МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА
ВЫСШАЯ ШКОЛА ГОСУДАРСТВЕННОГО АУДИТА

На правах рукописи

Сапронов Дмитрий Юрьевич

Обработка персональных данных в Российской Федерации: информационно-правовой аспект

Специальность: 5.1.2. Публично-правовые (государственно-правовые) науки

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук,
профессор Батурин Юрий Михайлович

Москва — 2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования Становление и развитие информационного общества и государства повысили значимость правового института защиты персональных данных в условиях углубляющейся цифровой трансформации государственного управления. Современные информационно-коммуникационные технологии не только создали новые уникальные возможности, но и породили неизвестные ранее вызовы и угрозы. Подписанный 7 мая 2024 года Указ Президента Российской Федерации № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»[1] обозначил сферу цифровой трансформации социальных отношений, связанных с государственным и муниципальным управлением, социальной сферой и экономикой, как одну из ключевых для достижения устойчивого социального и экономического развития нашей страны. Это актуализировало необходимость фундаментальных исследований в области информационно-правового регулирования обработки персональных данных и их защиты.

Возможности, принесённые новой информационно-технологической реальностью, придали мощный импульс развитию отношений во всех сферах социальной жизни и оказали существенное влияние на информационную безопасность. Собираемые электронные массивы личной информации физических лиц стали целью охоты различных злоумышленников и иных заинтересованных лиц, желающих с помощью этой информации незаконно обогатиться или совершить другие противоправные действия. Используя полученную информацию о людях, злоумышленники всё чаще наносят финансовый ущерб своим жертвам и заставляют их совершать противоправные действия, в том числе и в отношении государственных органов.

Проблему, решаемую в исследовании, можно сформулировать следующим образом. Стремительное развитие и повсеместное внедрение информационно-коммуникационных (цифровых) технологий привело к тому, что их применение

[1] См.: Указ Президента РФ от 07.05.2024 № 309 "О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года". // Собрание законодательства РФ, 13.05.2024, № 20, ст. 2584.

стало составной частью социальных отношений. Содержание части норм информационного права перестало соответствовать содержанию отношений, подлежащих правовому регулированию, ввиду десинхронизации (рассогласования) сущего и должного в регулируемых отношениях. Это привело к появлению дефектов информационного законодательства в рассматриваемой области из-за быстрого устаревания части правовых норм.

Становление и развитие информационного общества, которое обусловило динамичное изменение информационных общественных отношений, а также интенсификация процессов обработки персональных данных с помощью автоматизированных информационных систем порождают насущную потребность в концептуальном переосмыслении действующих механизмов информационно-правового регулирования обработки персональных данных в Российской Федерации. Степень актуальности последовательно повышается. Одновременно расширяется сфера влияния не только на индивидуальные и общественные интересы, но и на публично-правовые интересы государства.

Разработанность темы диссертационного исследования. Отечественная юридическая наука уделяла серьезное внимание тематике, рассматриваемой в настоящем исследовании. Проблемы, связанные с правовой защитой персональных данных, волнуют юридическое сообщество достаточно давно, по этой тематике опубликованы труды М.Н. Алексашиным, И.Л. Бачило, И.С. Бойченко, Ю.М. Батуриным, Е.А. Войниканис, Г.К. Гаджиевым, В.В. Грибом, Н.Н. Ковалёвой, А.В. Кротовым, Е.В. Кирильчик, И.А. Михайловой, А.В. Минбалеевым, А.В. Морозовым, В.Б. Наумовым, Т.А. Поляковой, И.М. Рассоловым, А.И. Савельевым, Л.К. Терещенко, А.А. Чеботаревой и другими исследователями. Различные правовые аспекты защиты персональных данных рассматривались в разные годы в следующих диссертационных исследованиях: Ф.А. Абаев «Правовое регулирование отношений по защите персональных данных работника в трудовом праве» (2014 г.), Н.Г. Белгородцева «Теоретико-правовые аспекты защиты персональных данных» (2012 г.), М.В. Бундин «Персональные данные в системе информации ограниченного доступа» (2017 г.), И.А. Вельдер

«Система правовой защиты персональных данных в Европейском Союзе» (2006 г.), С.И. Гутник «Уголовно-правовая характеристика преступных посягательств в отношении персональных данных» (2017 г.), А.В. Дворецкий «Защита персональных данных работника по законодательству Российской Федерации» (2005 г.), И.А. Ильюшина «Правовое регулирование и защита персональных данных в виртуальной среде организаций» (2025 г.), Я.В. Кудашкин «Правовое обеспечение безопасности обработки персональных данных в сети интернет» (2019 г.), А.В. Кучеренко «Правовое регулирование персональных данных в Российской Федерации» (2010 г.), Н.И. Петрыкина «Правовое регулирование оборота персональных данных в России и странах ЕС: сравнительно-правовое исследование» (2007 г.), О.Б. Просветова «Защита персональных данных» (2005 г.), А.А. Чеботарёва «Правовое обеспечение информационной безопасности личности в глобальном информационном обществе» (2018 г.) и др.

Таким образом, за прошедшие годы, работами российских исследователей-юристов были охвачены многие аспекты изучаемой области. Однако системно не рассмотренными остались такие важные актуальные вопросы как влияние цифровизации на правовое регулирование обработки персональных данных, актуализация понятийного аппарата, роль защиты персональных данных в обеспечении национальной безопасности Российской Федерации, влияние применения технологий bigdata[2] и искусственного интеллекта[3] на защищённость персональных данных, роль института общественного контроля в обеспечении безопасности персональных данных и др. Следовательно, рассматриваемые в

[2] Далее: bigdata, технология больших данных, большие данные. Здесь и далее под понятием большие данные (big data): понимаются большие массивы данных отличающиеся главным образом такими характеристиками, как объем, разнообразие, скорость обработки и/или вариативность, которые требуют использования технологии масштабирования для эффективного хранения, обработки, управления и анализа (ГОСТ Р ИСО/МЭК 20546-2021 «Информационные технологии. Большие данные. Обзор и словарь»).

[3] Далее: ИИ-системы, системы искусственного интеллекта, нейросети. Здесь и далее под искусственным интеллектом понимается — комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений (Национальная стратегия развития искусственного интеллекта на период до 2030 года, утв. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации»).

диссертации вопросы имеют фундаментальный и глобальный характер; проблематика, которому посвящено исследование пока не нашла системного и достаточно глубокого освещения в современной отечественной юридической науке.

Объект исследования – информационные общественные отношения, возникающие при обработке различными информационными системами массивов персональных данных, представленных в электронной форме, которые могут быть как анонимизированными, так и индивидуализированы.

Предмет диссертационного исследования — нормы права, которые регулируют обработку массивов персональных данных.

Цель диссертационного исследования **—** разработка обоснованной современной научной концепции совершенствования информационно-правового регулирования обработки персональных данных.

Для достижения указанной цели были сформулированы следующие **задачи** диссертационного исследования:

1) Выявить значимые для правового регулирования признаки и правовую природу «персональных данных» и актуализировать взаимосвязь и смысловое наполнение ряда ключевых правовых понятий образующих единую концептуальную группу в рассматриваемой области;

2) Определить систему принципов информационно-правового регулирования обработки персональных данных с использованием нейросетей, предусматривающих приоритет защиты прав и интересов субъектов персональных данных;

3) Установить требования к информационно-правовому регулированию обработки персональных данных системами искусственного интеллекта;

4) Определить степень воздействия цифровизации государственного управления на правовую защиту персональных данных и выявить основное направление системного совершенствования информационно-правового регулирования персональных данных в Российской Федерации;

5) Установить взаимосвязь между несанкционированным доступом к информации о населении и угрозами национальной и информационной безопасности Российской Федерации, выявить характер и масштабы ущерба, причиняемого в результате таких инцидентов, а также обосновать необходимость отражения в документах стратегического планирования значимости защиты персональных данных как неотъемлемого элемента системы обеспечения национальной и информационной безопасности Российской Федерации с учётом актуальных вызовов и угроз;

6) Выявить наиболее успешные и эффективные примеры зарубежной практики информационно-правового регулирования обработки персональных данных, для выявления источников возможной рецепции;

7) Установить значимость роли общественного контроля в повышении эффективности работы механизма правовой защиты персональных данных при использовании для их обработки сквозных технологий.

Теоретическую основу диссертационного исследования составили труды отечественных ученых — по теории государства и права (А. Б. Венгеров, Н. В. Витрук, В. Б. Исаков, А. Н. Головистикова, Ю. А. Дмитриев, Т. В. Касаева, А. В. Малько, Н. И. Матузов, М. Н. Марченко, А. С. Мордовец, В. С. Нерсесянц, А. С. Пиголкин, С. Ю. Наумов и др.), теории конституционного права (С. А. Авакьян, М. В. Баглай, Н. А. Богданова, В. Д. Зорькин, А. В. Зиновьев, В. Е. Чиркин, С. М. Шахрай, Б. С. Эбзеев и др.), теории информационного права (И. Л. Бачило, Ю. М. Батурин, А. В. Минбалеев, А. В. Морозов, В. Б. Наумов, Т. А. Полякова, М. А. Федотов, М. М. Рассолов, А. А. Стрельцов, Н. Н. Ковалёва и др.) и др.. А также материалы, относящиеся к иным областям знаний, в том числе и по информационным технологиям.

Методологическую основу диссертационного исследования образуют общенаучные и специально-юридические методы.

Для решения поставленных задач применены следующие общенаучные методы: диалектический, исторический, системно-структурного анализа. К специально-юридическим методам относятся: сравнительно-правовой, формально-

юридический, функциональный и др. Применение сравнительно-правового метода позволило проанализировать действующие нормативно-правовые и подзаконные акты и выявить особенности отечественного и зарубежного правового регулирования в рассматриваемой области, а также определить общие и частные характеристики института персональных данных. Комплекс использованных методов позволил сформулировать предложения и рекомендации по совершенствованию информационно-правового регулирования обработки персональных данных, а также общую методику совершенствования в рассматриваемой области законодательства.

Нормативную основу исследования образуют положения Конституции Российской Федерации, федеральные конституционные законы, федеральные законы и иные нормативно-правовые акты в сфере обработки персональных данных, международные договоры, конвенции, соглашения, а также нормативно-правовые акты иностранных государств и межгосударственных организаций, которые затрагивают защиту персональных данных и реализацию права на невмешательство в частную жизнь.

Эмпирическая база диссертационного исследования образована решениями Конституционного Суда Российской Федерации, Европейского Суда по правам человека и иных российских и зарубежных судов, статистическими данными, в том числе документами, подготовленными межгосударственными органами и организациями, а также сведениями из других информационных ресурсов, затрагивающими информационно-правовое регулирование обработки персональных данных.

Научная новизна диссертации заключается в разработке положений современной научной концепции совершенствования информационно-правового регулирования обработки персональных данных, которая учитывает быструю динамику развития общественных отношениях в рассматриваемой области. Разработанная концепция включает положения, определяющие ключевые элементы системы обеспечения защиты персональных данных, к которым можно отнести: доказательство необходимости указания в документах стратегического

планирования в области информационной и национальной безопасности на важность высокого приоритета защиты персональных данных для государственного суверенитета и перечень формулировок таких указаний; предложения по актуализации понятийного аппарата в исследуемой области, а именно правовое определение понятия «персональные данные» и дефиниции ряда связанных понятий; сформулированные регулятивные установки касающиеся регламентации обработки персональных данных системами с искусственным интеллектом; разработанную в исследовании модель встраивания механизмов общественного контроля в систему правовой защиты персональных данных; обоснование возможности заимствования и адаптации к российским реалиям успешных подходов по защите персональных данных из других юрисдикций. Использованные в работе научные методы позволили составить существенно более расширенный в сравнении с другими исследованиями и обновившийся ввиду высокой динамики развития отношений связанных с обработкой персональных данных перечень пробелов правового регулирования.

Положения, выносимые на защиту:

1) персональные данные — документированная (электронно и\или неэлектронно) информация, относящаяся прямо или косвенно, к определенному или определяемому физическому лицу (субъекту персональных данных), позволяющая его (субъект) идентифицировать полностью или частично, в том числе с применением автоматизированных и неавтоматизированных информационных технологий;

большие данные — совокупность массивов информации (которые характеризуются объемом, скоростью обработки, разнообразием и вариативностью данных), содержащих как персональные, так и не персональные, данные физических лиц, обрабатывая которые, при помощи Искусственного интеллекта (нейросетей), можно получить новую информацию, в том числе и персональные данные физических лиц;

биометрические персональные данные — информация, составляющая совокупность физических, физиологических и\или поведенческих признаков

физического лица, используя которую можно выполнить или подтвердить однозначную идентификацию его личности.

2) Правовое регулирование обработки персональных данных с использованием нейросетей должно строиться на принципах, которые основаны на приоритете интересов личности, а именно: добровольности согласия субъектов персональных данных; защиты прав и свобод человека; прозрачности и объяснимости работы систем искусственного интеллекта; повышенных требований к безопасности и обязательности независимого аудита ИИ-систем, обрабатывающих специальные категории персональных данных и др.

3) Информационно-правовое регулирование обработки персональных данных системами искусственного интеллекта необходимо строить с учётом следующих особенностей: субъект персональных данных должен быть проинформирован о том, что его данные будут собираться и обрабатываться системой искусственного интеллекта; обработка персональных данных системой искусственного интеллекта осуществляется только с разрешения субъекта персональных данных или уполномоченного им лица; системы искусственного интеллекта, обрабатывающие персональные данные в коммерческих целях подлежат обязательной регистрации уведомительным порядком у уполномоченного государственного органа; необходимо повысить прозрачность для субъекта персональных данных процедур сбора, хранения, обработки и особенно передачи информации о человеке третьим лицам путём информирования физического лица о фактах передачи его данных; критерии соблюдения информационной безопасности при использовании систем искусственного интеллекта требуют нормативного закрепления.

4) Основным направлением системного совершенствования правового регулирования персональных данных в Российской Федерации должна выступать регламентация порядка того, как должно осуществляться функционирование механизма правовой защиты информации о физическом лице на электронном носителе. Систему защиты такой информации о физическом лице можно определить как совокупность правовых средств, направленных на защиту

информации, документированной (электронно и\или неэлектронно), относящейся прямо или косвенно, к определенному или определяемому физическому лицу (субъекту персональных данных), позволяющей его (субъект) идентифицировать полностью или частично, в том числе с применением автоматизированных и неавтоматизированных информационных технологий.

5) Ущерб, причиняемый вследствие несанкционированного доступа к информации о населении, носит комплексный (многокомпонентный) характер и непосредственно затрагивает ключевые аспекты информационной и национальной безопасности Российской Федерации. В документах стратегического планирования необходимо отразить значимость защиты персональных данных для системы обеспечения национальной и информационной безопасности Российской Федерации, с учётом современных вызовов и угроз.

6) При совершенствовании информационно-правового регулирования обработки персональных данных в Российской Федерации может быть использован следующий опыт зарубежных государств: правовая конструкция «чувствительных персональных данных» (персональные данные, разглашение которых может навредить субъекту персональных данных), юридическое закрепление тождественности принципов защиты информации о частной жизни и персональных данных, введение обязательного периодического независимого аудита информационных систем обработки персональных данных с предоставлением результатов в уполномоченный государственный орган (КНР); регламентация процедуры проверки, учёта и отзыва поданных заявлений о согласии на обработку персональных данных через единую государственную информационную систему или иную аналогичную систему (Республика Казахстан); механизм контроля и привлечения к юридической ответственности за нарушения в области защиты персональных данных (США и ЕС).

7) Обработка персональных данных требует, кроме государственного, дополнительного контура контроля. Предложено использовать в этом качестве общественный контроль, ранее в сфере обработки персональных не использовавшийся. Определены основные направления и подходы, разработана

концептуальная модель осуществления общественного контроля, включающая: формы участия гражданского общества в мониторинге соблюдения прав субъектов персональных данных; процедуры взаимодействия общественных институтов с регуляторами и операторами персональных данных.

Теоретическая значимость работы заключается в разработке методологии юридического анализа отношений по поводу обработки персональных данных во взаимосвязи с большими данными, а также в том, что она заложила основы теории информационно-правовой защиты персональных данных, представляемых в различных формах. Кроме того, результаты диссертационного исследования могут использоваться при преподавании дисциплин, относящихся к информационному праву, а также для написания и подготовки учебных пособий и методических материалов по дисциплине «Информационное право».

Практическая значимость работы состоит в предоставлении законодателю конкретного перечня изменений и дополнений, которые требуется внести в действующее информационное законодательство, регламентирующее обработку персональных данных, а также в том, что результаты работы могут использоваться в нормотворческой деятельности (в части законодательного развития правовой защиты персональных данных и совершенствования норм, связанных с реализацией конституционного права личности на невмешательство в частную жизнь) и в правоприменительной деятельности (интерпретационной практике судов и иных государственных органов).

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

Достоверность результатов диссертационного исследования подтверждается обоснованностью использования соответствующей научной методологии — сформулированные в настоящей работе выводы и рекомендации логически обоснованы и имеют высокую степень достоверности, что подтверждено следующими тезисами: исследование проведено на теоретическом и практическом уровнях при помощи методов, которые соответствуют предмету,

цели и задачам работы. Достоверность также определяется всесторонним анализом информации об объекте исследования и передовом зарубежном опыте в рассматриваемой области. Кроме этого, достоверность результатов подтверждается их апробацией.

