С. 11-15.

Во-первых, расширительное толкование объема понятия. Согласно современным правовым рамкам, таким как Общий регламент по защите данных (GDPR) Европейского союза, персональные данные – это любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу. В виртуальном пространстве к ним относятся не только явные идентификаторы (имя, паспортные данные, номер телефона), но и комплексные цифровые следы: IP-адреса, cookie-идентификаторы, геолокационные метки, история поисковых запросов и просмотров, лайки, репосты, метаданные коммуникаций (например, время отправки сообщения), биометрические данные с камер и датчиков, а также выводы, полученные в результате анализа (профили интересов, кредитные скоринги, предполагаемая сексуальная ориентация или политические взгляды)¹. Таким образом, в виртуальной среде даже анонимные на первый взгляд данные при их пересечении с другими массивами легко деанонимизируются, что стирает грань между персональными и не персональными данными.

Во-вторых, экономический аспект. В условиях цифровой экономики персональные данные превратились в «новую нефть» – сырье, которое добывается (собирается), перерабатывается (анализируется) и используется для создания рыночных продуктов и услуг. Бизнес-модели крупнейших интернет-компаний (социальных сетей, поисковых систем, маркетплейсов) построены на монетизации внимания пользователей, основанной на глубоком анализе их данных для таргетированной рекламы. Это порождает парадоксальную ситуацию: пользователь получает «бесплатные» услуги, но оплачивает их своими персональными данными и вниманием, что формирует отношения цифровой эксплуатации, где реальная стоимость данных для пользователя непрозрачна. Концепция предполагает признание данных не просто информацией, а формой цифрового труда и капитала.

¹ Регламент (ЕС) 2016/679 Европейского Парламента и Совета от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, и отмене Директивы 95/46/ЕС (Общий регламент по защите данных) // Официальный журнал Европейского союза. 2016. L 119. С. 1–88. URL: <https://eur-lex.europa.eu> (дата обращения: 20.03.2026).

В-третьих, правовой и регулятивный аспект. Ответом на вызовы виртуального пространства стало формирование строгих правовых режимов. Ядро современной концепции составляют ранее упомянутые принципы, закрепленные в ФЗ «О персональных данных», Общем регламенте по защите данных Европейского союза (GDPR), Конвенции Совета Европы 108+¹. Эти принципы включают в себя: законность, честность и прозрачность обработки; ограничение цели; минимизация данных; точность; ограничение хранения; целостность и конфиденциальность; а также подотчетность контролера данных. Ключевым нововведением здесь становится укрепление прав субъекта данных: право на доступ, исправление, удаление («право на забвение» в виртуальном пространстве), переносимость данных, а также право на ограничение и возражение против обработки персональных данных. Особое значение имеет требование, предусмотренное законом, а именно защиты данных по умолчанию и по их проектированию, которое обязывает разработчиков внедрять инструменты приватности на уровне архитектуры виртуальных сервисов и устройств.

В-четвертых, важную роль играет технологический аспект. Концепция персональных данных в виртуальном пространстве напрямую зависит от технологических трендов. Развитие больших данных (Big Data), искусственного интеллекта и цифровых товаров усугубляет проблемы. Алгоритмы искусственного интеллекта, обучающиеся на огромных массивах персональных данных, способны выявлять скрытые паттерны и принимать решения, влияющие на жизнь людей (от одобрения кредита до диагностики заболеваний), что порождает риски алгоритмической дискриминации и потери человеческого контроля. Интерне вещи стирают границу между онлайн и офлайн, превращая «умные» дома и города в постоянно собирающие данные системы, складывается ситуация, при которой все что нас окружает является инструментом по сбору наших данных в любой сфере.

¹ Конвенция о защите физических лиц при автоматизированной обработке персональных данных (пересмотренная) : (заключена в г. Страсбурге 10.10.2018) // Совет Европы. URL: <https://base.garant.ru> (дата обращения: 20.03.2026).

В ответ на сложившуюся ситуацию возникают и технологии, усиливающие приватность, – например, дифференциальная приватность, которая позволяет анализировать данные, полученные из огромного количества источников, минимизируя риски идентификации конкретного человека, или децентрализованные цифровые идентификаторы, дающие пользователям полный контроль над своими учетными данными.

В-пятых, социально-философский и этический аспект. Концепция персональных данных ставит фундаментальные вопросы о природе личности в цифровую эпоху. Цифровой профиль, составленный из разрозненных данных, зачастую становится нашей «виртуальной личностью», которой управляют корпорации и алгоритмы. Это ведет к квантификации и переработке человеческой идентичности, когда жизненный опыт, эмоции и отношения переводятся в измеримые и продаваемые метрики¹. Возникают этические дилеммы о согласии в условиях сложных и нечитаемых пользовательских соглашений, о праве на цифровое достоинство и автономию, о свободе от тотального наблюдения как со стороны корпораций, так и в некоторых случаях государств, использующих данные для социального контроля.

Говоря о проблематике концепции персональных данных в виртуальном пространстве, нельзя не упомянуть проблему трансграничности данных и конфликта юрисдикций. Суть проблемы заключается в том, что виртуальное пространство не признает государственных границ, в то время как правовое регулирование в области персональных данных остается национальным. Не редкими становятся ситуации, когда данные пользователя из одной страны могут физически храниться на серверах в другой и обрабатываться компанией, зарегистрированной в третьей стране. Отсюда возникает ряд вопросов какому правопорядку подчиняются такие данные? Применимо ли законодательство страны происхождения данных (принцип гражданства),

¹ Кочеткова Н. П. Цифровая реальность и приватность: вызовы и решения в современном коммуникативном пространстве. Ставрополь, 2024. С. 234-242.

страны расположения оператора (принцип территориальности) или страны пребывания субъекта данных? Это создает правовую неопределенность для компаний (операторов) и сложности в защите прав для граждан. Для решения таких проблем существуют разные юридические приемы, одним из которых является принцип «адекватности», который был предусмотрен в Общем регламенте по защите данных Европейского союза.

Таким образом, концепция персональных данных в виртуальном пространстве эволюционировала от узкого понимания идентифицирующей информации к комплексной модели цифровой личности как поведенческого и контекстуальной конструкции. Ядром данной концепции является конфликт между экономической ценностью персональных данных, фундаментальными, гарантированными Конституцией Российской Федерации правами человека на приватность и самоопределение, а также национальными интересами в сфере цифрового суверенитета¹. Что касается дальнейшего развития, то эта концепция будет определяться поиском баланса между инновациями, этикой, безопасностью и эффективным транснациональным регулированием, где субъект данных должен перестать быть пассивным объектом извлечения из него персональных данных и стать активным центром управления своей цифровой идентичности.

¹ Конституция Российской Федерации [принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020; с учетом поправок, внесенных законом Российской Федерации о поправке к Конституции Российской Федерации от 14 марта 2020 г. № 1-ФКЗ]. URL: <http://www.pravo.gov.ru> (дата обращения: 06.10.2022).

ГЛАВА 2. ПРАВОПРИМЕНИТЕЛЬНЫЕ АСПЕКТЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ПРАВОВОМ И ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ

2.1. Национальное законодательство в области защиты персональных данных и практика его применения

Защита персональных данных в Российской Федерации прошла сложный путь от фрагментарных норм в различных отраслях права к формированию специализированного законодательного массива, системообразующим элементом которого является ФЗ «О персональных данных». Необходимость создания такого правового института была обусловлена процессами цифровизации общества, возрастающими рисками несанкционированного использования информации о личности и обязательствами России по международным договорам, прежде всего Конвенции Совета Европы № 108 «О защите физических лиц при автоматизированной обработке персональных данных»¹.

До принятия Закона № 152-ФЗ отдельные аспекты защиты частной жизни и информации о личности регламентировались Конституцией РФ (ст. 23, 24), а также нормами Гражданского кодекса РФ (ст. 150-152), устанавливающими охрану частной жизни и компенсацию морального вреда, и Уголовного кодекса РФ (ст. 137, 138, 272). Однако данные нормы носили общий характер и не создавали целостного механизма регулирования обработки персональных данных в условиях развития информационных технологий.

¹ Ковалева Н. Н. Правовое регулирование бережного и устойчивого оборота данных. М., 2025. С. 141.

Принятие Федерального закона № 152-ФЗ в 2006 году стало отправной точкой для формирования отечественной модели защиты персональных данных. Как отмечает А.Н. Верещагин, «152-ФЗ изначально был компромиссом между либеральной моделью, основанной на уведомительном порядке и саморегулировании операторов, и жесткой административной моделью, предполагающей детальную регламентацию и разрешительный характер обработки»¹. Первоначальная редакция Закона базировалась на ранее упомянутых общепризнанных международных принципах, таких как законность и справедливость целей обработки, соответствие объема и характера обрабатываемых данных заявленным целям, обеспечение точности и достаточности данных, а также хранение в форме, позволяющей идентифицировать субъекта персональных данных не дольше, чем этого требуют цели обработки. Однако практика применения выявила значительное количество декларативных и противоречивых положений, что потребовало многочисленных изменений.

Качественно новый этап развития законодательства связан с внесением масштабных поправок в 2011 году, когда был принят Федеральный закон от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»».² Главной новацией здесь стало введение требования о локализации баз данных, содержащих персональные данные граждан РФ, на территории Российской Федерации, это отражено в п. 5 ст. 18 Закона. Данная норма, известная как «локализация персональных данных», обязывает оператора при сборе персональных данных, в том числе посредством и с использованием сети «Интернет», обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) и извлечение персональных данных граждан РФ с использованием баз данных, находящихся на территории России. Данное положение стало предметом

¹ Петрыкина Н. И. Правовое регулирование оборота персональных данных. Теория и практика. М., 2011. С. 124.

² О внесении изменений в Федеральный закон «О персональных данных» : Федеральный закон от 25.07.2011 № 261-ФЗ. URL: <http://www.pravo.gov.ru> (дата обращения 25.07.2011).

активных дискуссий в научной среде и на практике, а его правоприменение потребовало разъяснений со стороны регулятора – Роскомнадзора¹.

Современное состояние законодательства характеризуется его постоянной динамикой, направленной на адаптацию к новым технологическим вызовам, таким как big data, интернет вещей, использование искусственного интеллекта для профилирования. Ключевыми нормативными актами, дополняющими и конкретизирующими Закон № 152-ФЗ, являются:

1. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», в котором установлены уровни защищенности персональных данных².

2. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», данный приказ является ключевым нормативным документом, устанавливающим конкретные требования к защите персональных данных в информационных системах использующим персональные данные³.

3. Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных», суть этого документа заключается в том, что он дает операторам персональных данных практический инструментарий для выполнения требований закона № 152-ФЗ в части обезличивания данных, что позволяет легально использовать данные

¹ Обзор типовых нарушений обязательных требований законодательства Российской Федерации в области персональных данных по результатам проведенных в 2022 году контрольно-надзорных мероприятий. 2023. URL: <https://rkn.gov.ru> (дата обращения: 20.03.2026).

² Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства от 01.11.2012 № 1119. URL: <http://www.pravo.gov.ru> (дата обращения 01.11.2012).

³ Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020). URL: <http://pravo.gov.ru> (дата обращения: 14.05.2020).

без получения согласия субъекта для статистических, исследовательских и иных целей¹.

4. «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» (утв. Президентом РФ 03.02.2012 № 803), этот документ затрагивает вопросы защиты персональных данных в контексте кибербезопасности².

Подводя промежуточный итог, можно сказать, что национальное законодательство в области защиты персональных данных, представляет собой многоуровневую систему, ядром которой является Закон № 152-ФЗ, детализированный подзаконными актами и находящийся в тесной взаимосвязи с нормами смежных отраслей права: информационного, гражданского, административного и уголовного законодательства.

Немаловажным видится обратить внимание на правовой механизм защиты персональных данных в РФ, который строится на совокупности принципов, прав субъектов персональных данных, обязанностей операторов и системы государственного контроля и надзора. Согласно ст. 3 Закона № 152-ФЗ, персональные данные – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Такой массив данных имеет ряд законных основания для обработки, эти основания перечислены в ст. 6 Закона № 152-ФЗ. Наиболее распространенным является дача согласия субъекта персональных данных на обработку данных. Согласие должно быть конкретным, информированным и

¹ Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных данных, за исключением случаев, указанных в пункте 9-1 части 1 статьи 6 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» : приказ Роскомнадзора России от 19.06.2025 г. № 140. URL: <http://pravo.gov.ru> (дата обращения: 19.06.2025).

² Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации : указ Президента от 03.02.2012 № 803. URL: <http://pravo.gov.ru> (дата обращения: 03.02.2012).

сознательным, а в случаях, предусмотренных законом, – также письменным (включая электронную форму).

Иные основания обработки включают: обработку для исполнения договора, стороной которого является субъект; исполнение оператором возложенной законом обязанности; защиту жизненно важных интересов субъекта; осуществление правосудия; осуществление профессиональной деятельности журналиста либо законной деятельности СМИ.

Для наглядности, стоит обратиться к правоприменительной практике, связанной с действительностью согласия субъекта персональных данных. Здесь нужно понимать, что суды и компетентные органы строго подходят к оценке формы и содержания согласия. Например, в решении Красноярского УФАС России от 23.04.2025 по делу № 024/05/18-662/2025¹, здесь рассматривалось действие онлайн-платформы, где для получения займа пользователь должен был согласиться (посредством проставления галочки у соответствующего пункта) одновременно и на обработку персональных данных и на рекламные рассылки. Без проставления этой галочки невозможно было нажать кнопку «получить» для оказания ему соответствующей услуги. Компетентный орган пришел к выводу, что такая конструкция не дает реальной возможности выразить согласие/несогласие и нарушает требование о согласии и рекламе. В данном примере видится пряма отсылка к нарушению норм Закона №152-ФЗ, поскольку согласие не является свободным, конкретным и информационным.

Ранее было упомянуто, что при внесении изменений в ФЗ «О персональных данных», куда было внесено такое понятие, как «локализация персональных данных», данный термин несет в себе обязанность оператора при сборе персональных данных, в том числе посредством и с использованием сети «Интернет», обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) и извлечение

¹ Решение Красноярского УФАС России от 23 апреля 2025 по делу № 024/05/18-662/2025 // Официальный сайт Федеральной антимонопольной службы. URL: <https://www.tenderguru.ru/fas/1865461> (дата обращения: 16.03.2026).

персональных данных граждан с использованием баз данных, находящихся на территории России. Такой подход к хранению персональных данных субъектов порождает важность контроля за тем насколько безопасно и законно хранятся данные граждан на базе тех или иных организаций.

Нередкими становятся случаи утечки персональных данных, яркий пример такой утечки можно увидеть в судебной практике, связанной с раскрытие данных клиента банка. Для наглядности стоит взять решение Арбитражного суда Республики Башкортостан от 14.02.2024 года № А07-3409/023¹, где в данном судебном разбирательстве общество с ООО «Промтрансбанк» обратилось в Арбитражный суд с исковым заявлением к ООО «Экспресс лаб» о взыскании убытков в размере 60 000., расходов государственной пошлины в размере 2 400 рублей. Суть данного судебного разбирательства заключалась в том, что компания ООО «Экспресс лаб» по договору дорабатывала функционал сайта ООО «Промтрансбанк». В результате производимых работ на сайте произошла утечка персональных данных клиентов этого банка, которые направляли в банк заявки для получения кредита в онлайн формате. В частности сотрудник ООО «Экспресс лаб» опубликовал журнальный файл, содержащий в себе информацию о персональных данных пользователей, в открытом виде в сети интернет и при этом не использовал никаких систем защиты таких данных, что повлекло потерю данных заказчика, а явилось причиной утечки персональных данных лиц, подавших в банк заявку на получение кредита. Рассмотрев материалы дела, оценив относимость, допустимость, достоверность каждого доказательства в отдельности, а также достаточность и взаимную связь доказательств в их совокупности, руководствуясь статьями 110, 167-171 Арбитражного процессуального кодекса Российской Федерации, суд решил: исковые требования ООО «Промтрансбанк» удовлетворить и взыскать с ООО «Экспресс лаб» в пользу Промтрансбанка сумму в размере 60 000 рублей и

¹ Решение Арбитражного суда Республики Башкортостан от 14 февраля 2024 года по делу № А07-3409/023. URL: <https://sudact.ru> (дата обращения: 14.03.2026).

расходы по оплате государственной пошлины в размере 2 400 рублей. Данный пример из судебной практики показывает, насколько бывает уязвима система хранения персональных данных субъектов особенно при внесении в нее доработки и попытки улучшения защищенности данных клиентов.

Видится необходимо обратить внимание на правовой режим так называемых «белых списков», в контексте организаторов распространения информации. «Белый список» – это перечень интернет-ресурсов и сервисов, доступ к которым сохраняется даже при ограничениях связи по соображениям безопасности. Особого внимания заслуживает практика применения таких «белых списков» в отношении организаторов распространения различной информации в том числе и персональной. Так в соответствии с требованиями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», организаторы распространения информации обязаны хранить на территории Российской Федерации данные о фактах приема, передачи, доставки и обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей¹.

В октябре 2025 года ФСБ России направила ряду банков требования об установке комплекса технических средств для обеспечения функций оперативно-разыскных мероприятий, указав о распространение на них статуса организаторов распространения информации. С января 2026 года срок хранения соответствующих данных увеличен до трех лет.

В связи с этим особое значение приобретает механизм включения в региональные «белые списки» – перечни информационных ресурсов, доступ к которым не подлежит ограничению. Как указывается в информационных материалах, включение банковских сервисов в региональные «белые списки» теперь осуществляется по согласованию с профильными ведомствами, отвечающими за вопросы безопасности, и требует размещения системы

¹ Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2025). URL: <http://www.pravo.gov.ru> (дата обращения 29.12.2025).

хранения переписки¹. Примечательно, что приложения «Сбера» и ряда других банков не были включены в перечень именно из-за несоблюдения требований по установке таких серверов, что демонстрирует реальное применение данного механизма и показывает сложность некоторых организаций придерживаться правил по защите персональных данных клиентов.

Ключевой новеллой отечественного законодательства 2025 года в области защиты персональных данных и идентификации стало принятие Федерального закона от 24 июня 2025 г. № 156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации»². Данный закон предусматривает использование многофункционального сервиса обмена информацией (цифрового ID) для предоставления гражданами Российской Федерации сведений, содержащихся в документах, удостоверяющих личность, либо иных документах, выданных государственными органами. Часть 6 статьи 1 Закона закрепляет эквивалентность цифрового предоставления сведений физическому предъявлению документов, что создает основу для использования цифрового ID в различных правоотношениях. Наглядным примером использования данного закона можно отследить в области изменений отраслевого законодательства и в части проверки сведений, позволяющих установить возраст покупателя при покупке товара, предусматривающего возрастные ограничения.

Подводя итог, можно сказать, что практика применения национального законодательства в области защиты персональных данных находится в стадии активного формирования, она систематически меняется и дорабатывается. Несмотря на наличие развитой нормативной базы, сохраняются проблемы,

¹ О порядке формирования региональных «белых списков» информационных ресурсов : разъяснения Роскомнадзора от 20.01.2026 // Официальный сайт Роскомнадзора. URL: <https://rkn.gov.ru> (дата обращения: 13.03.2026).

² О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 24.06.2025 № 156-ФЗ. URL: <http://www.pravo.gov.ru> (дата обращения 24.05.2025).

связанные с пробелами в регулировании новых технологий и сложности, связанные с доказыванием нарушений и определении адекватного размера ответственности. Также наблюдаются сложности исполнения различными организациями законодательства регламентирующее требования по уровню сохранности личных данных клиентов. Что касается области правоприменения, то судебная практика и решения компетентных органов, играет важнейшую роль в конкретизации общих норм и выработке баланса интересов личности, бизнеса и государства в цифровую эпоху.

2.2. Международно-правовые стандарты и зарубежный опыт регулирования защиты персональных данных

Защита персональных данных в современную эпоху цифровой трансформации перестала быть сугубо национальной проблемой, трансформировавшись в одну из центральных тем международного публичного и частного права. Глобализация экономики, беспрецедентная трансграничная циркуляция информации, развитие технологий больших данных и искусственного интеллекта создали ситуацию, при которой данные о личности индивида практически мгновенно могут быть собраны, обработаны и использованы на территории множества государств, зачастую без его ведома и осознанного согласия. Эта объективная реальность обусловила необходимость выработки универсальных международно-правовых стандартов в области защиты персональных данных, призванных создать общее правовое поле, гарантировать базовый уровень прав личности вне зависимости от юрисдикции и содействовать свободному, но безопасному трансграничному потоку информации. Изучение этих стандартов и их имплементации в национальное законодательство различных государств и регионов представляет собой критически важную задачу для понимания

современных тенденций правового регулирования, выявления оптимальных моделей защиты и оценки их эффективности.

Формирование международных стандартов происходило под влиянием философско-правовых концепций приватности, развивавшихся на протяжении XX века, от понимания права на частную жизнь как «права быть оставленным в покое» до более комплексного подхода, рассматривающего контроль над личной информацией как неотъемлемый элемент человеческого достоинства и автономии личности в информационном обществе¹.