Апробация результатов диссертационного исследования Результаты и основные выводы диссертационного исследования представлены в выступлениях автора на более чем 30 научных конференциях, посвящённых проблемам информационной безопасности, вопросам регулирования отношений в информационном обществе, оценке законодательства в условиях цифровизации социальных отношений и др., среди которых можно выделить следующие: XV Международная научно-практической конференция преподавателей, докторантов, магистрантов и студентов «Интеграция науки и практики — механизм эффективного развития современного общества» (апрель 2023, г. Астана, университет «Туран-Астана»); Международная научно-практическая конференция «Стратегия развития экономики Беларуси: вызовы, инструменты реализации и перспективы» (октябрь 2022, г. Минск, Институт экономики Национальной академии наук Беларуси); Пятая международная научно-практическая конференция «Бачиловские чтения» (февраль 2022, г. Москва, ИГП РАН); Шестая международная научно-практическая конференция «Бачиловские чтения» (февраль 2023, г. Москва, ИГП РАН); Седьмая международная научно-практическая конференция «Бачиловские чтения» (февраль 2024, г. Москва, ИГП РАН); Научно-практический семинар «Персональные данные в условиях цифровой экономики» (октябрь 2022, г. Москва, ИЗИСП); XII Международная научно-практическая конференция «Право и информация: вопросы теории и практики» (ноябрь 2022, г. Санкт-Петербург, Президентская библиотека имени Б.Н. Ельцина); Аспирантский юридический форум 2023 (июнь 2023, г. Москва, ГАУГН); Аспирантский юридический форум 2024 (июнь 2024, г. Москва, ГАУГН); Шестая международная научно-практическая конференция «Вызовы информационного общества: Тенденции развития правового регулирования цифровых трансформаций» (ноябрь 2025, г. Москва, НИУ ВШЭ) и др.

Основные положения диссертационного исследования отражены в научных работах автора, опубликованных в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 5.1.2. «Публично-правовые (государственно-правовые) науки»:

1. *Сапронов Д. Ю.* К вопросу о правовом режиме больших данных (big data) // Вестник Московского университета. Серия 26. Государственный аудит. — 2019. — № 2. — С. 94–98. EDN: WXFSPR. Импакт-фактор: 0,153 (РИНЦ). 0,40 п.л.
2. *Сапронов Д. Ю.* Особенности правового регулирования персональных данных в Китайской Народной Республике // Вестник Московского университета. Серия 26. Государственный аудит. — 2022. — № 4. — С. 149–157. EDN: MONJKM. Импакт-фактор: 0,153 (РИНЦ). 0,49 п.л.
3. *Сапронов Д.Ю.* Цифровая трансформация государственного управления в Российской Федерации: особенности совершенствования законодательства о защите персональных данных // Государственная власть и местное самоуправление. — 2025. — № 6. — С. 39-43. EDN: UFTSQP. Импакт-фактор: 0,549 (РИНЦ). 0,31 п.л.
4. *Сапронов Д. Ю.* К вопросу о совершенствовании информационно-правового регулирования обработки персональных данных в Российской Федерации // Вестник Московского университета. Серия 26: Государственный аудит. – 2025. – № 3. — С. 136-151. EDN: FXDHKD. Импакт-фактор: 0,153 (РИНЦ). 0,94 п.л.
5. *Сапронов Д.Ю.* К вопросу об эволюции правового института защиты персональных данных // Вестник Российской правовой академии. — 2025. — № 6. – С.83-95. EDN: AKJZNF. Импакт-фактор: 0,069 (РИНЦ) 0,87 п.л.

Прочие публикации:

6. *Сапронов Д. Ю.* Особенности правового регулирования информационных отношений в области обработки персональных данных в зарубежных государствах (10.7). // Информационное право: учебник для вузов; под редакцией М. А. Федотова. 4-е изд., перераб. и доп / М. А. Федотов, Р. А.

Будник, Е. А. Войниканис и др. — Издательство Юрайт Москва, 2025. — 855 с./13 с. — 978-5-534-17958-3

7. *Сапронов Д. Ю., Будник Р. А., Иваева Э. А.* Особенности публично-правовой защиты персональных (в том числе биометрических) данных на постсоветском пространстве: модель республики Казахстан // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. — 2024. — Т. 10, № 76. — С. 159–164. EDN: BLBDPK. 0,04 п. л. из 0,13 п. л. (**в перечне ВАК**).
8. *Сапронов Д. Ю., Мелехин А. В., Пархоменко А. Г., Усанов В. Е.* К вопросу о публично-правовой защите персональной информации (на примере Республики Казахстан) // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. — 2024. — Т. 10, № 76. — С. 190–194. EDN: GTFXOP. 0,03 п. л. из 0,10 п. л. (**в перечне ВАК**).
9. *Сапронов Д. Ю.* Историческая ретроспектива правового регулирования персональных данных в некоторых странах // Труды по интеллектуальной собственности. — 2022. — Т. 42, № 3. — С. 26–32. 0,44 п. л. EDN: ULSYYW (**в перечне ВАК**).
10. *Сапронов Д. Ю.* Эволюция правового регулирования персональных данных в России // Труды по интеллектуальной собственности. — 2020. — Т. 36, № 3-4. — С. 180–186. 0,44 п. л. EDN: PNFYBW **(в перечне ВАК).**

Сапронов Д. Ю. Правовая эволюция общеевропейского регулирования защиты персональных данных. // Труды по интеллектуальной собственности. — 2019. — № 3-4. — С. 83–89. 0,44 п. л. EDN: CPMRRN **(в перечне ВАК)**.

Диссертация подготовлена и обсуждена на кафедре компьютерного права и информационной безопасности Высшей школы государственного аудита (факультет) МГУ имени М.В. Ломоносова.

Структура диссертационного исследования отражает логику исследования, обусловлена его предметом, поставленными целями и задачами. Работа включает в себя введение, три главы, в совокупности состоящих из девяти параграфов, заключение и библиографию.

ГЛАВА 1. Персональные данные: понятие, сущность и особенности информационно-правового регулирования

§ 1.1 Понятие и сущность персональных данных как информационно-правового института

Институционализация персональных данных в праве отражает стремление общества и государства обеспечить гарантии реализации основополагающих прав, включая право на неприкосновенность частной жизни и охрану соответствующих сведений. Потребность в обеспечении конфиденциальности такой информации стала причиной возникновения идеи о необходимости правового регулирования определённого рода информации, относящейся к человеку, которая позволяет так или иначе его идентифицировать — персональных данных. Они были юридически выделены в отдельный вид информации ограниченного доступа. Таким образом, рассматривать право на защиту персональных данных следует в связке с правом на неприкосновенность частной жизни, а также следует рассматривать их соотношение и взаимосвязь.

В современном мире право на неприкосновенность частной жизни (приватности), закреплённое в конституциях многих государств, является неотъемлемым правом человека и гражданина. Для воплощения принципа приватности в праве потребовалось значительное время. Появление и становление таких идей приходится на середину XX века, хотя сама концепция приватности была сформулирована в США в конце XIX века. Однако особенно этот вопрос о принятии норм правового регулирования персональных данных актуализировался ближе к 1970-м годам, в том числе и в связи появлением средств вычислительной техники, которые позволили автоматизировать процесс хранения и обработки персональных данных. Однако, всему этому предшествовала достаточно длинная и непростая история становления права на неприкосновенность частной жизни и закрепление его как неотъемлемого права человека и гражданина.

Рассматривая вопрос приватности, следует обратить внимание на лежащие в её основе философские взгляды. В основе неотъемлемого права человека на

невмешательство в его частную жизнь лежит идея свободы личности. Она была выдвинута Сократом, именно он принёс идею свободы личности в античную философию, до него философы античности больше интересовались вопросом «что есть природа?». По мнению Сократа, свобода — это «самообладание»; будучи в радости, печали, находясь под властью страстей человек должен сохранять власть над собой руководствуясь своими добродетелями[4]. Однако в античном обществе периода расцвета полисов уединение от общества не приветствовалось, о чём писал в своих трудах Платон «…толпе не присуще быть философом. — И значит те, кто занимается философией, неизбежно будут вызывать её порицание»[5]. Кроме этого, в Афинском государстве практиковалось изгнание из полиса провинившихся его жителей, они подвергались остракизму[6]. Итак, в тот период времени для того, чтобы воспользоваться правом на уединение нужно было иметь веские причины, например, быть философом.

С течением времени восприятие права личности на уединение менялось, и в отличие от античного времени, позднее оно стало выступать, как способ самопознания, который основан на вере и нацелен на поиски единения с Богом[7]. Таким образом, возможность реализации права человека на уединение в средние века зависела от того, к какой социальной страте он принадлежал, что отражало суть феодального времени, где права личности не имели значения.

С развитием юриспруденции мысль о необходимости уважения к личности и её правам нашла своё отражение в идеях естественного права. Джон Локк в своих работах писал: «Право каждого человека отстаивать свою жизнь, свободу и имущество, то есть то, что ему принадлежит»[8]; в дальнейшем именно этот принцип ляжет в основу закреплённых в конституциях многих государств прав человека и гражданина. Павел Иванович Новгородцев, который относился к т.н. «Московской

[4] См.: Нерсесянц В. С. Научные биографии. Сократ / АН СССР. — Москва: Наука, 1977. — 150 с.
[5] См.: Платон. Сочинения в четырех томах. т. 3. ч. 1 / Под общ. ред. А. Ф. Лосева и В. Ф. Асмуса; Пер.: с древнегреч. — С-Пб: Изд-во С.-Петерб., 2007. — 752 с.
[6] См.: Суриков И. Е. Институт остракизма в Афинах: проблемы и перспективы изучения. С .126–143.
[7] См.: Гагарин А. С. Одиночество как экзистенциал средневековой философии // Научный ежегодник Института философии и права Уральского отделения Российской академии наук. — 2012. — № 12. — С. 148–165.
[8] См.: Локк Д. Избранные философские произведения. Т. 2. М.: Соцэкгиз, 1960. — 532 с.

школе естественного права», в своих работах основывался на том, что «личность берется за основу для общественного созидания»[9], соответственно, с течением времени и развитием правовой науки, всё больше внимания уделялось личности и обеспечению её неотъемлемых прав.

Впервые концепцию приватности[10] (права на конфиденциальность частной жизни) обосновали в США в 1890 году американские юристы Сэмюэл Уоррен и Луис Брандейс в своей статье «Право на неприкосновенность частной жизни»[11]. Где дано определение неприкосновенности частной жизни: «право быть оставленным в покое», что в некоторой степени перекликается с идеями Сократа. Именно эту статью зарубежные исследователи называют «основой американского закона о конфиденциальности»[12]. Положения, изложенные в статье, послужили базисом и ориентиром для дальнейшего развития правовой мысли в этом направлении, что позволило позднее, опираясь на изложенную концепцию защиты информации о частной жизни индивидуума, разработать систему правовых норм, отражённых, как в международных правовых актах, так, позднее, и в конституциях многих государств.

Однако несмотря на то, что юридическая концепция права на приватность была высказана ещё в 1890 году, только в середине XX века идея неприкосновенности частной жизни получила всеобщее признание и была закреплена юридически на международном уровне. После принятия в 1948 году «Всеобщей декларации прав человека», в статье 12 которой, закреплено что: «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких

[9]См.: Новгородцев, П. И. Об общественном идеале. — М.: Издательство «Пресса», 1991. — 640 с.
[10] Агл. Privacy.
[11] См.: Warren S. D., Brandeis L. D. The Right to Privacy // Harvard Law Review. 1890. Vol.IV. № 5. p. 193–220, (пер.: Яндекс-переводчик).
[12] См.: Richards N. M. and Solove D. J., Privacy's Other Path: Recovering the Law of Confidentiality. // Georgetown Law Journal, Vol. 96, p. 123.

посягательств»[13]. Так, неприкосновенность частной жизни встала в один ряд с другими свободами индивидуума: правом на жизнь, свободой мысли, свободой слова, свободой передвижения, и была признана фундаментальным правом человека. В дальнейшем аналогичные нормы появились в большинстве конституций планеты. Помимо «Всеобщей декларации прав человека», нормы о неприкосновенности частной жизни позднее становились частью различных международных правовых документов: статья 17 «Международного пакта о гражданских и политических правах»[14] (1966), статья 8 «Европейской конвенции о правах человека»[15] (1950) и статья 7 «Хартии основных прав Европейского союза»[16] (2000). Неприкосновенность частной жизни утвердилась в качестве неотъемлемого права индивидуума. Однако её правовая интерпретация остаётся предметом научных споров. В разных странах содержание данного права формируется под влиянием национальных традиций, культурных норм и социальной среды. Согласно исследованиям ряда иностранных юристов, на механизмы защиты частной жизни воздействуют три основных фактора: «политический, социокультурный и личностный»[17]. За всё время существования концепции права на защиту частной жизни ей было дано множество правовых определений. Р. Поснер в своих работах высказывает мысль: «Одним из аспектов неприкосновенности частной жизни является удержание или сокрытие информации»[18], Ч. Фрайд замечал, что «конфиденциальность — это контроль, который мы имеем над информацией о себе»[19], интересным представляется определение конфиденциальности, которое дал венгерский правовед М. Сабо — «неприкосновенность частной жизни — это право индивида принимать решение о

[13] См.: Всеобщая декларация прав человека от 10 декабря 1948 г. // Международное публичное право. Сборник документов / Бекяшев К. А., Бекяшев Д. К. — М.: Проспект, 2009. — С. 221–224.
[14] См.: Международный пакт о гражданских и политических правах (Нью-Йорк, 19 декабря 1966 г.) // Бюллетень Верховного Суда РФ. 1994. № 12. С. 5.
[15] См.: Конвенция о защите прав человека и основных свобод. Заключена в г. Риме 4 ноября 1950 г. (с изм. от 13.05.2004, вместе с протоколами № 1, № 4 и № 7 // Собрание законодательства РФ. 2001. № 2. ст. 163.
[16] См.: Хартия Европейского Союза об основных правах: Комментарий / под ред. д.ю.н., проф. С. Ю. Кашкина. — М.: Юриспруденция, 2001.
[17] См.: Westin A. F.: Social and political dimensions of privacy // Journal of Social Issues Vol 59, No. 2. (2003) p. 431-434.
[18] См.: Posner D. T. on Privacy // International Journal of Applied Philosophy. Vol. 27, № 2(2013), p. 147–160
[19] См.: Rössler, B. The Value of Privacy // Cambridge; Polity Press.

себе»[20]. В отечественной юридической науке тоже не пришли к единому знаменателю по поводу содержания права на частную жизнь. К примеру, интересную мысль в своих работах высказывает А. В. Кротов: «По сути своей, право на частную жизнь непосредственно защищает ключевые гуманитарные ценности — свободу и человеческое достоинство. Символически это право олицетворяет собой ценностный смысл прав человека и все права человека в совокупности. Оно наиболее тесно пересекается с сущностью свободы, защищает личную свободу и человеческое достоинство, определяет возможности полноценного развития личности»[21]. Такой подход расширяет толкование права на защиту частной жизни и делает его более фундаментальным и значимым, особенно, когда неприкосновенность частной жизни тесно связывают с таким фундаментальным правом человека как право на жизнь. Отечественные юристы отмечают, что правовая защищённость неприкосновенности частной жизни «является важным показателем демократизации общества, служит необходимой предпосылкой становления и формирования правового государства»[22]. Эта мысль приводит нас к тому, что на сохранность информации о частной жизни индивидуума оказывает влияние свобода общества, по причине того, что именно государство является гарантом данного права, и в демократическом обществе правительство вынуждено создавать такую систему защиты неприкосновенности частной жизни, которая удовлетворяет потребности избирателей. Специалисты по конституционному праву рассматривают частную жизнь как неприкосновенность «среды обитания» человека; точка зрения других исследователей связана с тем, что понятие «частная жизнь» «…отражает естественное стремление каждого человека иметь собственный мир интимных и деловых интересов, скрытый от чужих глаз»[23]. С. А. Авакян отмечает, что понятие частной жизни включает в себя «1)

[20]См.: Szabo M . D. Kisérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival. // Információs Társadalom 2005-2. p. 46, (пер.: Яндекс-переводчик).
[21] См.: Кротов А. В. Соотношение права на частную жизнь с правом на жизнь, свободу и личную неприкосновенность // Адвокат. — 2011. — № 1. — С. 32–39.
[22] См.: Аберхаев Э. Р. "Право на неприкосновенность частной жизни: юридическая характеристика и проблемы реализации" // Russian Journal of Economics and Law, №. 1 (5), 2008, С. 90–94.
[23] См.: Баглай М. В. Конституционное право Российской Федерации: учеб. для вузов. — 13-е изм. и доп. — М. : Норма, 2018. — с. 228.

непосредственно собственную личную жизнь человека; 2) его жизнь в семье; 3) трудовую (в широком смысле слова) деятельность; 4) состояние здоровья; 5) общение человека с другими людьми, в том числе через современные технические средства такого общения»[24]. Отсюда можно сделать вывод, что право на неприкосновенность частной жизни может толковаться исследователями по-разному, но все они сходятся в том, что конфиденциальность частной жизни является неотъемлемым правом человека и включает различные стороны его жизни. Во многих случаях авторы рассматривают это понятие достаточно широко, относя к нему сведения, относящиеся к другим видам тайн. Следовательно, рассматривая зарубежный и отечественный подходы правовой науки к определению сущности права на неприкосновенность частной жизни, можно сделать вывод о том, что эта правовая категория имеет сложносоставной комплексный характер. Однако общим сходством большинства авторских концепций является то, что неприкосновенность частной жизни индивида основана на его свободе распоряжаться информацией о себе. Это подтверждается позицией Европейского суда по правам человека (ЕСПЧ) «Частная жизнь — это широкое понятие, которому невозможно дать исчерпывающее определение»[25], но, несмотря на это, ЕСПЧ выработал ряд подходов к этой теме, которые успешно применяет на практике. «Понятие частной жизни не ограничивается “внутренним миром”, в котором человек может жить своей собственной, личной жизнью, по своему желанию, полностью исключив из него внешний мир. Уважение частной жизни должно также в определенной мере предполагать право на установление и развитие отношений с другими людьми… Учитывая

очень широкий спектр вопросов, который охватывает частная жизнь, дела, подпадающие под это понятие, сгруппированы в три широкие категории (которые иногда частично совпадают), чтобы дать возможность провести определенную классификацию, а именно: i) физическая, психологическая или моральная

[24] См.: Авакьян С. А. Конституционное право России. Учебный курс: учеб. пособие: в 2т. — 5*е изд., перераб. и доп. — М.:Норма : ИНФРА*М, 2014. — с.675.
[25] См.: п.46, ст. 8 Европейской конвенции по правам человека. // European Court of Human Rights : [Электронный ресурс]. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_rus (дата обращения: 07.20.23).