Первым системообразующим документом, заложившим концептуальные основы защиты персональных данных на международном уровне, стали Рекомендации Совета Организации экономического сотрудничества и развития (далее – Рекомендации ОЭСР) о защите частной жизни и трансграничных потоках персональных данных, принятые 23 сентября 1980 года². Несмотря на свой рекомендательный характер, данный акт оказал колоссальное влияние на последующее законодотворчество как на национальном, так и на международном уровне. Рекомендации ОЭСР сформулировали восемь базовых принципов защиты персональных данных, которые стали своего рода «золотым стандартом» в данной области. К ним относятся: 1) принцип ограничения сбора, предполагающий законные и честные способы получения данных с информированного согласия субъекта; 2) принцип качества данных, требующий, чтобы данные были актуальными, полными и адекватными целям их использования; 3) принцип определения цели, запрещающий использование данных в целях, несовместимых с первоначально заявленными; 4) принцип ограничения использования, вытекающий из предыдущего; 5) принципы безопасности и открытости, обязывающие оператора обеспечивать защиту данных и быть прозрачным в отношении политики и практики их обработки; 6) принцип участия

¹ Талапина Э. В. Оборот данных в государственном управлении: перспективы правового регулирования. М., 2020. С. 236.

² Рекомендации Совета ОЭСР о защите частной жизни и трансграничных потоках персональных данных (23 сентября 1980 г.) [официальный сайт ОЭСР]. URL: <https://www.sps-ib.ru> (дата обращения: 23.02.2026).

индивидуума, предоставляющий субъекту права на доступ к своим данным и возможность оспорить их точность; 7) принцип подотчетности, возлагающий на оператора ответственность за соблюдение указанных принципов.

Особое значение Рекомендации ОЭСР придавали вопросу трансграничной передачи данных, призывая государства-члены избегать создания неоправданных препятствий для таких потоков, кроме случаев, когда государство-реципиент не обеспечивает сопоставимого уровня защиты или когда передача затрагивает национальный суверенитет. Дальнейшим развитием подхода ОЭСР стала Ревизия Рекомендаций 2013 года, которая, сохранив базовые принципы, дополнила их положениями, отражающими вызовы нового времени. В новых рекомендациях был сделан акцент на управление рисками для приватности, усиление роли механизмов подотчетности, поощрение разработки и внедрения технологий, ориентированных на защиту приватности, а также развитие национальных программ повышения осведомленности о защите персональных данных.

Параллельно, в рамках Совета Европы, изначально ориентированного на защиту прав человека, формировался более жесткий, конвенционный подход. Краеугольным камнем европейской системы защиты данных стала Конвенция о защите физических лиц при автоматизированной обработке персональных данных, открытая для подписания 28 января 1981 года. Это первый и до недавнего времени единственный обязывающий международный договор в данной сфере. Конвенция № 108 закрепила многие принципы, созвучные Рекомендациям ОЭСР, но придала им обязательную юридическую силу для государств-участников. Она установила, что персональные данные должны: получаться и обрабатываться добросовестно и законно; храниться для точно определенных и законных целей и другие.

Для мониторинга соблюдения Конвенции был создан Консультативный комитет. Чтобы модернизировать устаревшие положения Конвенции в свете технологических вызовов, 10 октября 2018 года Комитет министров Совета Европы принял Протокол о поправках (СЕД № 223) к Конвенции № 108,

известный как Конвенция 108+. Модернизация значительно усилила уровень защиты: были введены новые принципы – «приватность по умолчанию»; расширен каталог «особых категорий данных», включив генетические и биометрические данные и даже данные о сексуальной ориентации. Стоит отметить, что Конвенция 108+ позиционируется как глобальный стандарт, открытый для присоединения государств, не входящих в Совет Европы.

Воплощением высочайшего на сегодняшний день уровня защиты персональных данных является законодательство Европейского Союза. Долгое время основным актом была Директива 95/46/ЕС на базе которой был сформирован очень интересный принцип «адекватности», однако ее фрагментарность и недостаточная гармонизация привели к разработке Общего регламента о защите данных (General Data Protection Regulation, GDPR), вступившего в силу 25 мая 2018 года. GDPR, будучи актом прямого действия на всей территории ЕС, заменил Директиву и создал единое, строгое правовое поле.

Его философия базируется на идее предоставления индивиду большего контроля над своими персональными данными и возложения на организации (контроллеров и обработчиков) всей полноты ответственности за их обработку. Ключевые новеллы GDPR включают в себя: 1) Экстерриториальное действие: Регламент применяется к обработке данных субъектов, находящихся в Европейском союзе, независимо от места нахождения и гражданства обработчика или контроллера, если их деятельность связана с предложением товаров/услуг или мониторингом поведения в ЕС. 2) Ужесточение условий согласия: согласие должно быть добровольным, конкретным, информированным и недвусмысленно выраженным (ясное утвердительное действие). Предусмотренные галочки о которых говорилось ранее более не допустимы. 3) Расширение прав субъектов данных: помимо традиционных прав доступа, исправления и удаления, введены право на переносимость данных, позволяющее получать данные в структурированном формате для передачи другому оператору, и

право на ограничение обработки. 4) Обязанность уведомления надзорного органа и субъектов данных о нарушениях защиты персональных данных в течение 72 часов с момента обнаружения. Стоит отметить и огромный размер административных штрафов, предусмотренных за нарушение положений GDPR. Размер санкции может достигать 20 миллионов евро или 4% от годового мирового оборота компании, в зависимости от того, что больше¹.

В GDPR также предусмотрена жесткая система трансграничной передачи данных, сформированный в принципе «адекватности». Суть данного принципа заключается в том, что он является правовым механизмом, позволяющим передавать персональные данные из стран ЕС в третьи страны или международные организации без получения дополнительных разрешений. Европейская Комиссия оценивает, обеспечивает ли правовая система конкретной третьей страны уровень защиты персональных данных, по сути эквивалентный уровню GDPR. Если да, то такой стране присваивается статус «адекватной», и передача данных на её территорию становится свободной.

GDPR стал эталоном, вызвав эффект «брюсселизации» – множество стран по всему миру начали реформировать свое законодательство, стремясь приблизить его к стандартам ЕС для обеспечения беспрепятственного трансграничного обмена данными с Европейским Союзом. В пример такой динамики, связанной со стремлением приведения законодательства к стандартам GDPR, можно привести Китай, который в последние годы резко ужесточил свое регулирование, приняв в 2021 году Закон КНР о защите персональных информации (Personal Information Protection Law, PIPL)², который, вобрал в себя многие элементы GDPR (принципы законности, минимальной необходимости, информированного согласия, права субъектов, обязанности операторов, ограничения трансграничной передачи). Китай

¹ Ястребова А. Ю. Право человека на защиту персональных данных: международно-правовые основы, примеры их имплементации в законодательстве государств, особенности регламентации в праве ЕС и национальном праве США. М., 2021. С. 93.

² О защите персональной информации : Закон от 01.11.2021 года // Personal Information Protection Law of the People's Republic of China. URL: <http://ru.china-embassy.gov.cn> (дата обращения: 01.11.2021).

успешно сочетает заимствованные положения с достаточно разработанным внутренним государственным законодательством, включающим требования о хранении персональных данных на территории Китая и предоставлении информации государственным органам по их запросу в целях национальной безопасности.

В рамках данного исследования стоит также обратить внимание на Азиатско-Тихоокеанский регион, модели которого носят своеобразный компромисс моделям европейской системы. Так, модель АТЭС, представленная Рамочными принципами конфиденциальности АТЭС (APEC Privacy Framework), пересмотренная в 2015 году, делает акцент на предотвращении вреда, гибкости и содействии трансграничному потоку данных через механизм Системы перекрестной конфиденциальности (Cross-Border Privacy Rules, CBPR)¹. Система CBPR является добровольной и сертификационной, суть данной системы заключается в том, что компании, прошедшие аудит на соответствие принципам АТЭС и получившие сертификат соответствия, могут беспрепятственно передавать данные внутри экономик-участниц системы. Для наглядности и комплексного сравнения двух систем передачи персональных данных, стоит систематизировать и представить в таблице 1.

Таблица 1.

**Сравнение Системы перекрестной конфиденциальности (CBPR) и
Общего регламента о защите данных (GDPR).**

Параметр	CBPR	GDPR
Подход	Гибкий, основанный на управлении рисками и подотчетности.	Жесткий, нормативный, основанный на правах субъекта.
Юридическая сила	Рамочный документ. Является добровольной системой сертификации для компаний.	Обязательный регламент прямого действия.
Основа передачи данных	Осуществляется через сертификацию компаний в системе CBPR и выполнение принципа подотчетности.	Осуществляется через принцип «адекватности» уровня защиты страны или специальные инструменты.
Роль согласия	Один из возможных законных оснований, но не единственный.	Играет центральную роль, должно быть явным, информированным,

¹ Азиатско-Тихоокеанское экономическое сотрудничество (АТЭС). Рамочные принципы защиты частной жизни АТЭС (2015) // Asia-Pacific Economic Cooperation : [официальный сайт АТЭС]. URL: <https://www.apec.org> (дата обращения: 19.02.2026).

	Акцент на цели использования.	конкретным.
Территориальное действие	Применяется к компаниям-участникам системы СВРР, независимо от их местонахождения.	Применяется ко всем, кто обрабатывает данные субъектов в ЕС, независимо от места нахождения компании.
Санкции	Не предусмотрены самими принципами. Нарушения ведут к исключению из системы СВРР и санкциям по национальному праву.	Штрафа крайне высокие (до 4% глобального оборота или 20 млн евро).

Источник информации: составлено автором по данным¹.

При сравнении Системы перекрестной конфиденциальности и Общем регламентом о защите данных, можно отметить, что оба нормативных акта являются драйверами глобального тренда на усиление защиты приватности, но отражают разные правовые традиции и подходы: европейский – основанный на правах человека, а разработанная в рамках Азиатско-Тихоокеанского экономического сотрудничества – основана на защите прав потребителей и предотвращении недобросовестной практики.

Таким образом, зарубежный мировой опыт показывает, что модель эффективного правового регулирования в XXI веке должно представлять собой баланс между универсальным соблюдением базовых принципов защиты приватности персональных данных при их трансграничной обработке и передаче (как фундаментальной ценности) и гибкостью, позволяющей учитывать национальные правовые традиции и экономические интересы той или иной страны. На основании вышеперечисленного можно предполагать, что будет наиболее эффективная система будет представлять собой гибрид, сочетающий жёсткие гарантии прав граждан по образцу GDPR с эффективными механизмами межправового взаимодействия и признания адекватности, как это заложено в Конвенции 108+.

¹ Свиридова Е. А. Региональные модели правового регулирования защиты данных в странах ЕС и АТЭС. М., 2024. С. 81-88.

2.3. Особенности правовой регламентации защиты персональных данных в виртуальном пространстве

В условиях современной цифровизации и информатизации правовое регулирование виртуального пространства выступает одним из актуальных направлений деятельности как государства и практиков, так и научных деятелей. В данном направлении особое внимание уделяется институту цифровых прав. Цифровое пространство обладает рядом специфических признаков (таких как анонимность, масштабность, высокая степень изменений и возможность влияния на данный процесс любого субъекта), которые не позволяют реализовывать «классические правовые» модели регулирования данной сферы. Цифровые права в таких условиях рассматриваются не только как универсальное средство регламентации, но и механизм реализации прав и свобод человека и гражданина в киберпространстве. Данное положение наглядно отражает европейский опыт регламентации цифрового пространства, который направлен не только на принятие и выделение исключительно цифровых прав, но и обеспечение реализации «классического» правового статуса человека и гражданина в виртуальном пространстве.

Повсеместное использование цифрового пространства, а в данном случае виртуального, поражает ряд нововведений и является некоторым вызовом для правовой сферы. Сложность рассматриваемого вопроса заключается в том, что киберпространство перерастает в новую реальность, однако правовая регламентация данной сферы только развивается. Все больший интерес вызывают «цифровые (виртуальные) права» человека, набор, положение, регламентация и признание которых выступают актуальным аспектом как для представителей научных кругов, так и для практических деятелей.

Первоначально стоит рассмотреть, такую категорию, как «цифровые права» на сегодняшний день они являются феноменом юридической сферы. Данное понятие имеет прямую взаимосвязь с виртуальным пространством, оно представляет собой базу взаимодействия и деятельности в киберреальности, которая устанавливает определенные правила поведения, нормы, возможные санкции за их нарушения и т.д. стоит отметить, что во многих научных работах можно встретить синонимическое представление понятий «цифровые права» и «интернет-права», так как в настоящее время цифровое пространство функционирования общества и государства представлено сетью Интернет. Естественно, что цифровое право в первую очередь рассматривается как некоторое средство регулирования Интернета. Отсюда вытекает и проблематика регулирования персональных данных в виртуальном пространстве, так как модель построения и функционирования виртуального пространства не позволяет регламентировать отношения в данной среде классическими, традиционными моделями правовой регламентации. В частности, это связано со сложностями функционирования и восприятия субъектов киберпространства – их невозможно контролировать с помощью правовых норм в классическом понимании, так как сама виртуальная среда предопределяет некоторую скрытность, анонимность существования и идентифицировать того или иного субъект (установить личность) в таких условиях довольно сложно¹.

Рассматривая особенности правовой регламентации защиты персональных данных в виртуальном пространстве, стоит выделить основные особенности этой сферы. Так первой особенностью будет являться – высокий уровень анонимности в виртуальном пространстве обоснован и вызван тем, что виртуальное пространство пользуется повышенным интересом среди криминальных и противоправных субъектов и структур в данной сфере. В качестве примера можно привести пример одной из таких

¹ Плотнокова Т. В. Феномен «цифровых прав» в контексте правового регулирования виртуального пространства. Тамбов, 2022. С. 392-400.

противоправных структур, а именно о функционировании теневого, криминального сектора Интернета – Darknet, данную площадку, действующую в виртуальном пространстве, можно рассматривать как теневой рынок в экономической сфере на которой можно приобрести не только в обыденном понимании запрещенные законом предметы и вещества, но и даже украденные персональные данные субъектов, а в некоторых случаях представляется возможным и «заказать кражу» данных о субъекте. Еще одной из причин высокого уровня анонимности пользователей становятся всяческие попытки совершения кибератак, мошенничества, экстремистская и террористическая деятельность, распространение запрещенных веществ и предметов, а также материалов – все это успешно функционирует и развивается в виртуальном пространстве.

Сложившаяся ситуация накладывает отпечаток на реализацию возможных моделей правового регулирования киберпространства: в частности, в рамках ограждения общества от негативных проявлений и влияний, которые оказывают на виртуальную среду, некоторые государства вынуждены реализовывать сложное, закрытое правовое регулирование данной сферы. В качестве примера можно привести Китай с закрытым Интернетом. Стоит отметить, что Российская Федерация на сегодняшний день также дает ответ на вызовы связанные с кибербезопасностью, сюда стоит включать и санкционное давление, а также стремление к технологической независимости, для этого в России был инициирован проект по созданию суперприложения «Мах», которое укрепило становление концепции цифрового суверенитета, понимаемая как способность государства осуществлять контроль над своей цифровой инфраструктурой, персональными данными субъектов и правилами функционирования самой цифровой среды.

Второй особенностью виртуального пространства выступает его масштабность. Данная сфера выходит далеко за рамки определенного государства, так как сеть Интернет имеет значение «всемирной паутины». В

связи с этим правовое регулирование киберпространства также выходит далеко за рамки традиционного национального законодательства. В данном направлении необходимо отметить важность применения международно-правового взаимодействия: так, международные нормы способны если не урегулировать взаимодействия в виртуальном пространстве во всем его объеме и многоаспектных проявлениях, то дать фундаментальные основы (основные идеи и принципы) правового положения личности, общества и государства в киберпространстве, на основе которых в дальнейшем возможно будет усовершенствовать и более четко регламентировать национальное законодательство.

Следующей особенностью виртуального пространства выступает высокий темп изменений и возможность влияния на данный процесс любого субъекта виртуального пространства посредством использования различных кодов (языков программирования). В отличие от реального (физического) мира изменения в киберпространстве зарождаются и реализуются молниеносно. Более того их направление и концепцию определяет не государство посредством политики, принятия документов стратегического планирования и т.д., а обычные пользователи. Неоднократно как зарубежом, так и в России поднимаются идеи свободного Интернета (концепция, связанная с отсутствием правовой регламентации со стороны государства), так как правовое регулирование данного феномена выходит далеко за рамки классического понимания правового надзора со стороны государственных органов и должностных лиц. Подробно анализируя современные взаимоотношения в сети Интернет, можно отметить, что их регламентация формируется стихийно на основе некоторых традиций, обычаев, совокупности технических и социальных норм. Если смотреть на этот феномен с другой стороны, то такая хаотичная динамика затрудняет для государства выработку стандартного набора прав и обязанностей в сфере киберпространства, а также дает возможность субъектам виртуального пространства диктовать свои условия и правила, которые зачастую

соотносятся с достижением личных интересов и целей таких субъектов, что в свою очередь может приводить к нарушению безопасности персональных данных субъекта¹.

Выделив особенности виртуального пространства и определив основные проблемы регламентации, которые обусловлены особенностями данного цифрового пространства, можно сделать вывод о необходимости последовательной законодательной работы, направленной на развитие цифровых прав и разработку новых концепций в области цифровых прав субъектов. Важно понимать, что новеллы применимые в цифровых правах должны делать акцент на право субъекта быть защищенным от посягательств на его персональные данные, которые находятся в этом самом виртуальном пространстве. Отсюда возникает необходимость рассмотреть и обратить внимание на отечественный опыт развития цифровых прав.

Оценивая современное положение российского законодательства, можно отметить, что цифровые права не только как самостоятельная отрасль, но даже легальная трактовка данного понятия как совокупности прав и обязанностей в сети Интернет в российском законодательстве отсутствует. В стратегических документах, например в Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы², можно встретить понятие «цифровая экономика», которая по своей природе связана с использованием цифровых технологий и реализацией в виртуальном пространстве, то есть находится в довольно тесной взаимосвязи с реализацией цифровых прав.

Законодателем в 2019 году был введен в российское законодательство институт цифрового права. Однако смысловая нагрузка данного института и понятия не имеет никакого отношения к идеям правового положения человека и личности в виртуальном пространстве и к формирующейся в международном праве концепции цифровых прав. Необходимость введения

¹ Степанов О. А. Правовое регулирование генезиса цифровой личности. Омск, 2022. С. 19-32.

² О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы : указ Президента от 09.05.2017 № 203. URL: <http://pravo.gov.ru> (дата обращения: 09.05.2017).

понятия «цифровые права» в российское гражданское право изначально объяснялась стремлением найти более соответствующий отечественным правовым традициям термин¹. В частности, в пояснительной записке к законопроекту № 424632-7, ставшему впоследствии Федеральным законом от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации», которым в ГК РФ и были введены цифровые права, специально подчеркивалось: «Проект вводит в гражданское законодательство базовое понятие «цифровые права» (вместо термина «токен», который изначально обозначает устройство для идентификации, а сейчас стал использоваться в IT-лексиконе для обозначения шифров, владение которыми дает в сети определенные возможности, предлагается отвечающее традициям российского права понятие «цифровое право»)². Сущность цифровых прав как новой юридической фикции близка к сущности ценной бумаги, поэтому под таким правом предлагается понимать совокупность электронных данных (цифровой код, обозначение), которая удостоверяет права на объекты гражданских прав (п. 1 новой статьи 141.1 ГК РФ). Исходя из вышеперечисленного складывается ситуация при которой цифровые права могут удостоверить лишь права на вещи, иное имущество, результаты работ, оказание услуг, исключительные права, но никак не делается акцент на защиту именно персональных данных субъектов в виртуальном пространстве.

Таким образом возникает тенденция, при которой вместо введения новых законов, которые бы фундаментально регламентировали защиту персональных данных в виртуальном пространстве, законодатель предусматривает ряд нововведений уже в действующее законодательство с

¹ Ибрагимова Ю. Э. Устранение пробелов гражданского законодательства путем внедрения категории «цифрового права». М., 2019. С. 49-53.

² Заключение Правового управления, подготовленное к рассмотрению законопроекта в первом чтении (по поручению Совета Государственной Думы (протокол от 09.04.2018 № 111, пункт 66) : [интернет портал «Системы обеспечения законодательной деятельности»]. URL: <https://sozd.duma.gov.ru> (дата обращения: 14.02.2026).

целью защитить оставшиеся за рамками законодательного контроля персональные данные субъекта, которые находятся в виртуальном пространстве. В качестве примера составляющую данную тенденцию стоит привести Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ» (далее – закон о КИИ)¹. Этот закон задает общие рамки информационной безопасности в стране. Закон о КИИ обязывает операторов значимых объектов (к которым могут относиться и крупные базы персональных данных) соблюдать дополнительные требования по защите от компьютерных атак. Немаловажную роль в области регламентации и защиты персональных данных субъекта в виртуальном пространстве играют Федеральные законы № 374-ФЗ и 375-ФЗ от 06.07.2016, известные как «Пакет Яровой». Они внесли изменения в ряд законодательных актов, введя требование о локализации баз данных российских граждан на территории РФ (ст. 18 152-ФЗ). Это означает, что при сборе персональных данных граждан России, в том числе в виртуальном пространстве, оператор обязан обеспечить их запись, систематизацию, накопление, хранение и уточнение с использованием баз данных, находящихся в Российской Федерации.

Подводя итог всему вышеперечисленному, можно говорить о том, что виртуальное пространство является крайне сложной, динамичной, и в некой степени даже неподвластной системой со слабым уровнем правового контроля. На фоне этого видится острая необходимость более детальной и четкой регламентации киберпространства и как следствие принятие и реализация цифровых прав предопределены современными условиям и активной цифровизацией и информатизацией. Как было выявлено, цифровые права в настоящее время выступают актуальными регуляторами и не подчиняются классическим законам правового регулирования. Основное предназначение данной зарождающейся отрасли – это регламентация

¹ О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 07.04.2025). URL: <http://www.pravo.gov.ru> (дата обращения 07.04.2025).