неприкосновенность; ii) неприкосновенность частной жизни; iii) идентичность»[26]. Однако, несмотря на сложности, которые связаны с толкованием смысла «права на защиту конфиденциальности информации о частной жизни», специалистами Европейского Суда по правам человека были выделены его главные особенности, что позволяет обеспечить защиту неприкосновенности частной жизни при обращении в ЕСПЧ. Важность вопроса подчёркивается тем обстоятельством, что, как известно, практически все современные государства в своём конституционном развитии пришли к настоятельной необходимости закрепить принципы защиты информации о личности на уровне своих Конституций. В этом и выражается институциональная и конституциональная ценность института защиты персональных данных как важного элемента системы обеспечения защиты прав и свобод человека. В частности, в Основном законе ФРГ гарантируются права человека и неприкосновенность личности[27]. В Конституции Италии в ч.1 ст.15 закреплена «ненарушаемость всех форм общения»[28], в Греции Конституция устанавливает неприкосновенность частной жизни через иммунитет жилища, неприкосновенность личной и семейной жизни[29]. Швейцарская Конституция в ст. 13 провозглашает, что: «1. Каждое лицо имеет право на уважение его частной и семейной жизни, его жилища, а также его переписки, почтовой и телесвязи. 2. Каждое лицо имеет право на защиту от злоупотребления его личными данными».[30] В Японии Конституция также устанавливает в ст.17 и ст. 97 «вечность и

[26] См.: п.48, Руководство по применению статьи 8 Европейской конвенции по правам человека. // European Court of Human Rights : [Электронный ресурс]. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_rus (дата обращения: 07.20.23).
[27] См.: Основной закон для Федеративной Республики Германия (Grundgesetz für die Bundesrepublik Deutschland) от 23.05.1949 23.05.1949 г. — с изм. и допол. в ред. от 19.12.2022. // Федеральный центр политического просвещения : [Электронный ресурс]. URL: http://www.recht-harmonisch.de/GG-russisch.pdf (дата обращения: 21.09.23).
[28] См.: Конституция Итальянской Республики "Costituzione della Repubblica Italiana" от 1.01.1948 г. с изм. и допол. в ред. от 26.09.2023 // Senato della Repubblica : [Электронный ресурс]. URL: https://www.senato.it/sites/default/files/media-documents/Costituzione_RUSSO.pdf (дата обращения: 29.09.23).
[29] См.: Конституция Греческой Республики "Το Σύνταγμα της Ελλάδας" от 11.06.1975 г. с изм. и допол. в ред. от 2008 г. // WIPO : [Электронный ресурс].. URL: https://www.wipo.int/wipolex/en/legislation/details/9463 (дата обращения: 29.09.23), (пер.: Яндекс-переводчик).
[30] См.: Федеральная Конституция Швейцарской конфедерации "Federal Constitution of the Swiss Confederation" от 18.04.1999 г. с изм. и допол. в ред. от 13.02.2022 г. // Swiss Right: [Электронный ресурс]. URL: https://www.swissrights.ch/gesetze/uebersicht.php?buch=BV&jahr=2024&lg=EN (дата обращения: 30.09.23) , (пер.: Яндекс-переводчик).

нерушимость»[31] основных прав человека. Таким образом, в той или иной степени, право на защиту неприкосновенности частной жизни в разных формах закреплено практически во всех конституциях мира, что особенным образом подчёркивает значимость защиты этого права.

Что касается отечественного опыта в вопросе определения правового смысла права на защиту частной жизни, то Конституционный Суд Российской Федерации придерживается следующей позиции: «…право на неприкосновенность частной жизни, личную и семейную тайну означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера»[32]. В результате рассмотрения многообразия подходов к трактовке права на неприкосновенность частной жизни проведённый анализ позволяет заключить, что фундаментальную основу данного права составляет свобода индивида в управлении информацией личного характера. Эволюция права на невмешательство в частную жизнь свидетельствует о том, что его неоднозначная правовая природа поставила перед юридической доктриной задачу выработки эффективных регуляторных моделей, способных гарантировать защиту информации о частной жизни индивида.

В условиях интенсификации процессов становления информационного общества и автоматизации хранения данных о физических лицах, а также с развитием банковского сектора и сферы финансовых услуг, обострилась проблематика правовой защиты идентификационной информации, относящейся к персональным данным физического лица[33]; а именно особую роль в регулировании защиты персональных данных сыграл рост рынка кредитования населения и появление способов дистанционного управления банковским счётом. Важным

[31] См.: Конституция Японии "日本国憲法" от 3 ноября 1946 г // Prime Minister of Japan and His Cabinet : [Электронный ресурс]. URL: https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html(дата обращения: 30.09.23), (пер.: Яндекс-переводчик).

[32] См.: Постановление Конституционного Суда РФ от 16.06.2015 № 15-П "По делу о проверке конституционности положений статьи 139 Семейного кодекса Российской Федерации и статьи 47 Федерального закона "Об актах гражданского состояния" в связи с жалобой граждан Г. Ф. Грубич и Т. Г. Гущиной"// "Вестник Конституционного Суда РФ", № 5, 2015.

[33] См.: Бачило И. Л. Правовое обустройство информационной действительности: проблемы и перспективы / И. Л. Бачило, П. У. Кузнецова // Российский юридический журнал. — 2008. — № 5(62). — С. 15–25.

аспектом развития рынка кредитования является наличие у кредитной организации актуальной информации о получателе кредита. Именно необходимость в обеспечении обмена актуальной и достоверной информацией между финансовыми и кредитными организациями о физических лицах стала одним из основных факторов, способствовавших выработке правовых подходов к регулированию обработки информации о физических лицах. Важной задачей, связанной с хранением и обработкой финансовой информации об индивидуумах, является защита права на неприкосновенность частной жизни. Для решения этих двух непростых правовых задач, развитые страны в середине прошлого века начали изменять своё законодательство. В 70-х годах прошлого века стали появляется национальные нормативно-правовые акты, которые регулировали хранение, передачу и обработку информации о физических лицах.

В США сначала появился федеральный закон «О добросовестном предоставлении кредитной информации» (Fair Credit Reporting Act)[34], который регулировал обмен кредитными досье физических лиц (принят в 1970 году), этот документ был призван обеспечить то, чтобы агентства по предоставлению кредитной отчётности «выполняли свою функцию по сбору и оценке информации о потребительских кредитах честно, беспристрастно и с уважением права потребителя на неприкосновенность частной жизни»[35]. В дальнейшем потребность в обмене информации о физических лицах стала ещё более актуальной, особенно для государственных органов. В связи с этим, перед юридической наукой того времени возникла задача, связанная с защитой права на неприкосновенность частной жизни в условиях изменяющихся общественных отношений. А поскольку это право достаточно неоднозначно, то юридическая наука вынуждена была выработать более формальные подходы к регулированию обработки информации, относящейся к личной жизни индивидуума. В 1974 году в США был принят «Закон

[34] См.: Fair Credit Reporting Act // Federal Trade Comisson : [Электронный ресурс]. URL https://www.ftc.gov/system/files/ftc_gov/pdf/fcra-may2023-508.pdf (дата обращения: 30.09.23.
[35] См.: USA: Data Protection in the Financial Sector // Data Guidance : [Электронный ресурс]. URL https://www.dataguidance.com/opinion/usa-data-protection-financial-sector (дата обращения: 30.09.23).

о невмешательстве в частную жизнь граждан» (Privacy Act)[36]. Этот документ «был принят в ответ на опасения по поводу того, как создание и использование компьютеризированных баз данных может повлиять на права частных лиц на неприкосновенность частной жизни. Он защищает неприкосновенность частной жизни путем установления четырех процедурных и материальных прав в отношении персональных данных. Во-первых, он требует, чтобы правительственные учреждения показывали физическому лицу любые записи, хранящиеся на него или нее. Во-вторых, он требует, чтобы агентства придерживались определенных принципов, называемых “добросовестной информационной практикой”, при сборе и обработке персональных данных. В-третьих, он накладывает ограничения на то, как агентства могут делиться данными физического лица с другими людьми и агентствами. В-четвертых, он позволяет частным лицам подавать в суд на правительство за нарушение его положений».[37]

Введение новой правовой дефиниции позволило обеспечить защиту неприкосновенности частной жизни индивида путём создания особого правового режима для конфиденциальной информации, относящейся к частной жизни физического лица, включая и автоматизированную обработку таких данных.

С развитием информационных технологий и юридической науки появился институт защиты персональных данных, фундамент которого составило право человека на защиту своих конституционных прав и свобод, эта проблематика подробно рассмотрена в научной литературе[38]. А. В. Морозов характеризует взаимосвязь персональных данных и права на неприкосновенность частной жизни так: «Персональные данные как институт охраны права на неприкосновенность частной жизни и идентификации лица в социально-экономической, политической и культурной жизни общества»[39]. Исходя из чего, следует вывод о том, что основой

[36] См.: Privacy Act // Gerald R. Ford Presidential Library & Museum : [Электронный ресурс]. URL https://www.fordlibrarymuseum.gov/library/document/0055/12006251.pdf (дата обращения: 30.09.23).
[37] См.: The Privacy Act of 1974 // EPIC : [Электронный ресурс]. URL : https://epic.org/the-privacy-act-of-1974/ (дата обращения: 30.09.23).
[38] См.: Копылов В. А. Информационное право: учебник. — 2-е, перераб. и доп изд. — Москва: Юристъ, 2005. — 510 с.
[39] См.: Морозов, А. В. Информационное право и информационная безопасность. Часть 1 : учебник для магистров и аспирантов / А. В. Морозов, Л. В. Филатова, Т. А. Полякова. — Москва, Саратов : Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. — 604 с.

института защиты персональных данных послужило именно право человека на неприкосновенность частной жизни и защиту информации о ней.

Отличие этих правовых институтов в том, что защита персональных данных в правовом смысле значительно более формализована, она имеет свой разработанный понятийный аппарат, принципы и требования защиты и обработки, а также другие чёткие юридические конструкции, в то время как неприкосновенность частной жизни значительно менее формализована. Рассматривая международные источники права, стоит отметить, что в «Конвенции о защите физических лиц при автоматизированной обработке персональных данных» в качестве предмета и цели зафиксировано «уважение его прав и основных свобод, и в частности его права на неприкосновенность частной жизни, в отношении автоматизированной обработки касающихся его персональных данных (“защита данных”)»[40].

Рассмотрение вопросов защиты прав человека в контексте наступления «цифровой эпохи»[41] через призму положений Конституции Российской Федерации требует обращения к аучным работам и позиции юристов в данной сфере: «Но очевидно, что вопрос обеспечения прав и свобод человека в цифровом мире гораздо глубже и шире, чем задачи идентификации пользователей, безопасности личных данных или даже защиты граждан от киберпреступлений. В цифровом мире, как и в реальном, должны соблюдаться основные конституционные права и свободы человека и гражданина. В первую очередь речь идёт о правах, закреплённых в ст. 19, 22–24, 29, 44 Конституции Российской Федерации»[42]. Можно отметить, что текст Конституции нашей страны, несмотря на развитие технологий и время, по-прежнему актуален и можно сказать о том, что его авторы смогли сформулировать положения Конституции таким образом, что даже несмотря на прошедшие десятилетия, закреплённые в ней нормы, в том числе, и связанные с правами

[40] См.: Конвенция о защите физических лиц при автоматизированной обработке персональных данных // Собрание законодательства РФ, 03.02.2014, № 5, ст. 419.
[41] См.: digital age. // Cambridge University : [Электронный ресурс]. URL: https://dictionary.cambridge.org/dictionary/english/digital-age (дата обращения: 29.09.23).
[42] См.: Шахрай С. М. Цифровая конституция. основные права и свободы личности в тотально информационном обществе // Вестник Российской академии наук. — 2018. — Т. 88, № 12. — С. 1075–1082.

человека, по-прежнему актуальны, и не требуют корректировок, в отличие от норм федеральных законов[43].

Изучая отечественное законодательство в контексте соотношения права на неприкосновенность частной жизни и права на защиту персональных данных, следует обратиться к формулировке, закреплённой в Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее — Закон о персональных данных): «Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну»[44]. С научной точки зрения взаимосвязь между категориями «персональные данные» и «право на защиту информации о личной жизни» является установленной и не вызывает концептуальных разногласий. Однако более точных юридических формул, характеризующих правовые подходы к определению соотношения персональных данных и информации о частной жизни физического лица, в российском законодательстве не имеется. Указанная ситуация может приводить к затруднениям при определении конкретных случаев, в которых доступ к персональным данным сопряжён с затрагиванием сведений о частной жизни субъекта.

Особенно это актуально в условиях глобальной цифровизации, когда «активность человека в электронной среде, пользование интернет ресурсами и иными технологиями оставляет его “цифровой след” — совокупность информации, размещаемой пользователем о себе в сети Интернет. Такая информация может в себе содержать различные аспекты частной жизни самого человека (фотографии, личные видео, аудиозаписи, документы, аккаунты в социальных сетях, платежных и других интернет-сервисах), доступна неограниченному кругу лиц в сети Интернет»[45]. Следовательно, можно констатировать, что с течением времени и

[43] См. подробнее: Сапронов Д.Ю. К вопросу об эволюции правового института защиты персональных данных // Вестник Российской правовой академии. — 2025. — № 6. – С.83-95.
[44] См.: Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" // "Собрание законодательства РФ", 31.07.2006, № 31 (1 ч.), ст. 3451
[45] См.: Велиева Д. С. Право на неприкосновенность частной жизни и проблемы его обеспечения в условиях развития цифровых технологий // Права человека: история, теория, практика: сборник научных статей. — Курск: Университетская книга, 2022. — С. 16–22.

развитием информационных технологий, грань между персональными данными и информацией о частной жизни как правовыми категориями стала более размытой. На это повлияло и то, что со временем у человека стал появляться «цифровой след», по которому не только можно получить информацию о его частной жизни, но также доступ к его персональным данным. Этот феномен далее подробно будет рассмотрен в работе. Исследуя это явление с правовых позиций, следует обратиться к определению персональных данных, которое дал законодатель — «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»[46], однако в условиях, когда развитие информационно-аналитических технологий достигло значительных высот, перечень информации, которую теперь можно отнести к персональным данным значительно расширился. Существенное влияние на развитие ситуации оказала автоматизация процессов обработки персональных данных, позволившая обеспечить мгновенный доступ к необходимой информации. Согласно оценкам специалистов, в настоящее время идентификация личности может быть осуществлена даже с использованием косвенных данных: «Никнейм, имя-фамилия, дата рождения, телефон, адрес, образование, служба, ИНН (SSN), и т.д. Чаще известно лишь что-то одно, но зачастую этого достаточно чтобы начать»[47]. Именно такая информация и различные идентификаторы физического лица являются теми «крошками», позволяющими определить индивида, к которому они относятся. В современном мире их достаточно много, начиная с номера мобильного телефона или IP-адреса в сети Интернет и заканчивая идентификаторами в различных программах обмена мгновенными сообщениями. Особенную роль в современном мире играет номер мобильного телефона, который со временем стал не только использоваться для адресации при использовании сотовой связи, а превратился в один из способов идентификации физических лиц в Интернет пространстве. Вот что об этом говорят сотовые операторы связи:

[46] См.: Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. — 2006. — № 31 (ч. I). — ст. 3451.
[47] См.: Как найти аккаунты и личные данные человека в сети Деанон по открытым источникам // Вастрик Блог : [Электронный ресурс] URL: https://vas3k.blog/blog/389/ (дата обращения: 7.10.23).

«…мобильный ID позволяет заходить только по номеру телефона, а все остальные данные о пользователе — ФИО, дата рождения и место регистрации — уже хранятся у оператора связи. А в некоторых случаях не придется даже вводить и номер»[48]. Отсюда следует, что с развитием цифровых сервисов и информационных технологий, различные данные, относящиеся к физическому лицу, изначально не позволявшие достоверно установить его личность, трансформировались в идентификаторы, которые позволяют однозначно идентифицировать физическое лицо. Особенно этому способствуют периодические утечки данных у операторов сотовой связи и других организаций, где в большинстве случаев содержится номер мобильного телефона.

Рассматривая правовое определение «персональные данные», следует обратить внимание на развитие автоматизированных информационных технологий, которые дают возможность используя косвенную информацию о физическом лице, с высокой точностью его идентифицировать. Этот факт оказал серьёзное влияние на общественные отношения, касающиеся персональных данных. С течением времени сама сущность персональных данных стала претерпевать изменения, что потребовало обратить внимание на актуализацию понятийного аппарата в рассматриваемой области, о чём пишут некоторые исследователи в своих работах[49].

Для решения этой задачи следует рассмотреть вопрос совершенствования правового определения понятия «персональные данные» с опорой на изменения в общественных отношениях и появление новых информационных технологий. С учётом всего вышеизложенного предлагается определить правовое понятие «персональные данные» как — документированную (электронно и\или неэлектронно) информацию, относящуюся прямо или косвенно, к определенному или определяемому физическому лицу (субъекту персональных данных), позволяющую его идентифицировать полностью или частично, в том числе с

[48] См.: Токарев А. Телефон вместо почты: как развивается авторизация через мобильный ID // РБК : [Электронный ресурс].Тренды URL: https://trends.rbc.ru/trends/industry/cmrm/62cea5f69a79478c4a42cd63 (дата обращения: 7.10.23).
[49] См.: Бундин М. В. Персональные данные в системе информации ограниченного доступа, Специальность: 12.00.13 — информационное право, диссертация на соискание ученой степени кандидата юридических наук, 2017 год, URL: https://izak.ru/upload/iblock/a61/a61916d1bf3c94d110fd287137213345.pdf (дата обращения: 7.10.23).

применением автоматизированных и неавтоматизированных информационных технологий. Такая формулировка более полно раскрывает сущность понятия «персональные данные» в условиях наступления «цифровой эры», что позволит вывести их защиту на более высокий уровень, и повысить её эффективность, а также будет способствовать решению задачи приведения понятийного аппарата в рассматриваемой области в соответствие с реалиями и задачами информационно-правового регулирования обработки персональных данных. Говоря о правовом определении персональных данных, юридической науке возможно следует рассмотреть вопрос двух контуров регулирования их обработки: первый контур, когда информация о физическом лице документирована на не электронном (бумажном) носителе, и второй контур, в ситуации когда персональные данные обрабатываются в электронном виде. Этот вопрос является в достаточной степени дискуссионным и требует детального исследования юридической наукой.