поведения в виртуальном (цифровом) пространстве, которая также должна быть направлена на сохранение личных данных субъектов. В российских реалиях сформировалась неоднозначная и прагматичная ситуация: с одной стороны, в научных кругах доминирует положение противников выделения цифровых прав в качестве самостоятельной отрасли права, при этом законодатель интегрирует институт цифровых прав в гражданское законодательство как совокупность электронных данных, которые удостоверяют права на объекты гражданских прав и выносит защиту личных данных пользователей на второй план. Такая ситуация осложняет и без того непростое отношение в области регламентации и защиты персональных данных субъекта в виртуальном пространстве.

ГЛАВА 3. ПРАВОВЫЕ ДЕФЕКТЫ И МЕХАНИЗМЫ СОВЕРШЕНСТВОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СИСТЕМЕ РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА

3.1. Основные вызовы и угрозы для защиты персональных данных в виртуальном пространстве

Динамичное развитие информационно-коммуникационных технологий, пронизывающих все сферы общественной жизни, привело к формированию принципиально новой цифровой экосистемы. В её центре находится персональная информация, превратившаяся в ключевой экономический актив и объект повышенного внимания со стороны как коммерческих структур, так и злоумышленников. Виртуальное пространство, характеризующееся анонимностью, трансграничностью и высокой скоростью обработки информации, порождает уникальные по своей природе вызовы и угрозы для конфиденциальности и безопасности персональных данных в виртуальном пространстве. Эти угрозы носят комплексный характер, находясь на стыке технологических инноваций, правовой неопределённости и социально-поведенческих факторов.

Что касается законодательства, то оно по своей природе и на фоне крайне динамичного развития цифрового пространства, кажется консервативным и зачастую просто не успевает адекватно реагировать на стремительную эволюцию цифровых рисков, что создаёт значительные пробелы в защите фундаментального права на неприкосновенность частной жизни. Основная проблема заключается в фундаментальном противоречии между глобальной, децентрализованной архитектурой интернета и традиционными территориально привязанными правовыми режимами, что

существенно осложняет как предупреждение, так и преследование нарушений в данной сфере.

Ключевым технологическим вызовом, переопределяющим саму концепцию приватности, является феномен больших данных и последующий технологический анализ этих больших данных. Современные методы агрегации и обработки огромных массивов персональной информации, не смотря на обезличенность информации, дает возможность с высокой точностью идентифицировать субъекта данных, выявлять их скрытые предпочтения, модели поведения и даже предсказывать будущие действия. Процессы профилирования и принятия автоматизированных решений, основанных на алгоритмической обработке персональных данных, ставят под вопрос базовые принципы осознанного согласия и целевого использования информации.

Рассматривая уголовно-правовой аспект, основным и самым масштабным комплексом угроз цифрового пространства в данной сфере, на сегодняшний день выступают, давно нашумевшие, киберугрозы в виде целенаправленных атак злоумышленников. Данный вид атаки несет в себе целый список способов противоправного заочелучения данных субъекта. К данному комплексу атак можно отнести: фишинг и социальную инженерию, эксплуатирующие человеческий фактор; вредоносное программное обеспечение, которое блокирует доступ к данным человека и в последующем выставляет требование выкупа для возвращения заблокированных данных; очень распространенные и находящиеся на слуху DDoS-атаки, парализующие целые сервисы содержащие в себе огромное количество личной информации о его пользователях; и в последнюю очередь стоит отметить целевые взломы информационных систем операторов.

Последствия вышеперечисленных инцидентов носят катастрофический характер, приводя к массовым утечкам персональной информации, финансовым потерям и репутационному ущербу для организаций и операторов обработки данных. Правовой аспект решения

данной проблематики заключается в необходимости установления жёстких, но адекватных требований к технической и организационной защите персональных данных, обязательств по уведомлению регуляторов и субъектов о произошедших нарушениях, а также в эффективном уголовном преследовании киберпреступников, которые зачастую действуют из-за рубежа, что опять же сильно осложняет борьбу с преступностью в данной сфере. Стоит также указать на недостаточный уровень кибергигиены, которая заключается в соблюдении совокупности правил, направленных на обеспечение безопасного поведения в цифровом пространстве как у организаций, так и у рядовых пользователей, данный аспект остаётся критически слабым звеном в этой цепи.

Еще одним из вызовов стоящим перед защитой персональных данных состоит в том, что субъект данных зачастую не в состоянии осознать все возможные последствия предоставления своих данных, которые, будучи собраны одной организацией для одной цели, могут быть многократно перепроданы и использованы в совершенно неожиданных контекстах, формируя цифровой досье индивида. В перспективе это может привести к тому, что хакеры взламывают персональную страницу в социальных сетях, зачастую под взлом попадают страницы в социальных сетях и электронный почтовый ящик¹. Стоит отметить, что такого рода преступлениям в большей степени подвергаются все группы молодежи вне зависимости от социальных, экономических или демографических факторов. Как результат, преступники получают доступ к такой конфиденциальной информации, как персональные данные человека, личная переписка, фотографии, личные документы и т.п. Данная тенденция делает молодых людей более уязвимыми не только перед мошенниками ввиду их более активной вовлеченности в виртуальное пространство.

¹ Умаров Б. Киберпреступления с использованием персональных данных и электронных платежных систем: вызовы, угрозы и пути предупреждения. СПб., 2025. С. 50-56.

Последствия вышеперечисленных инцидентов носят катастрофический характер, приводя к массовым утечкам персональной информации, финансовым потерям и репутационному ущербу для организаций и операторов обработки данных. Правовой аспект решения данной проблематики заключается в необходимости установления жёстких, но адекватных требований к технической и организационной защите персональных данных, обязательств по уведомлению регуляторов и субъектов о произошедших нарушениях. С позиции уголовного права, деяния, описанные выше, подпадают под признаки целого ряда составов преступлений, предусмотренных главой 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации»¹. Квалификация содеянного зависит от способа и последствий: неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных программ (ст. 273 УК РФ) или нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и телекоммуникационных сетей (ст. 274 УК РФ). Особую общественную опасность представляет вымогательство выкупа за разблокировку данных, которое может дополнительно квалифицироваться по ст. 163 УК РФ (вымогательство) или ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации).

Однако эффективное уголовное преследование киберпреступников осложняется целым рядом факторов – высокая латентность данных преступлений, трансграничный характер атак (злоумышленники зачастую действуют из-за рубежа, используя VPN и анонимайзеры) и необходимость привлечения узких специалистов для проведения компьютерно-технических экспертиз создают серьезные препятствия для правоохранительных органов. Это порождает проблему неотвратимости наказания, которая является ключевой для общей превенции данных деяний. Стоит также указать на

¹ Уголовный кодекс Российской Федерации : Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 20.02.2026). URL: <http://www.pravo.gov.ru> (дата обращения 20.02.2026).

недостаточный уровень кибергигиены, которая заключается в соблюдении совокупности правил, направленных на обеспечение безопасного поведения в цифровом пространстве как у организаций, так и у рядовых пользователей.

Правовой вызов здесь заключается в обеспечении секретности и конфиденциальности таких сложных процессов для пользователя и установлении юридической ответственности за решения, принятые исключительно алгоритмами, особенно если они приводят к утечке персональных данных или иному нарушению прав человека. Глобальность виртуального пространства порождает, пожалуй, наиболее сложный юридический вызов – проблему трансграничных потоков данных. Персональные данные пользователей из одной страны могут храниться на серверах в другой и обрабатываться компанией, зарегистрированной в третьей. Это создаёт конфликт юрисдикций и значительные сложности в применении национального законодательства. В частности, ФЗ «О персональных данных», содержит в себе требование о локализации баз данных на территории Российской Федерации для граждан РФ, что является одним из правовых ответов на этот вызов. Однако такой ответ порождает новые вопросы, связанные с реализацией таких права, как право на забвение, право на портативность данных и последующее обеспечение их доступности для иностранных сервисов, действующих на базе виртуального пространства¹.

Вышеупомянутая ситуация, порождает противоречия между различными правовыми моделями – жёсткой европейской моделью, представленной системой GDPR; ситуативной американской моделью и императивной российской моделью, неизбежно создают барьеры для международных организаций, международного бизнеса и вносят неопределённость для пользователей, чьи личные данные пересекают границы страны.

¹ Забокрицкая Л. Д. Информационная культура современной молодежи: угрозы и вызовы виртуального социального пространства. Пермь, 2017. С. 114-123.

Широкое распространение сети Интернет и большого количества используемых человеком устройств формирует новый вызов и масштабную угрозу — создание постоянного, всепроникающего фона сбора сверхчувствительных биометрических и поведенческих данных. Умные дома, фитнес-браслеты, медицинские датчики собирают информацию в круглосуточном режиме, часто без явного и осознанного взаимодействия с пользователем. Угрозы здесь носят двойственный характер: это и риски несанкционированного доступа к этим данным (например, к информации о состоянии здоровья или распорядке дня человека), и риски их использования для манипулятивного воздействия. С гражданско-правовой точки зрения, утечка такой информации или её использование не по назначению влечет за собой ответственность оператора (владельца устройства или платформы). Возникают основания для деликтной ответственности — обязанности возместить причиненный моральный вред и убытки, поскольку сбор и обработка данных без надлежащего правового основания нарушают нематериальные блага и личные неимущественные права граждан.

Ряд мошенников благодаря считыванию биометрических и поведенческих данных, создают и определяют психологический портрет человека. Такой подход позволяет выявить какие у человека есть «интересы», узнать его предпочтения в том какой товар он хочет приобрести или какой услугой желает воспользоваться, этот набор факторов дает возможность мошенникам напрямую или через посредников похищать денежные средства. Часть преступников впоследствии также склоняют людей к противоправным действиям различной направленности. В контексте гражданского права это создает прецеденты для привлечения к ответственности не только прямых исполнителей, но и владельцев цифровых платформ (как владельцев источников повышенной опасности или как лиц, обязанных обеспечивать безопасность услуг), если будет доказано, что архитектура сервиса или недостаточная защита данных способствовали такому склонению и причинению вреда третьим лицам.

Одновременно с этим можно констатировать, что помимо угроз, связанных с возможным информационным противостоянием, существуют и достаточно важные внутренние угрозы, вызванные широкими возможностями применения современных информационно-коммуникационных технологий для манипулирования общественным сознанием в рамках политического управления со стороны государства и соответствующих политических элит¹.

Юридическая сложность усугубляется тем, что многие вышеперечисленные устройства не имеют адекватных интерфейсов для предоставления понятных уведомлений о конфиденциальности и получения действительного согласия субъекта, а их безопасность зачастую оставляет желать лучшего, делая их лёгкой мишенью для кибератак. Кроме того, возникает вопрос о правовом режиме данных, генерируемых не человеком, а его взаимодействием с устройством, и о разграничении ответственности между производителем устройства, разработчиком программного обеспечения и оператором платформы на базе которой происходит использование.