Помимо традиционных персональных данных в течение времени стало возможно выделить группу характеристик индивидуума, по которым можно определить его личность, используя для этого параметры его физического тела. Эта информация стала называться биометрической. Вот как её характеризуют исследователи: «Биометрические данные (признаки, свойства) личности являются уникальными для каждого человека и подразделяются на анатомические (физиологические) и функциональные (поведенческие)»[50]. К анатомическим, или как их ещё иногда называют «статическим», относят: дактилоскопическую информацию, геометрию лица, запись голоса, геометрию ладони и др., т.е. те данные, которые неизменны или слабо подвержены изменениями на протяжении всей жизни человека. К функциональным же биометрическим параметрам относятся параметры, которые характеризует «уникальное поведение и подсознательные движения человека в процессе воспроизведения каких-либо действий»[51]. К ним можно отнести кинематику тела, особенности голоса, оценку

[50] См.: Степкина Ю. С., Яворский М. А. Анализ динамических методов идентификации личности // Актуальные проблемы правоведения. 2022. № 3 (75). С. 28–31.
[51] См.: Что такое поведенческая биометрия и кто применяет её на российском рынке. // Рамблер.Новости : [Электронный ресурс]. URL: https://news.rambler.ru/other/41803543-chto-takoe-povedencheskaya-biometriya-i-kto-primenyaet-ee-na-rossiyskom-rynke/ (дата обращения: 9.10.23).

позы, анализ уникальных привычек и т.д. Применение поведенческой биометрии позволяет определить нетипичные состояния индивидуума и помогает повысить точность идентификации физического лица по биометрическим персональным данным. В соответствии со статьёй 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», «биометрические данные — это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность», однако, как отмечалось ранее, методы биометрической идентификации личности обладают более широким спектром возможностей. Современные технические возможности биометрической идентификации позволяют использовать значительно более широкий набор параметров для установления личности, чем это предусмотрено нормативными актами. Данный факт становится предметом активного обсуждения в среде юристов-исследователей, фокусирующихся на вопросах правового регулирования обработки биометрических данных[52]. Проведённый анализ показывает, что существующая юридическая трактовка понятия «биометрические данные» не в полной мере отражает сущность регулируемых правоотношений в сфере обработки биометрической информации. Требуется её концептуальное уточнение. Следовательно, биометрические персональные данные можно определить как информацию, составляющую совокупность физических, физиологических и\или поведенческих признаков физического лица, используя которую, оператор может выполнить однозначную идентификацию его личности. Такое определение биометрической информации о человеке позволит более полно, и в соответствии с реалиями и задачами осуществлять правовое регулирование обработки биометрии. Возможно целесообразно внести в дополнение к имеющемуся определению внести более широкое определение биометрических данных физического лица — биометрические персональные данные.

Исходя из всего вышесказанного, можно сделать вывод о том, что становление института защиты персональных данных заняло достаточно

[52] См.: Афанасьев С. Д. Биометрическая идентификация и права человека: демаркационная линия / С. Д. Афанасьев, И. А. Терещенко, Д. А. Яцкевич // Закон. – 2022. – № 3. – С. 33-46.

длительное время и в его основе лежит неотъемлемое право индивидуума на защиту информации о своей частной жизни. Развитие информационно-коммуникационных технологий и их повсеместное распространение привели к появлению многочисленных электронных (цифровых) идентификаторов человека в информационном пространстве, с помощью которых стало возможно провести полное или частичное определение личности человека и в реальном мире. В некоторых случаях они стали вытеснять паспортные или иные аналогичные привычные идентификационные данные, традиционно служащие для определения личности физического лица. Всё это в определённой степени повлияло на общественные отношения в области обработки персональных данных, что потребовало актуализации понятийного аппарата института правовой защиты персональных данных, по причине того, что закреплённые в законодательстве формулировки некоторых определений в рассматриваемой области перестали отвечать реалиям и задачам информационно-правового регулирования обработки персональных данных. Актуализация указанных положений будет способствовать повышению полноты и эффективности правового регулирования обработки персональных данных на территории Российской Федерации.

§ 1.2 Становление, особенности и состояние информационно-правового регулирования обработки персональных данных в Российской Федерации

Системное и последовательное исследование вопроса эволюции правового института защиты персональных данных физических лиц в России невозможно без учёта особенностей, присущих различным этапам развития российской государственности, потому что в отличие от других европейских государств, политический режим в России за относительно небольшие, в историческом понимании, промежутки времени, претерпевал фундаментальные изменения. И каждое такое изменение коренным образом влияло, в том числе, и на правовую доктрину государства. Кардинально менялись правовые подходы к обеспечению защиты прав человека, менялись приоритеты в отношении интересов личности и государства. Именно поэтому, перед тем как приступить к анализу современного

института персональных данных, нужно рассмотреть исторический аспект его формирования и становления в нашей стране. Изначально понятия «персональные данные» не существовало, институт защиты персональных данных появился в процессе эволюции прав человека, а именно, права на защиту информации о частной жизни.

История этого вопроса в России началась ещё в 1857 году, с принятием, и вступлением в силу несколькими годами ранее, Почтового и Телеграфного[53] уставов, которые защищали тайну частной жизни. Наказание за нарушение предусматривало уголовную ответственность в соответствии с действовавшим тогда Уголовным уложением. Революция 1917 года и отмена всех действующих законов повлекла за собой полную трансформацию российского права. Что на более чем полвека практически заморозило развитие юридической науки в России в этом направлении.

В первой Конституции РСФСР 1918 года был раздел, посвящённый правам «…трудящегося и эксплуатируемого народа»[54], однако в то неспокойное, военное время правам человека и защите персональных данных внимания не уделялось по причине того, что военный коммунизм исключал любой индивидуализм. Конституция СССР 1924 года не содержала раздела, посвящённого правам человека[55]. В основном законе РСФСР 1925 года защита частной жизни также закреплена не была[56]. В Конституции СССР 1936 года в статьях 127–128 закреплялись права гражданина на неприкосновенность личности, жилища и переписки[57]. Закрепление в основном законе этих норм стало значительным достижением молодой советской юридической науки в направлении охраны и защиты неприкосновенности личной жизни граждан. Однако, что касается

[53] См.: Свод законов Российской империи. Том двенадцатый. Часть I. Уставы путей сообщения, почтовый, телеграфический, строительный, и пожарный — 1857–1868 — Тип. Второго Отделения Собственной Е.И.В.Канцелярии — 664 с.
[54] См.: Конституция (Основной Закон) Российской Социалистической Федеративной Советской Республики. Принята V Всероссийским съездом Советов 10 июля 1918 года // СУ РСФСР. 1918.
[55] См.: Текст Конституции СССР 1924 г. // История Советской Конституции в документах. — М., 1957.
[56] См.: Конституция РСФСР 1925 // История советской Конституции (в документах) 1917–1956. М:. Юрид. лит.,1957.
[57] См.: Равин С. М. Три конституции Советского государства (1918–1924–1936 гг.) // С. Равин. — Л. : Изд-во Леноблисполкома и Ленсовета, 1937. — 79, [1] с.

соблюдения этих норм, то они носили декларативный характер. С началом Великой Отечественной войны вопрос защиты неприкосновенности личной жизни не ставился вовсе.

Лишь после ратификации «Пакта о гражданских и политических правах», и интеграции его принципов в новую Конституцию СССР, в 1977 году в ней появилась норма: «Уважение личности, охрана прав и свобод граждан — обязанность всех государственных органов, общественных организаций и должностных лиц»[58]. Внесение в Основной закон Советского Союза этой нормы можно рассматривать как одно из наиболее важных достижений советской юридической науки, ознаменовавших отход от принципа доминирования интересов государства над правами и свободами граждан.

Выделение неприкосновенности личной жизни как самостоятельной ценности в российской юридической науке произошло после 1991 года. «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются, за исключением случаев, указанных в законе»[59] — эта формула была зафиксирована в статье 9 «Декларации о правах и свободах человека и гражданина», принятой Верховным советом РСФСР 22 ноября 1991 года. В дальнейшем именно такая же формула была закреплена в ст.24 Конституции Российской Федерации. Однако дальнейшей правовой конкретизации в российском законодательстве не получила, как и соотношение понятий «частная жизнь» и «персональные данные».

В 1995 году был принят Федеральный закон от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации»[60], он действовал по 08.08.2006 г. В этом нормативном акте впервые на федеральном уровне было закреплено понятие персональных данных посредством термина «информация о

[58] См.: Конституция СССР 1977 года // Сборник нормативных актов по советскому государственному праву. М.: Юрид. лит., 1984. С. 179–194.
[59] См.: Постановление ВС РСФСР от 22 ноября 1991 г. N 1920-1 "О Декларации прав и свобод человека и гражданина" // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации от 26 декабря 1991 г., № 52, ст. 1865.
[60] См.: Федеральный закон от 20.02.1995 № 24-ФЗ ред. от 10.01.2003 "Об информации, информатизации и защите информации" // Собрание законодательства РФ, 20.02.1995, № 8, ст. 609.

гражданах (персональные данные) — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность»[61]. Правовой режим информации о гражданах был закреплён в статье 11 федерального закона. Требования к получению и обработке персональных данных характеризовались следующими основными условиями:

— персональные данные относятся к конфиденциальной информации;

— запрет на сбор информации о частной жизни без согласия владельца, за исключением случаев, когда получено разрешение суда;

— запрет на использование информации о частной жизни граждан с целью причинения вреда и ограничения прав;

— устанавливается ответственность юридических и физических лиц за нарушение режимов обработки, хранения персональных данных и порядка их использования.

— оговаривается право граждан на доступ к документированной информации о себе и данных о её использовании (статья 14);

— устанавливается требование защиты персональных данных (статья 21).

Среди недостатков, действовавшего тогда Федерального закона, можно отметить отсутствие требований к форме согласия на сбор персональных данных, отсутствие определения понятия «оператор персональных данных», а также отсутствие конкретизации соотношения понятий «частная жизнь», «персональные данные» и т. д.

В 2005 году была ратифицирована конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных»[62]. Ратификация этой конвенции обозначила необходимость адаптации российского законодательства в сфере регулирования персональных данных. Также одной из важных предпосылок принятия закона «О персональных данных» стала

[61] См.: Федеральный Закон РФ от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» // Собрание законодательства РФ, 20.02.1995, № 8, ст. 609.
[62] См.: «О защите физических лиц при автоматизированной обработке персональных данных». // Официальный интернет-портал правовой информации: [Электронный ресурс]. URL: http://www.pravo.gov.ru (дата обращения: 13.10.23).

необходимость более полно регулировать сферу обработки персональных данных и их защиту.

В 2006 году был принят, и в январе 2007 года вступил в силу, Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее — Закон, Закон о персональных данных). В нём устанавливались определения понятий «персональные данные», «оператор персональных данных», «обработка персональных данных» и другие дефиниции, которые необходимо было ввести в правовом поле. Кроме того, в Законе был закреплен и формализован подход, содержащийся в статье 24 Конституции Российской Федерации, что для получения и обработки персональных данных требуется письменное согласие их владельца, кроме определённых случаев, перечень которых приведён в статье 6 Федерального закона. Со вступлением в силу Закона о персональных данных обработка такой информации стала проводиться по единым принципам и стандартизированной процедуре. Это позволило в значительной степени урегулировать отношения, связанные с персональными данными.

Однако некоторая часть вопросов остаётся не урегулирована, например, как замечает Е. А. Войниканис — «в законодательстве отсутствует устоявшееся толкование понятий «сведения о частной жизни лица», «личная тайна», «семейная тайна», а также единый взгляд на их соотношение с понятием «персональные данные»»[63]. Другие юристы обращают внимание на проблемы, связанные с «обработкой обезличенных данных, специальных категорий персональных данных, личной информации умерших людей и незначительности штрафных санкций за нарушения в области обработки персональных данных»[64], кроме этого, в юридической литературе поднимается проблема регулирования персональных данных умерших[65]. Ещё одна проблема, которую отмечают в своих научных

[63] См.: Войниканис Е. А., Машукова Е. О., Степанов-Егиянц В. Г. Неприкосновенность частной жизни, персональные данные и ответственность за незаконные сбор и распространение сведений о частной жизни и персональных данных: проблемы совершенствования законодательства // Законодательство. 2014. № 12. С. 74–80.
[64] См.: Трофимцева С. Ю. К вопросу об обеспечении защиты персональных данных в России // Сборники конференций НИЦ «Социосфера». 2014. № 63. С. 120-125.
[65] См.: Ишеков К. А. Гражданско-правовое регулирование института персональных данных умерших в современной России / К. А. Ишеков, Д. С. Холопцев // Вестник Российской правовой академии. —2022. — № 1. — С. 76–81.

работах отечественные юристы, это случаи «изменения режима персональных данных, когда сначала владелец делает их общедоступными, а затем вновь ограничивает к ним доступ или случаев, когда социальные сети могут в одностороннем порядке менять степень приватности персональных данных зарегистрированных пользователей»[66]. Можно констатировать, что, несмотря на значительные изменения, которые со временем претерпело российское законодательство в области персональных данных, оно всё ещё требует постоянного совершенствования и актуализации. К примеру, проблема с отсутствием правового определения информации о частной жизни в российском законодательстве так и не решена, также не дано правовое толкование соотношения понятий «информация о частной жизни» и «персональные данные». Развитие и повсеместное внедрение информационно-коммуникационных технологий привели к размытию грани между частной жизнью и персональными данными; например, бурный рост электронной коммерции стал одним из факторов, повлиявших на увеличение объёмов автоматизированной обработки персональных данных. Отсюда следует, что для эффективной правовой защиты информации о частной жизни и персональных данных, необходимо более чётко обозначить правовую связность этих понятий. Как отмечают некоторые российские юристы[67] в своих исследованиях, два правовых режима существуют независимо друг от друга: в ГК РФ и Федеральном законе № 152-ФЗ от 27 июля 2006 года «О персональных данных». Как отмечает в своих работах И. А. Михайлова — «феномен неприкосновенности частной жизни проявляется в том, что разрозненные персональные данные не всегда имеют отношение к частной жизни, но их систематизация и объединение в массивы порождают социально-экономическую характеристику субъекта»[68]. В контексте активного развития аналитических систем обработки данных и нейросетевых технологий

[66] См.: Алексашин М. Н. Защита персональных данных как условие обеспечения безопасности личности // Право и безопасность.2014. № 1. С. 68–73.
[67] См.: Савельев А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М.: Статут, 2017. 164 с.
[68] См.: Михайлова И. А. Персональные данные и их правовая охрана: некоторые проблемы теории и практики // Законы России: опыт, анализ, практика: правовой журнал. 2017. — № 10. — С. 11–19.

значение этого аспекта возрастает, так как эти технологии позволяют проводить многофакторный анализ данных и широко применяются в маркетинге[69]. Это позволяет выявлять те или иные пристрастия человека, а также прогнозировать его поведение, что позволяет продавать эту информацию всем заинтересованным[70] лицам. Таким образом, можно рассматривать персональные данные и информацию о личной жизни и права на их защиту, как частное и общее. Однако же, в действующем законодательстве эти понятия достаточно слабо увязаны. Такой подход не позволяет выстроить эффективную систему правовой защиты информации о частной жизни и персональных данных.

Закон о персональных данных был ориентирован на ручную обработку информации о физических лицах, а не на автоматизированную; в настоящее время именно цифровизация обработки данных о физических лицах стала преобладать над ручными методами, что привело к снижению уровня защищённости персональных данных и обозначило необходимость разработки новых подходов к построению системы правовой защиты идентификационной информации физических лиц. В своих работах специалисты по информационному праву отмечают: «Важно учитывать, что указанные мероприятия требуют не внесения точечных изменений, а направлены на системное и обоснованное формирование правовых и регуляторных условий для развития цифровой экономики, что требует фундаментальных правовых исследований, прежде всего в области правового обеспечения информационной безопасности»[71].

Современные информационные и компьютерные технологии достигли такого уровня, что многие процессы, которые выполнялись вручную, стали автоматизироваться; не избежала этого и обработка персональных данных. Развитие глобальной сети Интернет стало причиной возникновения ряда последствий, в том числе привело к тому, что множество привычных для обычного

[69] См.: Использование персональных данных в маркетинге: законы и этика // РБК Тренды : [Электронный ресурс] URL: https://trends.rbc.ru/trends/industry/615fdf6f9a794719ca4d1ddc (дата обращения: 1.10.23).
[70] См.: Тотальная слежка: как устроен рынок торговли пользовательскими данными: [Электронный ресурс] // РБК. URL: https://www.rbc.ru/magazine/2018/04/5aafdfc99a7947654297214d (дата обращения: 1.10.23)
[71] См.: Полякова Т. А., Минбалеев А. В., Бойченко И. С. Концептуальные подходы к правовому регулированию информационной безопасности в условиях цифровизации и трансформации права // Вестник УрФО. Безопасность в информационной сфере. — 2019. — № 3 (33). — С. 64–68.

человека сервисов стало использовать её для взаимодействия с конечным потребителем, особенно на это повлияла эпидемия COVID-19. Современное развитие информационно-коммуникационных технологий привело к тому, что появились так называемые «цифровые права». Вот что о них говорит В. Д. Зорькин: «Цифровизация социальной жизни привела к появлению ранее неизвестных, так называемых, цифровых, прав. Под цифровыми правами понимаются права людей на доступ, использование, создание и публикацию цифровых произведений, на доступ и использование компьютеров и иных электронных устройств, а также коммуникационных сетей, в частности к сети интернет»[72]. Эти права стали неотъемлемой частью повседневной жизни граждан. Важную роль при их реализации играет идентификация личности в Интернет-пространстве, которая необходима для получения различных услуг и доступа к сервисам. Помимо распространения таких сервисов как аренда машины, заказ еды, приобретение различных товаров, появилась возможность совершать юридически значимые действия, используя современные технологии[73]. Современные информационные и компьютерные технологии достигли такого уровня, что необходимость модернизации национальной системы права стала важным условием дальнейшего эффективного развития государства. В результате появления цифровой составляющей у социальных отношений и перехода многих процессов из реального пространства в виртуальное, полностью или частично, возникла необходимость внесения изменений в действующее законодательство с целью более полного соответствия его положений новым вызовам.

Неслучайно в ходе Петербургского международного экономического форума 2017[74], Президент подчеркивал — «необходимо сформировать принципиально

[72] См.: Зорькин: Задача государства — признавать и защищать цифровые права граждан // Российская газета : [Электронный ресурс]. URL: https://rg.ru/2018/05/29/zorkin-zadacha-gosudarstva-priznavat-i-zashchishchat-cifrovye-prava-grazhdan.html (дата обращения: 1.10.23).

[73] См.: Применение электронной подписи. // ФНС России : [Электронный ресурс]. – URL: https://www.nalog.gov.ru/rn77/related_activities/el_doc/use_electronic_sign/ (дата обращения: 4.10.23).

[74] См. подробнее здесь и далее: Сапронов Д. Ю. Идентификация физических лиц в цифровую эпоху: информационно-правовые проблемы / Д. Ю. Сапронов // Третьи Бачиловские чтения. Цифровая трансформация: вызовы праву и векторы научных исследований : материалы Международной научно-практической конференции, Москва, 07 февраля 2020 года. – Москва: Общество с ограниченной ответственностью "Проспект", 2020. – С. 302-308.

новую, гибкую нормативную базу для внедрения цифровых технологий во все сферы жизни. При этом все решения должны приниматься с учетом обеспечения информационной безопасности государства, бизнеса и граждан»[75]. Проблемы развертывания цифровой экономики в последнее время находятся в фокусе внимания высшего политического руководства нашей страны. Цифровизация сделала множество вещей более доступными, но для того, чтобы ими воспользоваться, необходимо идентифицироваться в сервисе, предоставив свои персональные данные. Это в значительной степени повлияло на общественные отношения, связанные с обработкой персональных данных.

Во многих странах были приняты национальные программы цифровизации. Не стала исключением и Российская Федерация, в которой такая программа была принята в 2018 году, позднее она трансформировалась в национальный проект «Цифровая экономика Российской Федерации» [76], который завершился в 2025 году. Под влиянием цифровой трансформации народного хозяйства, стали меняться и социальные отношения, что потребовало совершенствования нормативной базы в этой области, поскольку имеющееся федеральное законодательство было ориентировано на неавтоматизированную обработку персональных данных. Поэтому в национальном проекте «Цифровая экономика Российской Федерации» было предусмотрено направление, которое связано с совершенствованием и адаптацией имеющегося законодательства к внедрению новых информационных технологий, «одной из задач программы является создание системы правового регулирования цифровой экономики, основанной на гибком подходе в каждой сфере. Реализации этой задачи был посвящен федеральный проект “Нормативное регулирование цифровой среды”, который курирует Министерство экономического развития Российской Федерации. Этот проект предусматривал разработку и принятие ряда нормативных правовых актов, направленных на снятие

[75] См.: Латухина К. Владимир Путин: Внедрить цифровые технологии во все сферы жизни. // Российская газета : [Электронный ресурс]. URL: https://rg.ru/2017/06/04/reg-szfo/vladimir-putin-vnedrit-cifrovye-tehnologii-vo-vse-sfery-zhizni.html (дата обращения: 4.10.23).

[76] См.: Опубликован паспорт национальной программы «Цифровая экономика Российской Федерации». // Официальный сайт Правительства Российской Федерации : [Электронный ресурс]. URL: http://government.ru/info/35568/ (дата обращения: 4.10.23).

первоочередных барьеров, которые препятствуют развитию цифровой экономики. Планируется также урегулировать сквозные технологии для различных отраслей законодательства, вопросы, связанные с идентификацией субъектов правоотношений в цифровой среде, электронным документооборотом, оборотом данных, в том числе персональных»[77], как в своих работах отмечает В. А. Северин, эта задача является новой[78] для юридического сообщества.

Национальный проект «Цифровая экономика Российской Федерации» предусматривал принятие значительного числа нормативных актов, связанных с идентификацией личности. Сюда можно отнести следующие инициативы: цифровой паспорт гражданина Российской Федерации[79], цифровой профиль гражданина Российской Федерации[80], единый регистр сведений о населении России[81] — перечисленные системы должны выполнять функции идентификации и аутентификации физических лиц. Однако стоит отметить важную особенность, связанную с тем, что каждая из этих систем самодостаточна и не предполагает интеграции с другими перечисленными информационными системами, например единый регистр сведений о населении России не предполагает, что в нём будет содержаться биометрическая информация[82]. В результате ввод в эксплуатацию нескольких несвязанных, или связанных опосредованно, информационных систем, которые предназначены для выполнения похожих, или одинаковых функций, окажет негативное влияние на безопасность персональных данных физических лиц и может породить еще большую избыточность хранения информации о физических лицах. Несогласованность данных, хранящихся в этих системах, может стать

[77] См.: Нормативное регулирование цифровой среды. // Министерство экономического развития Российской Федерации : [Электронный ресурс]. URL: https://www.economy.gov.ru/material/directions/gosudarstvennoe_upravlenie/normativnoe_regulirovanie_cifrovoy_sredy/ (дата обращения: 5.10.23).

[78] См.: Северин В. А. Правовые аспекты обеспечения информационной безопасности цифровой экономики // Пробелы в российском законодательстве. — 2023. — Т. 16, № 8. — С. 46–51.

[79] См.: Электронный паспорт гражданина РФ. // Комсомольская правда : [Электронный ресурс]. URL: https://www.kp.ru/putevoditel/zakony/ehlektronnyj-pasport-grazhdanina-rf/ (дата обращения: 5.10.23).

[80] См.: Цифровой профиль гражданина — что известно на сегодняшний день. // Экспертный центр электронного государства : [Электронный ресурс]. URL: https://d-russia.ru/tsifrovoj-profil-grazhdanina-chto-izvestno-na-segodnyashnij-den.html (дата обращения: 5.10.23).

[81] См.: Госдума приняла закон о едином регистре сведений о населении России. // ТАСС. URL: https://tass.ru/obschestvo/8527939 (дата обращения: 5.10.23).

[82] См.: Единый регистр сведений о населении РФ не будет содержать биометрических данных. // ТАСС : [Электронный ресурс]. URL: https://tass.ru/obschestvo/8657699 (дата обращения: 11.10.23).

причиной противоречий, когда сведения из одной системы не будут совпадать со сведениями из другой, что отрицательно может сказаться на идентификации физических лиц цифровыми средствами. Помимо всего прочего, наличие нескольких автоматизированных систем с одинаковым функционалом приведёт к излишнему расходу ресурсов на их разработку, реализацию и поддержание функционирования. С юридической точки зрения регулирование работы нескольких, не связанных друг с другом, систем федерального уровня, может представлять сложную задачу, по причине того, что правовое обеспечение функционирования этих систем будет не единообразным. Программа «Цифровая экономика Российской Федерации» обозначила потребность в модернизации правового регулирования защиты персональных данных путём системного обновления нормативного обеспечения. Перспективная реализация данных мер ожидается в контексте национального проекта «Экономика данных и цифровая трансформация государства»[83].

Повышение надёжности и достоверности процесса идентификации личности в цифровой среде становится одной из приоритетных задач для юридической и технических наук, подтверждение этому содержится в законодательных нововведениях, утверждённых в последние годы. Последние законодательные инициативы в сфере персональных данных свидетельствуют о формировании более строгой регуляторной модели в отношении биометрических данных: государство акцентирует внимание на контроле за их сбором, обработкой и централизованным хранением. Идентификация личности по физиологическим параметрам является одной наиболее эффективных и достоверных на данный момент[84]. В реальном пространстве идентификация личности производится по документу, в котором присутствуют какие-то отличительные атрибуты личности

[83] См.: Национальный проект «Экономика данных и цифровая трансформация государства». Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : [Электронный ресурс]. URL: https://digital.gov.ru/target/naczionalnyj-proekt-ekonomika-dannyh-i-czifrovaya-transformacziya-gosudarstva (дата обращения: 03.10.25)

[84] См.: Единая биометрическая система. // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : [Электронный ресурс]. URL: https://digital.gov.ru/ru/activity/directions/802/?utm_referrer=https%3a%2f%2fwww.google.com%2f (дата обращения: 11.10.23)

— например, фотография, по которой и проводится идентификация, юридическим подтверждением согласия является собственноручная подпись. Однако при электронной идентификации достоверность проверки личности в некоторых случаях менее надёжна. По следующим причинам:

— идентификация производится дистанционно;

— достоверно подтвердить, что процедуру проходит именно тот, кому в реальности принадлежат запрашиваемые идентификационные данные при онлайн-идентификации значительно сложнее, чем в реальности;

— регламенты идентификации по совокупности уникальных признаков не всегда чётко прописаны и качественно составлены.

Одним из способов уменьшения возможной остроты этой проблемы может быть включение в процедуру подтверждения личности обязательного условия считывания биометрических данных индивидуума в реальном времени, где атрибутом с высокой достоверностью для подтверждения личности может служить биометрическая информация. Об актуальности этого говорят участившиеся случаи мошенничества с использованием электронных подписей физических лиц. «Из материалов дела Бабушкинского районного суда г. Москвы № 2-3237/19 известно, что М. (ответчик) стал новым собственником его квартиры на основании договора дарения от 28 сентября 2018 г., заключенного посредством электронной подписи истца. Однако С. никаких сделок по отчуждению квартиры не совершал, договор дарения не подписывал, электронную подпись не получал. К сожалению, в материалах дела не описывается, каким именно образом ответчиком был получена электронная подпись С., которой он воспользовался, чтобы подписать названный договор и стать новым собственником. Зато указано, что сделка по отчуждению спорной квартиры произведена в электронном виде с использованием усиленной квалифицированной электронной подписи истца»[85]. Следовательно, внедрение обязательного подтверждения некоторых юридически значимых действий через считывание биометрии является требованием времени. Такой подход позволит

[85] См.: Кирильчик Е. В. Проблемы обеспечения защиты биометрических персональных данных в условиях цифровой экономики / Е. В. Кирильчик, Е. В. Белованс // ГлаголЪ правосудия. — 2022. — № 3(29). — С. 16–21.

решить проблему, связанную с использованием дистанционных механизмов совершения юридически значимых действий.

Исполнение национального проекта «Цифровая экономика» и «Экономика данных» актуализирует вопрос о достоверности электронной идентификации личности по причине перехода таких процедур на «цифровые рельсы».

С течением времени стало понятно, что имеющееся законодательство не в полной мере регулирует сбор биометрических данных физических лиц, поэтому был разработан, и принят в 2022 году, Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации». Этот Закон изменил регулирование обработки биометрической информации в нашей стране; главным нововведением документа стала необходимость для операторов, которые производят сбор биометрических данных физических лиц, передавать их в Единую биометрическую систему (ЕБС; полное название: «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных»). Обратим внимание на основные предписания Федерального закона от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации»:

— передача биометрических данных осуществляется только добровольно, принудительный сбор не допускается;

— закон предоставляет возможность отзыва согласия, это возможно сделать в любой момент, срок для отзыва не предусмотрен. Отзыв согласия осуществляется тем же способом, которым было получено согласие;

— дискриминация в отношении получателей услуг, которые не дали согласие на использование биометрии запрещена;

— все биометрические данные передаются в ЕБС, их обработка вне её запрещена;

— сбор биометрии осуществляется только аккредитованными компаниями и организациями, действующими в соответствии с требованиями закона.

Вступление в силу некоторых положений Закона растянуто по времени на несколько лет, некоторые вступили в силу с 1 июня 2023 года, с 2024 года начнёт действовать Часть 14 статьи 3, а с 2027 года — оставшиеся нормы.

Благодаря использованию Единой биометрической системы, при получении банковских услуг не нужно будет сдавать данные при переходе из одного банка в другой. Централизация хранения биометрических данных физических лиц позволит повысить уровень их защищённости и будет способствовать более полному контролю над функционированием такой системы.

Однако при функционировании этой критически важной для государства системы, следует уделять особое внимание вопросу её информационной безопасности. Данная проблематика поднимается в работах некоторых исследователей[86]; суть опасений, которые высказываются в этих работах, связана с тем, что технические решения, используемые для хранения биометрической информации о физических лицах, могут иметь уязвимости, посредством которых, разведки недружественных стран будут иметь возможность доступа к обрабатываемым биометрическим данным. Поэтому значительное внимание следует уделить тем технологиям, которые используются при построении технической инфраструктуры Единой биометрической системы. В 2025 году в Москве открылся единый центр биометрических испытаний, в котором «на новой площадке планируют проводить научные исследования, испытывать и оценивать различные продукты, а также вести открытый диалог с представителями делового

[86] См.: Субетто А. И. Закон о биометрии в России — это потенциальное оружие «запада» в войне против // Теоретическая экономика. — 2023. — № 3(99). — С. 128–130.

сообщества»[87]. Создание такого центра, безусловно, позволит выработать новые подходы к работе с биометрическими данными, возможно следует рассмотреть создание аналогичного центра на федеральном уровне, а также в регионах, для выработки эффективных методик работы с биометрическими данными, в том числе и правовых.

Ещё одной особенностью, связанной с изменениями в области регулирования обработки биометрических данных, является слабая информированность граждан о том, для чего была организована ЕБС, и какие задачи решались принятием изменений в законодательстве в данной области. Представляет научный интерес оценка воздействия принятых нормативных изменений на структуру и динамику взаимоотношений между гражданами и организациями (включая государственные органы и финансовые организации), использующими биометрические технологии. В результате предположительной информационной диверсии, совершённой неустановленными лицами, произошло то, что «Центры госуслуг столкнулись в последние недели с ажиотажным спросом на услугу отказа от сбора и хранения биометрических данных. Десятки тысяч граждан по всей России выстраивались в очереди еще до открытия МФЦ, чтобы написать соответствующие заявления. Поводом стало сообщение в мессенджерах, что отказ от сбора биометрии можно оформить лишь до 31 августа, после чего граждан якобы начнут принудительно фотографировать через камеры банкоматов и записывать голос по телефону. Разъяснения чиновников о фейке, а также о том, что законодательство позволяет подать заявление без временных ограничений, не помогли. Тем более что банки действительно обязаны передать в государственную Единую биометрическую систему образцы лиц до конца сентября, при этом только у Сбербанка накоплены данные на 30 млн. человек»[88]. Такая ситуация стала возможна из-за того, что государство не озаботилось своевременным информированием граждан о том, как использование биометрических данных позволит обезопасить их взаимодействие с

[87] См.: В Москве создан единый центр биометрических испытаний. // Interfax : [Электронный ресурс]. URL: https://www.interfax.ru/moscow/1012254 (дата обращения: 16.10.23)
[88] См.: Ажиотажный сброс. // Коммерсантъ : [Электронный ресурс]. URL: https://www.kommersant.ru/doc/8079421 (дата обращения: 16.10.23)

различными организациями. Поэтому следует учитывать возможные информационные диверсии со стороны недружественных государств, группировок и иных деструктивных элементов, и мнительность отдельных граждан, при внесении изменений в чувствительные разделы российского законодательства, что ставит перед государством важную задачу по информационному сопровождению различных инициатив в области совершенствования правового регулирования тех или иных общественных отношений. Мудрая и реалистичная информационная политика донесения до населения смысла законодательных новшеств позволит снизить уровень недопонимания между государством и обществом и будет залогом «процветания и благосостояния нации, стабильности общества»[89], Из-за непродуманности информационного освещения возникают ситуации, когда общество, на волне возникшей истерии, начинает сопротивляться нововведениям, которые призваны улучшить те или иные стороны общественной жизни.

Современные тенденции в сфере законотворчества демонстрируют комплексный подход: с одной стороны, происходит нормативное оформление работы с биометрическими данными, с другой — наблюдается устойчивая динамика ужесточения требований к защите персональных данных, что соответствует стратегическому курсу государства. В марте 2021 года вступил в действие Федеральный закон от 30.12.2020 г. № 519-ФЗ «О внесении изменений в Федеральный закон ”О персональных данных“»[90], а в 2022 году были внесены важные изменения в Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»[91], часть из которых вступила в силу с 1 сентября 2022 г., а часть с 1 марта 2023 г. Поскольку принятые изменения тесно связаны с влиянием

[89] См.: Теория государства и права: учебник для студентов высших учебных заведений, обучающихся по направлению и специальности "Юриспруденция" / Н. И. Матузов, А. В. Малько ; Саратовский филиал ин-та государства и права Российской акад. наук. — Изд. 2-е, перераб. и доп. — М : Юристъ, 2007. — 540 с.
[90] См.: Федеральный закон от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон "О персональных данных» // Собрание законодательства РФ, 04.01.2021, № 1 (часть I), ст. 58.
[91] См.: Федеральный закон от 14.07.2022 № 266-ФЗ "О внесении изменений в Федеральный закон "О персональных данных", отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона "О банках и банковской деятельности" // Собрание законодательства РФ, 18.07.2022, № 29 (часть III), ст. 5233.

цифровизации на государственное управление, они будут рассмотрены в дальнейшем.