Дополнительный пласт проблем связан с деятельностью государства в цифровой среде. С одной стороны, государство выступает гарантом защиты прав граждан, устанавливая «правила игры» и контролируя их соблюдение через органы надзора, такие как Роскомнадзор и Прокуратура. С другой стороны, есть обоснованная необходимость обеспечения национальной безопасности, борьбы с кибер-терроризмом и преступностью, которая ведёт к внедрению систем тотального наблюдения и контроля, масштабного сбора и анализа данных граждан государственными органами. Это создаёт риск возникновения «большого брата» и размывания приватности в интересах безопасности. Правовой баланс между этими конкурирующими ценностями крайне хрупок. Законодательные инициативы, обязывающие организаций

¹ Володенков С. В. Новые формы политического управления в киберпространстве XXI века: вызовы и угрозы. Саратов, 2011. С. 78–85.

предоставлять силовым структурам доступ к зашифрованным данным или хранить определённую информацию о действиях пользователей, часто вызывают критику со стороны правозащитников и бизнес-сообщества как избыточные и создающие «лазейки» для злоупотреблений.

Таким образом, можно сказать, что основные угрозы и вызовы для защиты персональных данных в виртуальном пространстве носят системный и взаимосвязанный характер, проистекая из самой природы цифровых технологий. Технологические риски, связанные с большими данными и кибератаками, усугубляются правовой неопределённостью в сфере трансграничных потоков, автоматизированных решений и юрисдикционной ответственности. Действующее законодательство, как российское, так и зарубежное, хотя и развивается в направлении усиления защиты данных, зачастую страдает реактивностью, фрагментарностью и сложностью практической реализации. Для формирования адекватного ответа на эти вызовы необходим переход от фрагментарного регулирования к созданию целостной экосистемы цифрового регулирования. Это предполагает не только ужесточение санкций и технических требований, но и развитие цифровой грамотности населения, введения принципа при котором защита данных включается на ранних стадиях разработки систем, продуктов и услуг на уровне разработки новых технологий. Также важно уделять пристальное внимание и направлять вектор в сторону международного сотрудничества, которое способствовало бы выработке совместимых правовых стандартов и механизмов управления. Можно констатировать, что будущее защиты приватности в виртуальном пространстве будет зависеть от способности правовой системы к гибкой адаптации, сохранению баланса между инновациями, безопасностью и фундаментальными правами человека в области защиты его личных данных.

3.2. Направления развития и гармонизация национального законодательства в области защиты персональных данных

Сфера защиты персональных данных в Российской Федерации переживает период глубокой и динамичной трансформации, движимой стремительной цифровизацией общества, возникновением новых технологических вызовов и необходимостью интеграции в глобальное правовое пространство. Современный этап развития национального законодательства характеризуется не столько созданием принципиально новой правовой базы, сколько ее тонкой настройкой, гармонизацией с международными стандартами и опережающим регулированием возникающих цифровых реалий. Российская Федерация, как активный участник международного диалога и обладатель одной из самых развитых цифровых экосистем, стоит перед сложной двуединой задачей: с одной стороны, необходимо развивать национальное законодательство, отвечающее внутренним вызовам и целям технологического развития, с другой – гармонизировать его с международными стандартами для обеспечения беспрепятственного трансграничного потока данных и интеграции в мировую экономику.

Гармонизация российского законодательства в области защиты персональных данных неразрывно связано с международными нормами, в первую очередь с Общим регламентом по защите данных GDPR и представляет собой сложный и многогранный процесс. С одной стороны, наблюдается очевидное сближение базовых принципов: законность, справедливость и прозрачность обработки; ограничение обработки заранее определенными целями; минимизация данных; обеспечение точности и актуальности; ограничение хранения. Российский закон, как и GDPR, закрепляет необходимость получения согласия субъекта на обработку его персональных данных, за исключением ряда установленных случаев. Однако

глубинная гармонизация сталкивается с существенными системными различиями. GDPR построен на идее защиты фундаментального права на приватность как права человека, в то время как российский подход традиционно имеет более административно-правовой, организационно-технический характер, где акцент смещен на обеспечение безопасности данных как информации ограниченного доступа. Это различие порождает и различные механизмы контроля: если в Европейском союзе ключевую роль играют независимые надзорные органы (такие как CNIL во Франции или ICO в Великобритании) и мощные механизмы гражданского общества, то в России регуляторная функция сосредоточена в руках государственного органа — Роскомнадзора, а роль судебной защиты прав субъектов находится на этапе активного развития¹.

Тем не менее, ряд нововведений свидетельствует о движении обеих систем навстречу. Это расширение прав субъектов, включая уточненные процедуры отзыва согласия, усиление требований к прозрачности политик операторов, активное развитие института уполномоченных лиц по защите прав субъектов персональных данных, что является аналогом европейского Data Protection Officer (DPO). Важным шагом в гармонизации стало также законодательное закрепление новых понятий, таких как «биометрические персональные данные» и «генетические персональные данные», важно отметить, что последний термин был введен сравнительно недавно в рамках поправок, Федеральным законом от 30.12.2020 № 519-ФЗ «О внесении изменений в ФЗ «О персональных данных», специальный правовой режим этих многогранных терминов, во многом коррелирует с повышенным уровнем защиты специальных категорий данных по системе GDPR.

Наиболее ярким направлением развития законодательства в области защиты персональных данных, стало создание национального мессенджера Max. Ввиду санкционного давления и слабой охраны личных данных

¹ Унижаев Н. В. Особенности моделирования угроз безопасности персональных данных для обеспечения достаточного уровня защищенности. М., 2022. С. 50-56.

граждан, выявилась острая необходимость в создании собственной платформы, которая бы соответствовала бы всем необходимым стандартам в области защиты данных ее пользователей. Правовым основанием создания данного мессенджера стал Федеральный закон от 24.06.2025 №156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации», в котором подчеркивалась необходимость разработки национальной платформы для обмена информацией и безопасной коммуникации граждан. Федеральный закон №156-ФЗ от 24 июня 2025 года утвердил создание в России национального мессенджера как части стратегии цифрового суверенитета. Согласно закону, национальный мессенджер – это программное приложение, которое позволяет не только обмениваться сообщениями и совершать звонки, но и заключать сделки, подписывать документы, получать доступ к государственным и другим сервисам.

Мессенджер Мах был разработан дочерней структурой VK – ООО «Коммуникационная платформа». Он стал основным претендентом на роль национального мессенджера и уже в июне 2025 года Мах был включён в Единый реестр российских программ для электронных вычислительных машин и баз данных. Распоряжение Правительства РФ от 12 июля 2025 года №1880-р определило ООО «Коммуникационная платформа» как организацию, которая обеспечивает создание и функционирование многофункционального сервиса обмена информацией на базе Мах. Это решение было принято в соответствии с пунктом 2 Федерального закона №156-ФЗ.

С 1 сентября 2025 года данное национальное приложение стало обязательным для предварительной установки на все смартфоны и планшеты, продаваемые в России, такое решение вызвано тем, что Мах детализирует и конкретизирует требования Закона № 152-ФЗ, особенно в части обеспечения безопасности персональных данных. Введение такого механизма преследует несколько стратегических целей:

1. Повышение фактической защищенности персональных данных за счет введения конкретных, измеримых требований к операторам;
2. Унификация подходов к оценке защищенности и проведению контрольных мероприятий;
3. Создание технологически нейтральной, но содержательной рамки, применимой к любым способам и средствам обработки;
4. Сближение с международными стандартами (ISO/IEC 27001, GDPR) в части подходов к управлению рисками и подотчетности.

Важно сказать, что приложение Мах систематизирует категории персональных данных, выделяя, помимо общих, специальных, биометрических и общедоступных, также иные категории, обработка которых представляет повышенный риск для прав и свобод субъектов (например, данные о здоровье в ограниченном объеме, данные о финансовом положении). Для каждой категории могут устанавливаться особые организационные и технические меры защиты. Это позволяет перейти от универсальных требований к риск-ориентированной модели, где строгость мер соответствует возможному ущербу¹.

Национальный мессенджер содержит в себе ужесточение регуляторных требований к трансграничной передаче, закрепляет и конкретизирует положения закона о трансграничной передаче данных. Здесь акцент делается на обязательной оценке рисков перед осуществлением трансграничной передачи и документировании ее результатов. Оператор должен не просто формально убедиться, что иностранное государство обеспечивает адекватную защиту, но и проанализировать, какие конкретные риски для субъектов данных возникают при передаче, и принять дополнительные меры для их минимизации. Такая система напрямую коррелирует с принципом «подотчетности» в системе GDPR.

¹ Маклачкова В. В. Основные риски персональных данных в мультиоблачных информационных средах. М., 2025. С. 169-181.

Если рассматривать развитие законодательства в области защиты от кибератак, то ключевым инструментом обеспечения национальной кибербезопасности в Российской Федерации будет являться Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Это государственная система создана в соответствии с указом президента РФ от 15 января 2013 N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Современные кибератаки, как уже ранее отмечалось, носят преимущественно трансграничный и скрытый характер. ГосСОПКА, аккумулируя информацию от тысяч субъектов критической информационной инфраструктуры, куда входят и базы организаций хранящие персональные данные, использует передовые технологии анализа больших данных, способна обнаруживать такие сложные угрозы, которые могут остаться незамеченными для отдельной организации. Исходя из постоянного развития способов и механизмов совершения кибератак, важно обратить внимание на то, что эта система всячески совершенствуется и дорабатывается на законодательном уровне, так Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», дополнил и более четко регламентировал список организаций и систем, которые должны быть подключены к ГосСОПКА¹.

Создание и функционирование ГосСОПКА является прямым исполнением требований современного российского законодательства в сфере кибербезопасности. В условиях геополитической напряженности цифровое информационное пространство стало ареной противостояния, где данная система выступает в качестве технологического щита, защищающего цифровой суверенитет страны, предотвращая потенциальные

¹ Колесникова М. Н. Основные функции ГОССОПКА в рамках, предупреждения и ликвидации компьютерных атак. Липецк, 2019. С. 31-35.

дестабилизирующие воздействия на финансовую, энергетическую, транспортную и коммуникационную системы.

Что касается гармонизации законодательства в области защиты персональных данных, то фокусе внимания государственных органов остается защита прав и интересов граждан при нарушениях и незаконных действиях, которые связаны с использованием персональных данных. В этих целях в 2021 году был создан Центр правовой помощи гражданам в цифровой среде. В 2022 году большая часть обращений, поступивших в центр, касались обработки личной информации без согласия человека, использования мошенниками конфиденциальных сведений и неправомерного задеирования персональных данных в рекламных целях¹. Такая мера является ответом на противоправные действия, связанные с личной информацией пользователей и помогает гражданам не только устранить данные нарушений, но и повысить уровень правовой грамотности субъектов цифрового пространства.