В сфере правового регулирования обработки персональных данных нарастает дискуссия о целесообразности введения системы оборотных штрафов[92] для операторов, допустивших утечки данных. На текущий момент указанная инициатива прошла этап концептуального обсуждения и перешла в фазу законопроектной деятельности[93]. Однако до стадии принятия изменений в законодательство эта, несомненно, важная новация была доведена только в 2024 году с принятием Федерального закона от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»[94]. Аналогичные правовые конструкции имеются в законодательстве США и государств Европейского союза. Потребность в ужесточении санкций из-за утечек персональных данных возникла по причине того, что в последние годы количество взломов и утечек персональных данных значительно возросло. Так, в 2019 году, у «Сбербанка» украли данные о 60 млн. клиентов[95], в том же году у компании «Дримакс» были похищены данные о 14 млн. пользователей[96], ещё одной крупной кражей персональных данных стал инцидент с компанией «Билайн», информация более 2 млн. клиентов была похищена злоумышленниками[97]. В России 2022 год ознаменовался большим числом масштабных утечек информации о физических лицах, среди них:

«1. «Яндекс.Еда», февраль 2022 г., В сеть попали почти 50 млн. данных пользователей сервиса: фамилии, номера телефонов, адреса доставок, комментарии к заказам и даже суммы чеков. Все это можно было найти на картах городов. 2. В

[92] См.: В России могут ввести оборотные штрафы за утечку персональных данных . // КоммерсантЪ : [Электронный ресурс]. URL: https://www.kommersant.ru/doc/5227921 (дата обращения: 19.10.23).
[93] См.: Утечки возьмут в оборот. // КоммерсантЪ : [Электронный ресурс]. URL: https://www.kommersant.ru/doc/5379590 (дата обращения: 19.10.23).
[94] См.: Федеральный закон от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // Собрание законодательства РФ, 02.12.2024, № 49 (часть IV), ст. 7411.
[95] См.: В Сбербанке крупнейшая утечка в истории российского банковского сектора. // Cnews : [Электронный ресурс]. URL: https://www.cnews.ru/news/top/2019-10-03_sberbank_dopustil_krupnejshuyu (дата обращения: 19.10.23).
[96] См.: Утечка данных с сервера ОФД «Дримкас» оказалась масштабнее, чем предполагалось ранее // SecurityLab.ru : [Электронный ресурс]. URL: https://www.securitylab.ru/news/501312.php (дата обращения: 19.10.23).
[97] См.: Степанова Ю. Абонентов загрузили на сервер // КоммерсантЪ : [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4986542 (дата обращения: 19.10.23).

мае 2022 на карту со «сливом» из «Яндекс.Еды» добавили данные ГИБДД, СДЭК, Wildberries, «Билайна», ВТБ, «ВКонтакте» и некоторых других компаний. 3. Delivery Club, июнь 2022 г. Слиты данные пользователей сервиса с 2019 года, в количестве 2,2 млн. пользователей. Имена, номера телефонов, адреса доставки, адреса электронной почты, составы и стоимость заказов, дата и время заказа, IP-адреса пользователей. 4. «Гемотест», май 2022 г. В сеть попали две базы данных: 554 млн. заказов и 31 млн. строк с информацией: ФИО, даты рождения, адреса, номера телефонов, адреса электронных почт, серии и номера паспортов, и результаты анализов. 5. «Туту.ру», июль 2022 г. В сеть попали данные пользователей, которые покупали автобусные туры: 2,6 млн. заказов; 2,29 млн. телефонных номеров, ФИО и адреса электронных почт»[98]. Как видно из приведённых примеров, даже крупные компании не уделяют достаточно внимания информационной безопасности своих систем, которые обрабатывают данные о физических лицах. Именно бизнес выступал главным противником введения оборотных штрафов за утечки персональных данных: «Компании настаивают, что на фоне экономической ситуации жесткая ответственность за утечки ухудшит условия ведения бизнеса»[99]. Введение таких санкций за утечки информации в отношении допустившей это организации чревато значительными финансовыми потерями. Именно это является причиной выступления бизнес-структур против введения оборотных штрафов за недостаточность внимания к информационной безопасности систем обработки персональных данных. Ужесточение санкций за утечки окажет влияние на то, что крупные операторы персональных данных будут вынуждены уделять больше внимания их защите; однако, помимо этого, следует уделить внимание вопросу предотвращения появления инцидентов безопасности, связанных с персональными данными. Нормативно-правовая база, ориентированная на предотвращение кражи информации о физических лицах, позволит как уменьшить ущерб для деловой репутации компаний, так и повысить

[98] См.: Самые громкие утечки персональных данных за 2022 год в России // vc.ru : [Электронный ресурс]. URL: https://vc.ru/u/1241455-delis-arhiv/494035-samye-gromkie-utechki-personalnyh-dannyh-za-2022-god-v-rossii (дата обращения: 19.10.23).

[99] См.: Минцифры согласилось не вводить штрафы для бизнеса за первый факт утечки персональных данных // RB.RU : [Электронный ресурс]. — URL: https://rb.ru/news/leak-law/ (дата обращения: 19.10.23).

доверие граждан к государству. Кроме этого, такое направление законотворческой деятельности в конечном счёте позволит выстроить правовую систему защиты персональных данных, особенностью которой будет предотвращение компрометации информации о физических лицах, что положительным образом скажется на доверии граждан к государству и улучшении делового климата в стране.

Рассматривая вопрос ужесточения контроля со стороны государственных органов за регламентацией работы информационных систем обработки персональных данных (ИСПДн), следует сказать о том, что в 2021 году был опубликован приказ ФСТЭК № 77[100] регулирующий аттестацию государственных и муниципальных объектов информатизации, (включающих также и персональные данные) не содержащих сведения о государственной тайне. Вот, что говорят эксперты про принятый документ: «Без сомнений, новые правила, которые введены в действие данным документом, в целом повлияют на рынок и позволят сократить количество недобросовестных аттестационных центров, которые предоставляют услуги низкого качества.

Теперь регулятор может без дополнительной проверки приостановить действие выданного аттестата соответствия в случае выявления ошибок при выдаче аттестата или не подтверждения проведения необходимых контрольных испытаний»[101]. К сожалению, данный документ относится только к государственным информационным системам обработки персональных данных. В свете того, что всё больше компаний, занимающихся обработкой информации о физических лицах, подвергаются атакам с целью получению неправомерного доступа к этой информации, такой подход не позволяет в полной мере обеспечить защиту данных о физических лицах. Периодический независимый аудит операторов персональных данных на предмет соблюдения требований

[100] См.: Приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 "Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну" (Зарегистрирован 10.08.2021 № 64589) // Официальное опубликование правовых актов : [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202108100027 (дата обращения: 27.10.23).
[101] См.: Разбираемся в приказе ФСТЭК России № 77 // ГК ЦИБИТ : [Электронный ресурс]. URL: https://www.cibit.ru/stati-ekspertov/razbirayemsya-v-prikaze-fstek-rossii77/ (дата обращения: 27.10.23).

законодательства с последующей передачей результатов регулятору, независимо от их принадлежности к государственным структурам, позволит своевременно выявлять нарушителей. Такой подход станет побуждающим фактором для операторов персональных данных более тщательно соблюдать требования законодательства о защите личных данных.

Анализируя историю становления, развития и особенности российского законодательства в области правового регулирования обработки идентификационной информации физических лиц, можно сделать вывод о том, что в нашей стране институт персональных данных прошёл достаточно длинный путь. Примечательно, что Россия приступила к системному регулированию защиты персональных данных сравнительно поздно (по историческим меркам). При сопоставлении с подходами США и стран ЕС становится очевидной недостаточная упорядоченность регулирования в этой сфере в нашей стране. К факторам, которые повлияли на активизацию усилий законодателей, можно отнести: ратификацию международных нормативных актов, связанных с защитой прав человека, смену политической формации и, как следствие, повышение внимания к защите прав человека. Однако, несмотря на все вносимые изменения и дополнения, в российском законодательстве остаётся множество неурегулированных вопросов. Один из наиболее важных — это соотношение правовых понятий «персональные данные» и «тайна частной жизни». Это отрицательным образом сказывается на уровне защищённости обоих правовых институтов.

Большое влияние на общественные отношения, связанные с обработкой персональных данных, оказало развитие и всестороннее внедрение информационно-коммуникационных технологий. Ручная обработка информации о физических лицах уступила место автоматизированным методам, что, в свою очередь, привело к тому, что доступ к хранимым данным о физических лицах значительно упростился и стал практически мгновенным. Такая информация превратилась в социально-экономическую характеристику субъекта, которая представляет интерес для множества организаций. С появлением технологий автоматизированного анализа подобных массивов данных, различные компании

стали использовать его результаты для принятия управленческих решений и получения прибыли. Отсюда следует, что эта информация стала стратегически важным ресурсом, за которым начали охотиться и деструктивные элементы, в том числе с целью использования в различных мошеннических схемах, что привело к росту числа атак на информационные системы операторов персональных данных с целью присвоения обрабатываемых данных. Количество инцидентов информационной безопасности и случаев компрометации личной информации ежегодно растёт. Одна из причин этого кроется в не всегда действенности санкций за утечки персональных данных. Фактором, из-за которого это происходит, является нежелание операторов персональных данных вкладывать значительные финансовые средства в информационную безопасность своих систем. Компании предпочитают заплатить штраф, размеры которого в большинстве случаев несопоставимы с размерами затрат на обеспечение информационной безопасности; возможно введение оборотных штрафов позволит снизить остроту проблемы. Цифровизация социальных отношений превратила персональные данные в товар, который покупается и продаётся. К сожалению, субъект персональных данных ограничен в возможности контроля над тем, кому информация о нём передаётся, что усложняет ограничение на передачу своих данных нежелательным организациям.

Развитие информационных технологий облегчило использование биометрической информации для идентификации физических лиц, что потребовало от государства упорядочивания общественных отношений в этой области. Были созданы правовые механизмы идентификации личности с использованием биометрических данных, что, по задумке разработчиков закона, должно было повысить безопасность взаимодействия физических лиц с государственными, муниципальными и финансовыми организациями. Однако из-за недостаточности внимания, которое было уделено информационному сопровождению правовых нововведений в этой области, а также целенаправленной информационной атаки неустановленных злоумышленников, множество граждан отказалось от сдачи биометрических данных. Учитывая эти обстоятельства,

приходим к заключению, что правотворческая деятельность государства должна учитывать необходимость информирования населения о значимых изменениях в законодательстве, с целью исключения манипулирования общественным мнением в этой области.

Анализируя действующее законодательство в области защиты персональных данных можно сделать вывод о том, что, несмотря на все вносимые изменения и дополнения, оно недостаточно эффективно, в том числе и потому, что изначально оно ориентировалось на общественные отношения, связанные с ручной обработкой персональных данных. В последнее время наметилась тенденция, связанная с ужесточением санкций за правонарушения в области защиты персональных данных, однако при этом наблюдается перекос в сторону интересов государства, интересы же личности оказываются задвинуты на второй план. Однако, многообразие общественных отношений в этой области усложняет поиск строгого баланса между интересами государства и личности. В связи с этим необходимо постоянно совершенствовать законодательство в сфере защиты персональных данных с целью устранения имеющихся противоречий при защите идентификационных данных физического лица. А именно, нужно не только ужесточать санкции за нарушение правил обработки персональных данных, но и работать над созданием механизмов выявления нарушений, связанных с несоблюдением правил обработки идентификационной информации физических лиц, до того, как произойдёт неавторизованный доступ к охраняемой информации. Такой подход позволит учитывать, как интересы личности, так и государства, что особенно актуально в связи с появлением всё новых цифровых технологий. Системный подход является одним из основных факторов эффективного устранения пробелов в законодательстве, он должен лечь в основу совершенствования регламентации обработки персональных данных в Российской Федерации, что особенно важно с учётом изменения методов обработки персональных данных физических лиц.

§ 1.3 Опыт зарубежных государств в области правового регулирования обработки персональных данных

Национальное законодательство, регулирующее отношения, касающиеся персональных данных, стало появляться во второй половине XX века[102]. Появление таких нормативных актов стало следствием того, что процесс обработки персональных данных стал автоматизироваться. Это произошло в 70-х годах прошлого века, когда хранение и обработка информации, в том числе и персональных данных, стали возможны не только в бумажной, но и в электронной форме. Первый закон, регулирующий автоматизированную обработку персональных данных, был принят в 1970 году в ФРГ, властями земли Гессен[103]: документ не был федеральным. Указанный акт регулировал автоматизированную обработку персональных данных на муниципальном уровне, при сборе налогов, оказании услуг в области жилищно-коммунального хозяйства и т.д. Действие документа распространялось на деятельность муниципальных властей и их подрядчиков.

Первым общегосударственным нормативным актом, регулирующим отношения, связанные с персональными данными, стал Шведский «Datalgen»[104], принятый в 1973 году. Ко дню вступления в силу этого закона Швеция была одной из самых компьютеризированных стран мира, значительная часть данных государственных органов с 60-х годов хранилась на магнитных лентах. Принятие данного нормативного акта было связано с обеспокоенностью правительства Швеции неурегулированностью отношений, связанных с хранением и обработкой персональных данных. В отличие от закона, ранее принятого в земле Гессен в ФРГ, нормы шведского правового акта были общеобязательными. Другой особенностью

[102] См. подробнее: Сапронов Д. Ю. Историческая ретроспектива правового регулирования персональных данных в некоторых странах // Труды по интеллектуальной собственности. — 2022. — Т. 42, № 3. — С. 26–32.
[103] См.: Datenschutzgesetz. Gesetz- und Verorbnugsblat // Landtagsinformationssytem : [Электронный ресурс]. URL: https://starweb.hessen.de/cache/GVBL/1970/00041.pdf#page=1 (дата обращения: 29.10.23) (пер.: Яндекс-переводчик).
[104] См.: Datalag (1973:289) // Notisum : [Электронный ресурс]. URL: http://www.notisum.se/rnp/document/?id=19730289 (дата обращения: 29.10.23), (пер.: Яндекс-переводчик).

было то, что единых правил обработки данных в законе сформулировано не было. Правила формулировались индивидуально при обращении в Инспекцию по защите данных (Data Inspection Board) для выдачи лицензии на право автоматической обработки персональных данных. Такой порядок лицензирования деятельности по электронной обработке персональных данных, тогда был обусловлен тем, что она не имела широкого распространения. Отметим, что лицензирование средних и крупных операторов персональных данных позволяет более полно контролировать исполнение действующих норм, регулирующих электронную обработку персональных данных, а индивидуальные условия хранения позволяют конкретизировать их для каждого оператора персональных данных, что может положительно сказаться на безопасности хранимой информации. Этот же закон регулировал трансграничную передачу персональных данных, вследствие чего организации, попавшие под действие его норм, были вынуждены получать специальную лицензию. В 1993 году, закон был пересмотрен, поскольку в нём не учитывалось появление телекоммуникационных сетей, и сети Интернет в частности. В 1995 году Швеция вступила в Европейский союз и стала внедрять общеевропейские нормы, регулирующие обращение с персональными данными.

В 1974 году в США был принят «Privacy Act», регулирующий сбор, обработку, использование и распространение персональных данных в системах государственных органов[105]. Помимо этого, закон регулировал вопросы оповещения граждан о системах регистрации государственных органов и раскрытия их записей, доступа граждан к записям, содержащих сведения о них, и внесения изменений в эти записи, запрет на разглашение информации и исключения, когда информация может быть предоставлена третьим лицам. Принятые нормы не относились к частному сектору и регулировали только деятельность государственных органов. Такой подход был связан с высокой стоимостью компьютерного оборудования, вследствие чего автоматизированная обработка персональных данных производилась, в основном, государственными

[105] См.: The privacy act // U.S. Department of Justice : [Электронный ресурс]. URL: https://www.justice.gov/opcl/privacy-act-1974 (дата обращения: 5.11.23).

агентствами США. В 1988 году был принят «The Computer Matching and Privacy Protection Act of 1988», который добавил определённые меры защиты для владельцев персональных данных[106]. Стоит отметить, что отношения в частном секторе также не были урегулированы. Законодательство США по защите персональных данных являет собой систему федеральных и местных актов. На федеральном уровне регулируются обработка персональных данных, банковские[107] операции[108], телекоммуникации[109], медицинская сфера[110], сбор данных детей младше 13 лет[111]. Важным этапом эволюции законодательства США в области регулирования обработки персональных данных является принятие и вступление в силу с 1 января 2020 года «California Consumer Privacy Act»[112] (CCPA). Этот нормативный акт в определённой степени перекликается с законодательством Европейского союза, но он имеет и отличия, например, оператор не обязан получать согласие на обработку данных от пользователя. Интерес представляет правовая конструкция, связанная со случаем утери или кражи данных: если такое происходит, то оператор должен заплатить каждому пользователю, чьих данных это коснулось, от 100 до 750 долларов. Документом закреплён запрет на дискриминацию пользователей, отказавшихся от передачи персональных данных. Одновременно предусматривается возможность введения системы скидок и поощрений для тех, кто дал соответствующее согласие. Такой подход может в будущем сформировать конструкцию, при которой компании будут в той или иной форме покупать у пользователей их персональные данные.

---

[106] См.: The computer matching and privacy protection act // IRS : [Электронный ресурс]. URL: https://www.irs.gov/irm/part11/irm_11-003-039 (дата обращения: 5.11.23).
[107] См.: Gramm–leach–bliley act // U.S. Goverment Publishing Office : [Электронный ресурс]. URL: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf
[108] См.: Fair Credit Reporting Act // Federal Trade Commission : [Электронный ресурс]. URL: https://www.ftc.gov/system/files/545a_fair-credit-reporting-act-0918.pdf (дата обращения: 5.11.23).
[109] См.: Electronic communications privacy act of 1986. // Library of Congress : [Электронный ресурс]. URL: https://www.loc.gov/law/opportunities/PDFs/ElectronicCommunicationsPrivacyAct-PL199-508.pdf (дата обращения: 5.11.23) (дата обращения: 5.11.23).
[110] См.: Health insurance portability and accountability act. // U.S. Department of Health & Human Service. URL: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf
[111] См.: Children's online privacy protection rule. // Federal Trade Comisson : [Электронный ресурс]. URL: https://www.ftc.gov/system/files/2012-31341.pdf (дата обращения: 5.11.23).
[112] См.: California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100]. // California Legislative Information website: [Электронный ресурс]. URL: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (дата обращения: 5.11.23).

Основная часть нормативных актов по защите персональных данных в США принималась по мере того, как информационно-коммуникационные технологии расширяли своё использование в тех или иных секторах экономики, и общественные отношения претерпевали всё большие изменения. Тот факт, что обработка персональных данных регулируется не одним, а несколькими нормативными актами для каждой сферы применения, позволяет более полно урегулировать общественные отношения. Поскольку в каждой области есть своя специфика работы с персональными данными, и использование единых требований к защите такой информации может не учитывать каких-то особенностей конкретных отношений, то в результате возможны случаи, как избыточного регулирования, так и ситуации, когда отношения, связанные с персональными данными в какой-то отрасли, будут отрегулированы нормами права не полностью. Возможно, российскому законодателю стоит обратить внимание на некоторые принципы, используемые в США для защиты персональных данных; положительный эффект могло бы оказать введение обязательной компенсации со стороны операторов персональных данных, людям чьи данные были украдены. Это способствовало бы повышению внимания компаний к защите персональных данных.

Не отставал в этом вопросе и Европейский союз, первый общеевропейский закон, призванный защитить права физических лиц в сфере персональных данных был принят в 1995 году, именно он стал тем базисом, который лёг в основу принятого в 2016 году нового «Общего регламента по защите данных»[113] (General Data Protection Regulation) (далее — GDPR), который открыл новую эру в вопросе правовой защиты персональных данных европейских граждан. «Основными целями принятия GDPR были: обеспечение возможности граждан контролировать обработку своих персональных данных и унификация нормативной базы для

[113] См.: Regulation (eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). // Official website of the European Union : [Электронный ресурс]. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (дата обращения: 5.11.23).

международных экономических отношений. Основными принципами GDPR выступают[114]:

«1) Законность, справедливость и прозрачность. Персональные данные должны обрабатываться законно, справедливо и прозрачно. Любую информацию о целях, методах и объёмах обработки персональных данных следует излагать максимально доступно и просто. 2) Ограничение цели. Данные должны собираться и использоваться исключительно в тех целях, которые заявлены компанией (онлайн-сервисом). 3) Минимизация данных. Нельзя собирать личные данные в большем объёме, чем это необходимо для целей обработки. 4) Точность. Личные данные, которые являются неточными, должны быть удалены или исправлены (по требованию пользователя). 5) Ограничение хранения. Личные данные должны храниться в форме, которая позволяет идентифицировать субъекты данных на срок не более, чем это необходимо для целей обработки. 6) Целостность и конфиденциальность. При обработке данных пользователей компании обязаны обеспечить защиту персональных данных от несанкционированной или незаконной обработки, уничтожения и повреждения»[115].

Несоблюдение правил GDPR жёстко карается штрафом в размере 4% от годового оборота компании или суммой до 20 000 000 евро, вне зависимости от того, находится на территории Европейского Союза оператор персональных данных, или нет. К примеру, ряд новостных сайтов в США был вынужден ограничить доступ к своим сайтам пользователям из ЕС, кроме этого другие сервисы были вынуждены закрыться[116] по причине невозможности выполнить нормы GDPR. Некоторые принципы «Общего регламента защиты персональных данных» являются революционными и нигде ранее не применялись. Одним из

[114] См. подробнее: Сапронов Д. Ю. Влияние всеобщей цифровизации на правотворчество в сфере персональных данных / Д. Ю. Сапронов // Стратегия развития экономики Беларуси: вызовы, инструменты реализации и перспективы : Сборник научных статей. В 2-х томах, Минск, 18–19 октября 2022 года / Редколлегия: Д.В. Муха [и др.]. Том 2. – Минск: Издательское общество с ограниченной ответственностью "Право и экономика", 2022. – С. 340-344.

[115] См.: GDPR — новые правила обработки персональных данных в Европе для международного IT-рынка. // Habr : [Электронный ресурс]. URL: https://habr.com/ru/company/digitalrightscenter/blog/344064/ (дата обращения: 5.11.23).

[116] См.: Жертвы GDPR: кто уже прекратил работу из-за нового регулирования персональных данных // Habr : [Электронный ресурс].URL: https://habr.com/en/company/it-grad/blog/418501/ (дата обращения: 5.11.23).

таких прав является возможность безвозмездного переноса данных от одного оператора персональных данных к другому по желанию их владельца. Эти нормы, при соответствующей доработке, могли бы быть внесены в российское законодательство, регулирующее обработку персональных данных[117].

Остановимся на опыте Китайской Народной Республики (КНР) в области защиты персональных данных[118], где первый общегосударственный «Закон о кибербезопасности», регулирующий отношения, связанные с персональными данными, был принят в 2017 году. Ранее же действовали десятки норм в разных отраслях. В соответствии с принятым документом вводится градация для информационных систем по степени влияния на безопасность государства, всего таких уровней пять[119]. К первым двум уровням относятся информационные системы, не оказывающие влияния на национальную безопасность. Принадлежность компьютерных систем к третьему и последующим уровням, обязывает компании-владельцы один раз в два года проходить аудит у одного из агентств-подрядчиков и отчитываться перед Бюро общественной безопасности. Такая градация позволяет более полно регулировать функционирование информационных систем, хранящих и обрабатывающих важную для государства информацию. Полнота регулирования достигается за счёт дифференциации требований функционирования к разным классам систем. Такой подход позволяет избежать ситуации, когда эти требования функционирования избыточны или, в случае больших, сложных и важных для государственной безопасности систем, недостаточны. Следствием обязательности периодического аудита у проверенных подрядчиков и предоставления результатов проверки в соответствующий государственный орган может являться актуализация базы критически важных информационных систем, а также их состояния и соответствия требованиям, предъявляемым к данному классу систем.

---

[117] См.: Сапронов Д. Ю. Правовая эволюция общеевропейского регулирования защиты персональных данных // Труды по интеллектуальной собственности. — 2019. — Т. 34, № 3–4. — С. 83–88.

[118] См. подробнее: Сапронов Д. Ю. Историческая ретроспектива правового регулирования персональных данных в некоторых странах // Труды по интеллектуальной собственности. — 2022. — Т. 42, № 3. — С. 26–32.

[119] См.: China passes new cybersecurity law. // Covington & Burling LLC : [Электронный ресурс]. URL: https://www.cov.com/-/media/files/corporate/publications/2016/11/china_passes_new_cybersecurity_law.pdf (дата обращения: 9.11.23).

Ещё одной важной нормой принятого в КНР закона является регулирование трансграничной передачи информации, по этой причине многие транснациональные компании были вынуждены перенести хранение информации о китайских пользователях своих сервисов в центры обработки данных, которые расположены на территории Китайской Народной Республики.

Влияние информационно-коммуникационных технологий на различные стороны экономики стало значительным, цифровизация позволила делать множество вещей буквально не выходя из дома. E-commerce стала одним из основных драйверов трансформации общественных отношений; в 2024 году оборот цифровой торговли приблизился к 7 триллионам долларов[120]. Вирус COVID-19 стал причиной скачкообразного роста сектора e-commerce во многих странах, в том числе, и в КНР. «Китайская электронная коммерция быстро развивалась в течение последних пяти лет благодаря широкому распространению Интернета и смартфонов, росту доверия потребителей к онлайн-покупкам, появлению платформ электронной коммерции и доступности различных альтернативных платежных решений, таких как Alipay и WeChatPay»[121]. Стремительное развитие электронной коммерции стало ключевым трендом, который оказал влияние на весь глобальный мировой рынок. Фундаментальная трансформация общественных отношений заставила правительства многих стран обратить внимание на проблему совершенствования своего законодательства под требования цифровой экономики. Не обошла стороной эта проблематика и КНР. Китай уже некоторое время работал над внедрением цифровых технологий в экономику. Одна из особенностей Китая — это огромное население, и вирус COVID-19 стал тем фактором, который ускорил перестройку национальной экономики этого государства. Цифровизация стала той опорной точкой, которая помогла КНР преодолеть саму пандемию и её последствия. Цифровизация увеличивает эффективность экономики и государственного управления, и в сложных ситуациях позволяет не потерять

[120] См.: Bernhardt G. Global Ecommerce Sales Growth Report for 2020–2025. // Shopify Blog : [Электронный ресурс]. URL: https://www.shopify.com/blog/global-ecommerce-sales (дата обращения: 13.11.23)

[121] См.: Китайскому eCommerce прогнозируют опережающий рост. // ShopifyBlog : [Электронный ресурс]. URL: https://e-pepper.ru/news/kitayskomu-ecommerce-prognoziruyut-operezhayushchiy-rost.html (дата обращения: 13.11.23)

управляемость, своевременно реагировать на имеющиеся угрозы и вызовы национальной стабильности. В этих условиях ключевым фактором является эффективность законодательства, связанного с дистанционной идентификацией личности; именно обработка персональных данных и их защита выходят на первый план в цифровой экономике.

Правительство КНР более 10 лет назад обратило внимание на необходимость совершенствования правовой защиты персональных данных. В Конституции КНР и «Общих принципах гражданского права»[122] защищались право на имя, честь, достоинство и неприкосновенность частной переписки. В 2010 году в силу вступили «Правила по противодействию отмывания денег и финансирования терроризма, для клиринговых организаций и организаций, занимающихся платежными операциями», после этого в законодательстве Китая было закреплено правовое определение «основных персональных данных»: имя, пол, контактные данные, вид и номер удостоверения личности, домашний адрес, рабочий адрес, профессия.

Появление больших ИТ-компаний, развитие информационно-коммуникационных технологий и всё более увеличивающаяся цифровизация социальных отношений, — эти факторы поставили перед государственными органами КНР задачу, связанную с необходимостью повысить защищённость персональных данных граждан. Цифровизация сферы обработки информации о физических лицах стала важным фактором и начала оказывать всё большее влияние на безопасность государства. Это способствовало, в том числе, и появлению запрета на размещение своих акций на зарубежных биржевых площадках крупными технологическими компаниями, поскольку получение возможности влиять на большие IT-компании, открывало возможности по перехвату управления над ними, что недопустимо для сохранения ИТ-суверенитета государства, особенно когда такие организации обрабатывают огромное количество персональных данных.

---

[122] См.: Общие положения гражданского права КНР. // Законодательство Китая : [Электронный ресурс]. URL: https://chinalawinfo.ru/civil_law/general_principles_civil_law (дата обращения: 15.11.23).

2020 год в КНР ознаменовался принятием «Гражданского кодекса КНР» (Civil Code of the People's Republic of China) (далее — ГК КНР)[123], который начал действовать в 2021 году. Нормы этого документа оказали влияние на повышение защищённости персональных данных физических лиц, но не все нормы ч.4 ГК КНР являлись прорывными. Большинство из них выступали как расширение, дополнение и консолидация уже действовавших положений различных нормативных документов: «Закона о кибербезопасности КНР» (Cybersecurity Law of the People's Republic of China)[124], Закона КНР «О защите прав потребителей» (Law of the People's Republic of China on the Protection of Consumer Rights and Interests)[125] и т.д. Гражданский Кодекс Китая в значительной степени детальнее разъяснял права субъектов персональных данных. Стоит отметить, что в законодательстве более чётко закреплена взаимосвязь между правом на защиту частной жизни и персональными данными. ГК КНР декларирует принцип применения положений о защите персональных данных, в том числе, и к информации о частной жизни. Очевидно, что такая увязка сделана китайским законодателем специально, с целью исключения неопределенности, связанной с понятиями «персональная информация» и «информация о частной жизни». Гражданский Кодекс Китая даёт следующее определение персональной информации: «Под “персональной информацией” понимается информация, фиксируемая в электронной или иной форме, которая позволяет идентифицировать определенное физическое лицо на автономной основе или в совокупности с другой информацией, включая ФИО, дату рождения, номер документа, удостоверяющего

[123] См.: Гражданский кодекс Китая 中国民法典 // Наблюдатель за правосудием Китая 中司观察 : [Электронный ресурс]. URL: https://ru.chinajusticeobserver.com/t/china-civil-code (дата обращения: 17.11.23).

[124] См.: Translation: Data Security Law of the People’s Republic of China (Effective Sept. 1, 2021) // DigiChina : [Электронный ресурс]. URL: https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ (дата обращения: 17.11.23).

[125] См.: Закон КНР «О защите прав потребителей». // Chinalaw.center 中国法律俄文网 : [Электронный ресурс] . URL: https://chinalaw.center/civil_law/china_consumer_rights_protection_law_revised_2013_russian/ (дата обращения: 17.11.23).

личность, биометрическую информацию, адрес, телефон, адрес электронной почты, информацию о состоянии здоровья и месте нахождения»[126].

Кроме Гражданского кодекса КНР следует упомянуть: «Закон о защите личной информации КНР» (Personal Information Protection Law of the People's Republic of China)[127], «Закон о безопасности данных КНР» (Data Security Law of the People's Republic of China)[128], «Закон о Кибербезопасности КНР» (Cybersecurity Law of the People's Republic of China)[129]. Отметим «Закон о защите личной информации КНР»: в нём закреплены основные цели, принципы, а также ответственность в сфере обработки персональных данных физических лиц. Этот рамочный документ предполагает, что более конкретные нормы будут закреплены в подзаконных актах, которые будут приняты надзорными и контролирующими органами, ответственными за область защиты персональных данных. Ключевая функция «Закона о защите личной информации КНР» — защита прав субъектов персональных данных. В законе много внимания уделено не только «персональной информации», законодатель обозначил важность и «приватности» — защиты информации о личной жизни. То, что почти каждый человек имеет смартфон, стало способствовать, накоплению огромных массивов индивидуальной информации и, на первый взгляд, информации, не относящейся к субъекту персональных данных. К таким случаям можно отнести обработку больших массивов данных аналитическими системами с элементами искусственного интеллекта. Именно это стало причиной того, что Государственные органы КНР стали прилагать больше усилий для повышения эффективности законодательства в сфере защиты персональных данных и информации о частной жизни.

---

[126] См.: Прозорова М. Гражданский кодекс Китая и защита персональных данных // Worldbussineslaw : [Электронный ресурс]. URL: https://worldbiz.ru/analytics/Grazhdanskii-kodeks-Kitaia-i-zaschita-personalnykh-dannykh (дата обращения: 17.11.23).

[127] См.: The PRC Personal Information Protection Law (Final): A Full Translation // China Briefing. URL: https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/ (дата обращения: 17.11.23).

[128] См.: Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021) // DigiChina. URL: https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ (дата обращения: 17.11.23).

[129] См.: China Cybersecurity Law // D-russia.ru. URL:https://d-russia.ru/wp-content/uploads/2017/04/China-Cybersecurity-Law.pdf (дата обращения: 17.11.23).

Подходы, применяемые в «Законе о защите личной информации КНР» в какой-то степени перекликаются с применяемыми в общеевропейском «Общем регламенте по защите данных» (GDPR). Но китайский закон имеет более рамочный характер, и законодатель исходил из того, что более подробные нормы будут закреплены в подзаконных актах соответствующих регуляторов. Такой подход во многом позволяет выстраивать более гибкую регуляторную политику, что повышает эффективность управления и реагирования на различные изменения в области обработки персональных данных. Также, этот подход позволяет соответствующим государственным органам разрабатывать, и вводить в действие, те правила обработки персональных данных, которые они посчитают наиболее эффективными в конкретной ситуации. Полномочия государственных органов в этом вопросе не ограничены, но этот подход, помимо положительных сторон, имеет предпосылки для возможных злоупотреблений со стороны регуляторов из-за наличия у них практически безграничных полномочий. Очевидно одной из основных целей, которые ставились законодателем в КНР, было формирование у государства правовых инструментов для повышения управляемости сферы защиты персональных данных и расширения возможностей по регулированию общественных отношений в этой области, и, как следствие, повышение защищённости интересов Китая, связанных с безопасностью государства. Именно этот факт и является ключевым различием в правовых политиках Европейского союза и Китая. Законодатели в ЕС отталкиваются от важности защиты прав своих граждан, в том числе, связанных с защитой персональных данных; вопрос национальной безопасности также актуален для Европы, но для европейских законодателей более приоритетным является защита прав физических лиц.

В Китае был выбран путь свойственный для централизованной модели регулирования отношений, связанных с персональными данными, однако дифференцированный подход к системам обработки персональных данных позволяет более полно регулировать обработку персональной информации о гражданах. Возможно, отдельные элементы китайского опыта регулирования персональных данных стоило бы применить и в России: к ним можно отнести

разделение информационных систем на классы и независимый аудит информационных систем с последующим предоставлением информации национальному регулятору.

Система правовой защиты персональных данных, выстроенная в Китайской Народной Республике, имеет ряд эффективных правовых конструкций, которые могут представлять интерес для российской юридической науки[130]. Наблюдаемое снижение эффективности российской системы правовой защиты персональных данных при продолжающемся обновлении нормативной базы определяет актуальность рассмотрения данного вопроса.

Перечислим следующие подходы законодательства КНР в области регулирования обработки персональных данных[131], на которые отечественному законодателю рекомендуется обратить внимание:

1. «Закрепление принципа взаимосвязи информации о частной жизни и персональных данных. Это позволило бы решить проблему, связанную с неопределенностью правового статуса информации о частной жизни физических лиц в российском законодательстве. Разделение операторов персональных данных на разные категории в зависимости от того, как они используют персональные данные. Использование такого механизма позволило бы более гибко регулировать деятельность компаний, занимающихся обработкой персональных данных, и выработать несколько правовых траекторий для разных категорий таких организаций.

2. Положение, обеспечивающее прозрачность автоматизированных решений при расчете цен в интернет-магазинах на основе информации о покупателе. Такой подход способствует большей транспарентности Интернет-торговли и повышает доверие к онлайн-площадкам, а также снижает возможности для дискриминации.

[130] См. подробнее: Сапронов Д. Ю. Историческая ретроспектива правового регулирования персональных данных в некоторых странах // Труды по интеллектуальной собственности. — 2022. — Т. 42, № 3. — С. 26–32.
[131] См. подробнее: Сапронов Д. Ю. Особенности правового регулирования персональных данных в Китайской Народной Республике // Вестник Московского университета. Серия 26. Государственный аудит. — 2022. — № 4. — С. 149–157.

3. Запрет применения принципа «соглашайся или не пользуйся» позволяет избежать дискриминации и гарантирует справедливость в отношении потребителей.

4. Законодатели в Китае отдельно выделяют такую категорию персональных данных, как «чувствительная персональная информация», которая представлена открытым перечнем. Ее защите должно уделяться особое внимание, на обработку таких данных требуется отдельное согласие.

5. Предъявление особых требований к государственным органам при обработке персональных данных граждан позволяет избежать ситуаций, когда они могут выйти за пределы своих полномочий.

6. Оценка рисков передачи персональных данных за пределы КНР обязательна. Для этого могут привлекаться соответствующие государственные органы.