Подводя итог, стоит сказать, что направления развития национального законодательства Российской Федерации в области защиты персональных данных, имеет активную тенденцию выраженную во всяческой доработке уже имеющихся систем (такой как ГосСОПКА) и созданием специализированных центров, призванных решать вопросы связанные с приватность и сохранением личных данных граждан в цифровом пространстве, но и созданием совершенно новых платформ для безопасной коммуникации. Ярким примером такой платформы стала разработка национального приложения Мах, демонстрирующее четкий вектор на ужесточение, конкретизацию и технологическую адаптацию регуляторных требований. Этот вектор направлен на построение современной, эффективной системы защиты прав субъектов персональных данных в условиях цифровизации всех сфер общества, где приложение Мах стало неким мостом, позволившим существенно сблизить российские стандарты с международными.

¹ Бокова Л. Н. Правовые вопросы защиты персональных данных граждан в цифровом пространстве. М., 2023. С. 46.

ЗАКЛЮЧЕНИЕ

Исследование теоретико-методологического аспекта персональных данных, анализ правоприменительных инструментов защиты персональных данных в правовом и виртуальном пространствах и выявление правовых дефектов и механизмов совершенствования защиты персональных данных в системе российского законодательства позволяет сделать следующие выводы.

Во-первых, теоретико-методологический аспект персональных данных позволил концептуально рассмотреть содержание дефиниции «персональные данные».

Персональные данные, как определяет законодательство – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Ключевым моментом здесь является формулировка «любая информация», означающая, что закон защищает не только определенный тип данных (паспортные и иные), но и иную информацию о субъекте, выраженную в любой форме.

Важно отметить, что изучаемая дефиниция характеризуется и базируется на фундаментально-правовых и государственных началах, исходя из которых формируется ряд принципов, регулирующих сферу защиты персональных данных в виртуальном пространстве:

1) принцип законности и справедливости, говорящий о том, что обработка персональных данных должна иметь четкое правовое основание и вытекать из согласия, договора или иного законного интереса;

2) принцип прозрачности, гласящий о том, что пользователь должен четко понимать, кто, какие данные и зачем собирает о нем в онлайн пространстве;

3) принцип безопасности обязывающий операторов обеспечить защиту данных от утечек и взломов. Отсюда вытекает необходимость

шифрования, использования защищенных протоколов и обязанности уведомлять власти и пользователей о негативных фактах;

4) принцип минимизации данных, который указывает, что объем собираемых данных должен быть строго ограничен заявленной целью;

5) принцип трансграничной передачи данных, которые устанавливает правила передачи личных данных в другие страны, зачастую выражающееся в локализации баз данных.

Во-вторых, исследование правоприменительного аспекта защиты персональных данных в правовом и виртуальном пространствах показало, что защищенность представленных данных обусловлена следующими факторами: уровнем законодательной проработки, наличие ФЗ «О персональных данных» который прямо регулирует сбор, обработку и хранение данных; определенность правового статуса субъекта, показывающая насколько четко закон закрепляет права гражданина в области различных манипуляций с персональными данными, а также отражает механизмы их реализации; законодателем предъявлен достаточно строгий перечень требований к оператору обработки персональной информации; имеется относительно развитая правоприменительная практика в области решения споров связанных с защитой персональных данных.

В-третьих, рассмотрение правовых дефектов и механизмов совершенствования защиты персональных данных в системе российского законодательства выявили проблемы законодательного, правоприменительного характера, а также позволили концептуально сформулировать правовые инструменты, обеспечивающие совершенствование защиты персональных данных в системе права.

Проведенное исследование позволяет сделать вывод, что процесс обеспечения защиты персональных данных в виртуальном пространстве сопряжен с рядом фундаментальных вызовов и актуальных угроз, которые носят динамический характер и требуют постоянного совершенствования методов противодействия. Наиболее критичной группой остаются угрозы,

связанные с несанкционированным доступом к информационным системам, основной угрозой здесь становится увеличение числа случаев целевого фишинга и DDoS-атак с использованием методов социальной инженерии, которые направлены на обход технических средств защиты, с целью за получения доступа к базам данных, на которых хранятся персональные данные субъектов.

Определены основные направления развития и гармонизации национального законодательства в области защиты персональных данных, а именно в условиях глобализации цифровых потоков наблюдается устойчивый тренд на конвергенцию национальных правовых режимов с международными стандартами, прежде всего с Общим регламентом по защите данных (GDPR) Европейского Союза. В противовес глобализации, ключевым трендом развития и гармонизации является усиление государственного суверенитета в области регулирования цифрового пространства, а именно был создан и введен национальный мессенджера Мах, который на фоне санкционного давления является отечественной платформой, соответствующей всем необходимым стандартам в области защиты личных данных ее пользователей.



СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты

1. Российская Федерация. Законы. Конституция Российской Федерации : [принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 ; с учетом поправок, внесенных законом Российской Федерации о поправке к Конституции Российской Федерации от 14 марта 2020 г. № 1-ФКЗ]. – URL: <http://www.pravo.gov.ru> (дата обращения: 06.10.2022).

2. Российская Федерация. Законы. О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных : Федеральный закон № 160-ФЗ : [принят Государственной Думой 25 ноября 2005 года : одобрен Советом Федерации 7 декабря 2005 года]. – URL: <http://www.pravo.gov.ru> (дата обращения: 19.12.2005).

3. Российская Федерация. Законы. Гражданский кодекс Российской Федерации (часть первая) : Федеральный закон № 51-ФЗ : [принят Государственной Думой 21 октября 1994 года : одобрен Советом Федерации 11 ноября 1994 года]. – URL: <http://www.pravo.gov.ru> (дата обращения 01.08.2025).

4. Российская Федерация. Законы. Уголовный кодекс Российской Федерации : Федеральный закон № 63-ФЗ : [принят Государственной Думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года]. – URL: <http://www.pravo.gov.ru> (дата обращения 20.02.2026).

5. Российская Федерация. Законы. О персональных данных : Федеральный закон № 152-ФЗ : [принят Государственной Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года]. – URL: <http://www.pravo.gov.ru> (дата обращения 24.06.2025).

6. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ : [принят Государственной Думой 08 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года]. – URL: <http://www.pravo.gov.ru> (дата обращения 29.12.2025).

7. Российская Федерация. Законы. О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон № 156-ФЗ : [принят Государственной Думой 10 июня 2025 года : одобрен Советом Федерации 18 июля 2025 года]. – URL: <http://www.pravo.gov.ru> (дата обращения 23.05.2025).

8. Российская Федерация. Законы. О внесении изменений в Федеральный закон «О персональных данных» : Федеральный закон № 261-ФЗ : [принят Государственной Думой 6 июля 2011 года : одобрен Советом Федерации 13 июля 2011 года]. – URL: <http://www.pravo.gov.ru> (дата обращения 25.07.2011).

9. Российская Федерация. Законы. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон № 187-ФЗ : [принят Государственной Думой 12 июля 2017 года : одобрен Советом Федерации 19 июля 2017 года]. – URL: <http://www.pravo.gov.ru> (дата обращения 07.04.2025).

10. Российская Федерация. Президент. О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы : указ Президента Российской Федерации от 09.05.2017 № 203. – URL: <http://pravo.gov.ru> (дата обращения: 09.05.2017).

11. Российская Федерация. Президент. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры

Российской Федерации : указ Президента Российской Федерации от 03.02.2012 № 803. – URL: <http://pravo.gov.ru> (дата обращения: 03.02.2012).

12. Российская Федерация. Правительство. Об определении состава сведений, размещаемых в единой биометрической системе, в том числе в ее региональных сегментах, а также о внесении изменений в некоторые акты Правительства Российской Федерации : постановление Правительства Российской Федерации от 30 июня 2018 г. № 772. – URL: <http://www.pravo.gov.ru> (дата обращения 23.03.2024).

13. Российская Федерация. Правительство. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119. – URL: <http://www.pravo.gov.ru> (дата обращения 01.11.2012).

14. Российская Федерация. Федеральная служба по техническому и экспортному контролю. Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК России от 18 февраля 2013 г. № 21. – URL: <http://pravo.gov.ru> (дата обращения: 14.05.2020).

15. Российская Федерация. Приказы. Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных данных, за исключением случаев, указанных в пункте 9-1 части 1 статьи 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» : приказ Роскомнадзора России от 19 июня 2025 г. № 140. – URL: <http://pravo.gov.ru> (дата обращения: 27.06.2025).

16. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (пересмотренная) : (заключена в г. Страсбурге 10.10.2018) // Совет Европы [электронный ресурс]. – URL: <https://base.garant.ru> (дата обращения: 20.03.2026).

17. Китайская Народная Республика. Законы. О защите персональной информации : [принят Постоянным комитетом Всекитайского собрания народных представителей 20 августа 2021 года] : Закон от 1 ноября 2021 года // Personal Information Protection Law of the People's Republic of China : – URL: <http://ru.china-embassy.gov.cn> (дата обращения: 29.12.2021).

18. Регламент (ЕС) 2016/679 Европейского Парламента и Совета от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, и отмене Директивы 95/46/ЕС (Общий регламент по защите данных) // Официальный журнал Европейского союза. – 2016. – L 119. – С. 1–88. – URL: <https://eur-lex.europa.eu> (дата обращения: 20.03.2026).

Монографии

19. **Ковалева, Н. Н.** Правовое регулирование бережного и устойчивого оборота данных : монография / Н. Н. Ковалева. – Москва : ИНФРА-М, 2025. – 215 с. – (Научная мысль). – DOI 10.12737/2209356. – ISBN 978-5-16-020996-8. – URL: <https://znanium.ru/catalog/product/2209356> (дата обращения: 17.03.2026). — Режим доступа: для зарегистрированных пользователей.

20. **Талапина, Э. В.** Оборот данных в государственном управлении: перспективы правового регулирования : монография / Д. Ю. Южаков. – Москва : Издательский дом «Дело» РАНХиГС, 2020. – 244 с. – ISBN 978-5-85006-220-0. – URL: <https://znanium.ru/catalog/product/1405786> (дата обращения: 17.03.2026). – Режим доступа: для зарегистрированных пользователей.

Научные статьи

21. **Галиев, М. С., Тупицын, Р. С.** Защита персональных данных: взгляд от теории к правоприменению / М. С. Галиев, Р. С. Тупицын // Юриспруденция: актуальные вопросы теории и практики: сборник статей XI

Международной научно-практической конференции. – Пенза: МЦНС «Наука и Просвещение». – 2026. – С. 10-16 (дата обращения: 15.03.2026).

22. **Галиев, М. С., Тупицын, Р. С.** Юридическая конструкция «Персональные данные»: теоретико-правовой и уголовно-правовой аспекты / М. С. Галиев, Р. С. Тупицын // Юриспруденция, закон и порядок: актуальные вопросы теории и практики: сборник статей XI Международной научно-практической конференции. – Пенза: МЦНС «Наука и Просвещение», 2026. – С. 12-17 (дата обращения: 20.03.2026).

23. **Петрыкина, Н. И.** Правовое регулирование оборота персональных данных. Теория и практика / Н. И. Петрыкина. – Москва : Статут, 2011. – 134 с. ISBN 978-5-8354-0771-2, 1000 экз. – URL: <https://znanium.com/catalog/product/317790> (дата обращения: 17.03.2026). — Режим доступа: для зарегистрированных пользователей.

24. **Минбалеев, А. В.** Проблемные вопросы понятия и сущности персональных данных / А. В. Минбалеев // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 2 (4). – С. 4-9. – URL: <http://kononov42.ru/wp-content/uploads/2020/09/> (дата обращения: 12.12.2025).

25. **Абрамова, А. Г.** Современные проблемы осуществления защиты персональных данных в сети : основополагающие принципы защиты персональных данных / М. Е. Соколкова // Регион и мир. – 2020. – № 4. – С. 21-25. – URL: <https://cyberleninka.ru/article/n/sovremennyye-problemy-osuschestvleniya-zaschity-personalnyh-dannyh-v-seti-osnovopolagayushchie-principy-zaschity-personalnyh-dannyh> (дата обращения: 11.12.2025).

26. **Чурилов, А. Ю.** Принципы Общего регламента Европейского союза о защите персональных данных (GDPR) : проблемы и перспективы имплементации / А. Ю. Чурилов // Сибирское юридическое обозрение. – 2019. – Т. 16. – № 1. – С. 29-35. – URL: <https://cyberleninka.ru/article/n/printsiipy-obshchego-reglament-a-evropeyskogo-soyuza-o-zaschite-personalnyh-dannyh-gdpr-problemy-i-perspektivy-implementatsii> (дата обращения: 18.12.2025).

27. **Могунова, М. М.** Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг) / М. М. Могунова // Вестник Саратовской государственной юридической академии. – 2020. – № 4 (135). – С. 135-141. – URL: <https://cyberleninka.ru/article/n/tehnologiya-osuschestvleniya-i-pravovaya-reglamentatsiya-nezakonnogo-ovladieniya-personalnymi-bankovskimi-dannymi-fishing> (дата обращения: 12.11.2025).

28. **Савельев, А. И.** Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) / А. И. Савельев // Право. Журнал Высшей школы экономики. – 2015. – № 1. – С. 43-66. – URL: <https://cyberleninka.ru/article/n/problemny-primeneniya-zakonodatelstva-o-personalnyh-dannyh-v-epohu-bolshih-dannyh-big-data> (дата обращения: 28.12.2025).

29. **Голоскоков, Л. В.** Сетевое законодательство: концепция развития / Л. В. Голоскоков // Информационное право. – 2006. – № 4. – С. 11-15. – URL: <https://elibrary.ru/item.asp?id=12690842> (дата обращения: 12.01.2026).

30. **Кочеткова, Н. П.** Цифровая реальность и приватность: вызовы и решения в современном коммуникативном пространстве / Е. А. Чурашова // KANT. – 2024. – № 4 (53). – С. 234-242. – URL: <https://cyberleninka.ru/article/n/tsifrovaya-realnost-i-privatnost-vyzovy-i-resheniya-v-sovremennom-kommunikativnom-prostranstve> (дата обращения: 12.01.2026).

31. **Ястребова, А. Ю.** Право человека на защиту персональных данных: международно-правовые основы, примеры их имплементации в законодательстве государств, особенности регламентации в праве ЕС и национальном праве США / А. Ю. Ястребова, Т. Ф. Акчурин, И. О. Анисимов, И. Б. Горелик // Международный правовой курьер. – 2021. – № 7. – С. 93. – URL: <https://elibrary.ru/item.asp?id=47553502> (дата обращения: 13.02.2026).

32. **Свиридова, Е. А.** Региональные модели правового регулирования защиты данных в странах ЕС и АТЭС / Е. А. Свиридова // Проблемы экономики

и юридической практики. – 2024. – Т. 20. – № 2. – С. 81-88. – URL: <https://cyberleninka.ru/article/n/regionalnye-modeli-pravovogo-regulirovaniya-zaschity-dannyh-v-stranah-es-i-ates> (дата обращения: 16.03.2026).

33. **Ибрагимова, Ю. Э.** Устранение пробелов гражданского законодательства путем внедрения категории «цифрового права» / Ю. Э. Ибрагимова // Пробелы в российском законодательстве. – 2019. – № 5. – С. 49 – 53. – URL: <https://cyberleninka.ru/article/n/ustranenie-probelov-grazhdanskogo-zakonodatelstva-putem-vnedreniya-kategorii-tsifrovye-prava> (дата обращения: 17.02.2026).

34. **Плотникова, Т. В.** Феномен «цифровых прав» в контексте правового регулирования виртуального пространства / Т. В. Плотникова, В. В. Харин // Право: история и современность. – 2022. – Т. 6. – № 3. – С. 392-400. – URL: <https://cyberleninka.ru/article/n/fenomen-tsifrovyyh-prav-v-kontekste-pravovogo-regulirovaniya-virtualnogo-prostranstva> (дата обращения: 15.01.2026).

35. **Степанов, О. А.** Правовое регулирование генезиса цифровой личности / О. А. Степанов, М. М. Степанов // Правоприменение. – 2022. – Т. 6. – № 3. – С. 19-32. – URL: <https://cyberleninka.ru/article/n/pravovoe-regulirovanie-genezisa-tsifrovoy-lichnosti> (дата обращения: 21.02.2026).

36. **Володенков, С. В.** Новые формы политического управления в киберпространстве XXI века: вызовы и угрозы / С. В. Володенков // Известия Саратовского университета. Новая серия. Серия: Социология. Политология. – 2011. – Т. 11, № 2. – С. 78–85. – URL: <https://cyberleninka.ru/article/n/novye-formy-politicheskogo-upravleniya-v-kiberprostranstve-xxi-veka-vyzovy-i-ugrozy> (дата обращения: 14.03.2026).

37. **Забокрицкая, Л. Д.** Информационная культура современной молодежи: угрозы и вызовы виртуального социального пространства / Л. Д. Забокрицкая // Вестник Пермского национального исследовательского политехнического университета. Социально-экономические науки. – 2017. – № 4. – С. 114-123. – URL: <https://cyberleninka.ru/article/n/informatsionnaya-kultura>

sovremennoy-molodezhi-ugrozy-i-vyzovy-virtualnogo-sotsialnogo-prostranstva (дата обращения: 16.12.2025).

38. **Бокова, Л. Н.** Правовые вопросы защиты персональных данных граждан в цифровом пространстве / Л. Н. Бокова // Вестник Московского городского педагогического университета. Серия: Юридические науки. – 2023. – № 1 (49). – С. 41-48. – URL: <https://cyberleninka.ru/article/n/pravovye-voprosy-zaschity-personalnyh-dannyh-grazhdan-v-tsifrovom-prostranstve> (дата обращения: 22.01.2026).

39. **Колесникова, М. Н.** Основные функции ГОССОПКА в рамках, предупреждения и ликвидации компьютерных атак / М. Н. Колесникова, С. В. Ананьев // Информационные технологии в процессе подготовки современного специалиста. – 2019. – № 23. – С. 31-35. – URL: <https://elibrary.ru/item.asp?id=41482602> (дата обращения: 18.01.2026).

40. **Маклачкова, В. В.** Основные риски персональных данных в мультиоблачных информационных средах / В. В. Маклачкова // Экономика и качество систем связи. – 2025. – Т. 3. – № 37. – С. 169-181. – URL: <https://cyberleninka.ru/article/n/osnovnye-riski-personalnyh-dannyh-v-multioblachnyh-informatsionnyh-sredah> (дата обращения: 17.01.2026).

41. **Умаров, Б.** Киберпреступления с использованием персональных данных и электронных платежных систем: вызовы, угрозы и пути предупреждения / Б. Умаров // Общество и инновации. – 2025. – Т. 6. – № 6. – С. 50-56. – URL: <https://cyberleninka.ru/article/n/kiberprestupleniya-s-ispolzovaniem-personalnyh-dannyh-i-elektronnyh-platezhnyh-sistem-vyzovy-ugrozy-i-puti-preduprezhdeniya> (дата обращения: 14.12.2025).

42. **Унижаев, Н. В.** Особенности моделирования угроз безопасности персональных данных для обеспечения достаточного уровня защищенности / Н. В. Унижаев // Вопросы инновационной экономики. – 2022. – Т. 12. – № 1. – С. 95-110. – С. 50-56. – URL: <https://cyberleninka.ru/article/n/osobennosti-modelirovaniya-ugroz-bezopasnosti-personalnyh-dannyh-dlya-obespecheniya-dostatochnogo-urovnya-zaschishennosti> (дата обращения: 11.02.2026).

Правоприменительная практика

43. Решение Арбитражного суда Республики Башкортостан от 14 февраля 2024 года по делу № № А07-3409/023 // Интернет-ресурс Судебные практики и нормативные акты РФ. – URL: <https://sudact.ru> (дата обращения: 14.03.2026).

44. Решение Красноярского УФАС России от 23 апреля 2025 по делу № 024/05/18-662/2025 // Официальный сайт Федеральной антимонопольной службы. – URL: <https://www.tenderguru.ru/fas/1865461> (дата обращения: 16.03.2026).

45. Обзор типовых нарушений обязательных требований законодательства Российской Федерации в области персональных данных по результатам проведенных в 2022 году контрольно-надзорных мероприятий. – 2023. – URL: <https://rkn.gov.ru> (дата обращения: 20.03.2026).

46. О порядке формирования региональных «белых списков» информационных ресурсов : разъяснения Роскомнадзора от 20.01.2026 // [официальный сайт Роскомнадзора]. – URL: <https://rkn.gov.ru> (дата обращения: 13.03.2026).

47. Рекомендации Совета ОЭСР о защите частной жизни и трансграничных потоках персональных данных (23 сентября 1980 г.) [официальный сайт ОСЭР]. – URL: <https://www.sps-ib.ru> (дата обращения: 23.02.2026).

Электронные ресурсы

48. Азиатско-Тихоокеанское экономическое сотрудничество (АТЭС). Рамочные принципы защиты частной жизни АТЭС (2015) // Asia-Pacific Economic Cooperation : [официальный сайт АТЭС]. – URL: <https://www.apec.org> (дата обращения: 19.02.2026).

49. Заключение Правового управления, подготовленное к рассмотрению законопроекта в первом чтении (по поручению Совета

Государственной Думы (протокол от 09.04.2018 № 111, пункт 66) : [интернет портал «Системы обеспечения законодательной деятельности»]. – URL: <https://sozd.duma.gov.ru> (дата обращения: 14.02.2026).

50. Путин заявил о достижении полного цифрового суверенитета России // ФедералПресс : [официальный сайт]. – 2025. – 19 декабря. – URL: <https://fedpress.ru> (дата обращения: 13.03.2026).