7. Обязательный аудит и сертификация систем защиты персональных данных соответствующим уполномоченным государственным органом позволяет своевременно обнаруживать возможные угрозы и риски для систем обработки персональных данных»[132].

Таким образом, использование опыта Китая при совершенствовании отечественного законодательства, регулирующего отношения в области персональных данных позволит в определённой степени повысить правовую защиту персональных данных физических лиц. Отдельного упоминания заслуживает юридическая увязка защиты персональных данных с защитой информации о частной жизни гражданина на законодательном уровне в КНР и необходимость операторам которые допустили утечку данных физических лиц доказывать свою невиновность.

Рассматривая правовые механизмы защиты персональных данных за рубежом особое внимание следует уделить законодательству Республики

[132] См.: Сапронов Д. Ю. Особенности правового регулирования персональных данных в Китайской Народной Республике. // Вестник Московского университета. Серия 26: Государственный аудит. — 2022. — № 4. — С. 149–157.

Казахстан, где сформирована комплексная система регулирования обработки персональных данных[133]. В системе конституционных гарантий Республики Казахстан особое место занимает право гражданина защиту информации, которая относится к личной, закрытой от посторонних стороне жизни человека[134]. Понятие «персональные данные» и его правовое определение в законодательстве Республики Казахстан появилось с принятием Закона № 94-V «О персональных данных и их защите» от 21 мая 2013 года[135], что создало правовую основу для дальнейшего регулирования отношений в рассматриваемой области. Этот нормативный акт регламентирует полный цикл обработки персональных данных: от первичного сбора до хранения и последующей обработки.

Закон гарантирует равные права операторам и субъектам персональных данных, а также необходимость обеспечения многоуровневой безопасности, охватывающей интересы личности, общества и государства.

Документ устанавливает, что все собираемые персональные данные — конфиденциальные, доступ к ним ограничен, но в некоторых случаях, установленных законодательством, персональные данные могут быть общедоступны. Проведённый анализ нормативного документа позволяет выделить двухуровневую классификацию персональных данных: общедоступные данные и данные ограниченного доступа. Законодательно закреплён императив: оператор обязан в суточный срок исключить из публичного доступа информацию, полученную с нарушением правовых норм; финансовые издержки, сопряжённые с этой процедурой, полностью ложатся на оператора. Сбор и обработка третьими лицами общедоступной информации о физических лицах допускаются исключительно при соблюдении условия об обязательном указании

[133] См. подробнее: Будник Р. А. Особенности публично-правовой защиты персональных (в том числе биометрических) данных на постсоветском пространстве: модель Республики Казахстан / Р. А. Будник, Д. Ю. Сапронов, Э. А. Иваева // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2024. – Т. 10, № 4. – С. 159-164.

[134] См.: Конституция Республики Казахстан (принята на республиканском референдуме 30 августа 1995 года) (с изменениями и дополнениями по состоянию на 19.09.2022 г.) // Параграф : [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=1005029 (дата обращения: 19.11.23).

[135] См.: Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 01.07.2024 г.) // Эділет : [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/Z1300000094/links (дата обращения: 22.11.23).

первоисточника сведений, обеспечивающего субъекту персональных данных, предоставляется право идентифицировать источник, из которого были получены его персональные данные. Передача сведений, идентифицирующих физическое лицо за пределы Казахстана возможна только при наличии: отдельно выраженного согласия субъекта персональных данных и гарантий обеспечения надлежащего уровня защиты передаваемой информации о физическом лице.

При детальном рассмотрении иерархии приоритетов, в документе обнаруживается явный акцент на защите интересов отдельной личности, в то время как государственные интересы занимают подчинённое положение в данной системе приоритетов. Модель регламентации обработки персональных данных в Республике Казахстан имеет сходство и в определённой степени ориентирована на европейские подходы и стандарты стандартами, где принцип защиты прав личности традиционно занимает доминирующее положение в системе правовых ценностей. Подписание Республикой Казахстан соглашения о расширенном партнёрстве с Европейским союзом в сфере защиты персональных данных демонстрирует приверженность государства курсу на интенсификацию сотрудничества с европейскими институтами.

Правовая система Республики Казахстан выстраивает механизм обработки персональных данных на принципе обязательного получения согласия субъекта либо его законного представителя, оформленного в соответствии с установленными требованиями. По аналогии с иными процедурами обработки, размещение персональных данных в общедоступных информационных ресурсах допустимо исключительно при наличии юридически оформленного согласия субъекта. Отступления от указанного порядка возможны лишь в случаях, прямо закреплённых законодательством Казахстана как обязанность по публикации определённых сведений.

Сбор персональных данных должен осуществляться с определённой, оговоренной целью, при выходе за установленные целевые рамки обработка персональных данных должна прекращаться.

В Законе системно изложены ключевые параметры деятельности государственного органа по контролю за обработкой персональных данных, а именно: круг возложенных обязанностей; границы зон ответственности; объём делегированных полномочий.

В контексте правового регулирования обработки персональных данных принципиальное значение приобретает механизм подтверждения согласия субъекта (либо его законного представителя). Реализация данной функции в соответствии с рассматриваемым документом возложена на специализированные сервисы — как государственные, так и негосударственные. Важной особенностью является то, что установлен прямой запрет на использование негосударственных сервисов контроля доступа к персональным данным в случаях, когда сбор информации о физическом лице осуществляется уполномоченными государственными органами. Оператор обязан интегрировать свою информационную инфраструктуру с государственным сервисом контроля доступа к персональным данным. Использование негосударственных сервисов операторами персональных данных возможно при соблюдении определённых условий: получение согласия или отказа субъекта (либо его законного представителя) на сбор и/или обработку персональных данных; информирование субъекта о любых действиях с его данными (просмотр, изменение, дополнение, передача, блокирование, уничтожение); уведомление о доступе третьих лиц к персональным данным субъекта.

В соответствии с действующим законодательством Республики Казахстан право субъекта персональных данных на отзыв ранее предоставленного согласия подлежит ограничению в случае: установления прямого законодательного запрета на осуществление отзыва или факта неисполнения оператором персональных данных возложенных на него нормативных обязательств.

Наличие такого сервиса обеспечивает надлежащие гарантии осуществления предусмотренного законодательством Республики Казахстан права физических лиц на защиту принадлежащих им персональных данных.

В нашей стране уже некоторое время идёт обсуждение инициативы по централизации учёта согласий на обработку персональных данных создании похожего сервиса[136].

Закон предусматривает ограниченный перечень исключительных случаев, допускающих отступление от общеустановленных требований при обработке персональных данных, включая такие области как: деятельность правоохранительных органов, судов и иных уполномоченных государственных органов в рамках возбуждения и рассмотрения дел об административных правонарушениях, а также ведения исполнительного производства; реализацию функций государственной статистической деятельности; обработку персональных данных соответствующими государственными органами в сфере финансового контроля, а также в области налогового и таможенного администрирования; деятельность связанную с хранением резервных копий электронных информационных ресурсов с персональными данными ограниченного доступа на единой платформе.

Рассмотрев положения Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» можно сделать вывод следующий вывод: документ ориентирован на нормативное упорядочение автоматизированных процессов, связанных с хранением и обработкой персональных данных; положения учитывают современные технологические условия функционирования информационных систем; некоторые принципов и подходы схожи с положениями законодательства Европейского союза в сфере защиты персональных данных.

Проведённое исследование содержания Закона Республики Казахстан № 94-V от 21.05.2013 «О персональных данных и их защите» демонстрирует его адекватность современным вызовам информационного общества. Законодательный акт обеспечивает необходимую нормативную базу для

[136] См.: Новый сервис позволит проверять и отзывать согласия на обработку персональных данных на "Госуслугах" // Российская газета : [Электронный ресурс]. URL: https://rg.ru/2025/08/28/na-gosuslugah-mozhno-budet-otozvat-soglasiia-na-obrabotku-personalnyh-dannyh.html (дата обращения: 28.09.25).

формирования действенной системы охраны персональных данных физических лиц.

Изучение правовых механизмов защиты персональных данных Республики Казахстан позволяет заключить: опыт в сфере верификации согласия на обработку данных Казахстана может послужить эффективной базой для разработки нормативной методологии совершенствования законодательства Российской Федерации, регулирующего обработку персональных данных.

Рассматривая зарубежный опыт правового регулирования хранения и обработки персональных данных, можно сделать вывод о том, что первые нормативные акты, регулирующую эту сферу стали приниматься в 70-х годах прошлого века. Повсеместное их появление связано со сменой этапов развития информационных технологий, увеличением роли вычислительной техники при обработке персональных данных и внедрением компьютерных сетей и сети Интернет. С развитием информационно-коммуникационных технологий подвергались изменениям и нормы права, регулирующие соответствующие отношения. В Швеции, Германии, а позднее в Европейском союзе, Китае и Республике Казахстан, это породило централизованную модель регулирования; в США же, и ряде других стран, прижилась децентрализованная модель законодательства по защите персональных данных.

Централизованная модель регулирования персональных данных подразумевает, что регулирование хранения, обработки и использования персональных физических лиц, основано на единых подходах, которые закреплены в одном общегосударственном нормативном акте, и контролируется одним контрольным органом. Для децентрализованной системы характерно наличие отраслевых нормативных актов и отсутствие единых подходов к регулированию использования персональных данных, а также отсутствие единого контрольного органа. Частным случаем является смешанная система регулирования использования персональных данных, для неё характерно наличие одного или нескольких признаков централизованной или децентрализованной систем. С целью совершенствования российского законодательства, регулирующего защиту

персональных данных, российским законодателям следовало бы использовать передовой опыт КНР, ЕС, США и Республики Казахстан в этой области, переработав его под отечественные реалии.

Подходы иностранных государств к решению задач, связанных с совершенствованием законодательства в этой сфере, в значительной степени разнятся. Однако, несмотря на это, выработанные юридические конструкции оказываются эффективными и позволяют решать необходимые для государства задачи.

Российской Федерации для использования зарубежного опыта следует учитывать особенности отечественного законодательства, и адаптировать некоторые успешные зарубежные решения к российским реалиям. К ним можно отнести, например, некоторые, представляющие интерес нормы, из законодательства КНР: выделение специальной правовой категории «чувствительных персональных данных», обязательный независимый аудит информационных систем обработки персональных данных, юридическое закрепление тождественности принципов защиты информации о частной жизни с аналогичными принципами защиты персональных данных. Кроме этого, некоторые механизмы законодательства Республики Казахстан также выглядят достаточно эффективно для анализа и адаптации к российской действительности, в частности механизм проверки, учёта и отзыва поданных заявлений о согласии на обработку персональных данных через единую государственную информационную систему, а также ряд других правовых конструкций казахского законодательства в рассматриваемой области. Не менее актуальным представляется анализ, и возможное использование в работе над совершенствованием отечественного законодательства опыта Европейского Союза, например, принципы и подходы, применяемые к нарушителям правил обработки персональных данных.

Таким образом, анализ зарубежного опыта в области правовой защиты персональных данных может обогатить отечественную юридическую науку новыми эффективными юридическими конструкциями в области правовой защиты

персональных данных. Это позволило бы урегулировать ряд проблем, которые не в полной мере охвачены отечественным законодательством.

ГЛАВА 2 Особенности совершенствования информационно-правового регулирования отношений зависимых от персональных данных

§ 2.1 Цифровизация социальных отношений и трансформация информационно-правового регулирования обработки персональных данных

Появление вычислительной техники оказало огромное влияние на общество. Множество операций, которые выполнялись вручную, стали автоматизироваться. Со временем компьютеры стали объединяться в сети, в результате чего появилась «Сеть Сетей» или глобальная информационная сеть Интернет. Этот факт способствовал тому, что множество привычных для обычного человека сервисов обзавелось Интернет-версией, начиная от различных магазинов и заканчивая вызовом такси, заказом еды, телемедициной и приобретением недвижимости. Использование в различных сферах общественной жизни информационно-коммуникационных технологий стали называть «цифровизацией»[137] — от английского *digital (*что не совсем корректно переведено как *«цифровой»*; в некоторых вариантах перевода данный термин определяется, помимо слова «цифровой», ещё и как «электронный»*)*. Распространение цифровых сервисов в последние годы стало все более повсеместным, что привело к кардинальной перестройке экономики и права во многих странах, ощутимому переформатированию общественных отношений.

Важной особенностью цифровизации социальных отношений является то, что она — не только ключевой фактор, на который опирается экономический рост, но и новый элемент, который влияет на государственный суверенитет, стабильность и национальную безопасность государства. Об этом говорится в Стратегии национальной безопасности Российской Федерации — «быстрое

[137] См.: Глоссарий понятий и терминов, используемых в исследовании проблем декартелизации экономики, включая ее цифровой сегмент. // ИПРАН РАН : [Электронный ресурс]. URL: https://www.issras.ru/competition/glcon_a.php (дата обращения: 25.11.23).

развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства»[138] (раздел: информационная безопасность).

В последнее время всё чаще говорят о таком понятии, как «цифровой суверенитет». В правовой доктрине определение ещё не сформировалось, однако его содержательные характеристики могут быть представлены следующим образом: «использование отечественного IT-оборудования и приоритетную поддержку отечественных IT-компаний в цифровой сфере; обеспечение безопасности национальной интернет-инфраструктуры, национального интернет-трафика; национальную организацию по использованию больших данных в рамках национального государства»[139]. Особенно этот вопрос актуализировался в последние годы, после усиления санкционного воздействия на нашу страну. Зарубежные компании стали ограничивать доступ к своим продуктам, не только российским государственным и негосударственным организациям, но и физическим лицам. Кроме этого, широкое распространение носимых устройств и смартфонов, использующих зарубежное программное и аппаратное обеспечение, постоянно собирающих огромное количество персональных данных, требует выработки таких правовых подходов, которые бы учитывали и вопрос национальной безопасности в контексте масштабного применения новых информационных технологий, в том числе, и обработки персональных данных.

Фактор цифровизации социальных отношений привёл к тому, что возникла необходимость выработки оценочных критериев эффективности этого процесса. Неслучайно «показатель “Информационная безопасность”, вошедший в рейтинг руководителей цифровой трансформации в июле текущего года, будет рассчитываться на ежемесячной основе»[140], — обязательное введение Министерством цифрового развития, связи и массовых коммуникаций Российской

[138] См.: Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ, 05.07.2021, № 27 (часть II), ст. 5351.
[139] См.: Brokeš F. Russia’s Sovereign Internet // Central European Financial Observer. 2018 : [Электронный ресурс]. URL: https://financialobserver.eu/cse-and-cis/russias-sovereign-internet/ (дата обращения: 26.11.23)
[140] См.: Минцифры заявило о ежемесячном расчете показателя информбезопасности чиновников // ТАСС : [Электронный ресурс]. URL: https://tass.ru/ekonomika/18566019 (дата обращения: 26.11.23).

Федерации (Минцифры) такого показателя как одного из критериев оценки эффективности лиц, ответственных за цифровое развитие означает фокусирование внимания государства на такой важной составляющей цифровизации как информационная безопасность.

Российское научное юридическое сообщество сходится во мнении, что затронутые вопросы имеют крайне важное значение для нашей страны. В. А. Вайпан в своих работах характеризует влияние цифровизации на социальные отношения как систему экономических взаимодействий субъектов, в которой именно данные в цифровой форме выступают фундаментальным фактором производства[141]. В юридическое литературе отмечается значимость цифровизации: «современные информационные технологии — bigdata, облачные технологии, блокчейн, смарт-контракты и другие, открывают окно возможностей для системного решения многих проблем, связанных с недостаточной эффективностью государственного управления»[142]. Т. А. Полякова также акцентирует внимание на важности вопроса цифровой трансформации: «Следует признать, что цифровизация как импульс эволюционных, инновационных изменений должна стать определенной базой не только в экономике, но и в сфере государственного управления»[143].

В 2017 году на Петербургском международном экономическом форуме, Президент Российской Федерации подчёркивал: «необходимо сформировать принципиально новую, гибкую нормативную базу для внедрения цифровых технологий во все сферы жизни. При этом все решения должны приниматься с учетом обеспечения информационной безопасности государства, бизнеса и граждан»[144]. В своих работах специалисты по информационному праву отмечают: «Важно учитывать, что указанные мероприятия, требуют не внесения точечных

[141] См.: Проблемы гармонизации экономических отношений и права в цифровой экономике: монография / отв. ред. В. А. Вайпан, М. А. Егорова. М. : Юстицинформ, 2020. С. 13.
[142] См.: Шахрай С. М. Цифровая конституция. основные права и свободы личности в тотально информационном обществе // Вестник Российской академии наук 2018. Том 88. № 12. С. 1075–1082.
[143] См.: Полякова Т. А. Влияние цифровой экономики на развитие транспортной отрасли и проблемы обеспечения информационной безопасности: правовой аспект // Транспортное право и безопасность. 2019. № 1 (29). С. 82–86.
[144] См.: Путин: Россия ускорит внедрение цифровых технологий // Вести.RU : [Электронный ресурс]. URL: https://www.vestifinance.ru/articles/86338 (дата обращения: 17.11.23).

изменений, а направлены на системное и обоснованное формирование правовых и регуляторных условий для развития цифровой экономики, что требует фундаментальных правовых исследований, прежде всего в области правового обеспечения информационной безопасности»[145].

Появление у привычных обществу сервисов «цифровой» составляющей привело к увеличению массива обрабатываемых персональных данных. Это породило феномен «цифровых следов». «Цифровой след, иногда называемый цифровой тенью — это данные, которые вы оставляете при использовании интернета. Эти данные включают посещаемые веб-сайты, отправляемые электронные письма и информацию, указываемую в онлайн-формах. Цифровой след можно использовать для отслеживания действий физического лица и его устройств в интернете. Пользователи глобальной сети активно или пассивно создают собственный цифровой след»[146]. Следовательно, использование сети Интернет приводит к тому, что о человеке скапливается множество различной информации, которая как явно, так и неявно, может содержать персональные данные. И не всегда индивидуум желал бы, чтобы эта информация о нём была сохранена и обработана. Сбор таких сведений, на первый взгляд, может казаться бесполезным, потому, что они во многих случаях обезличены и достаточно разрознены. Однако имея такую информацию, её можно использовать для так называемого «профайлинга»[147] (от англ. Profile), который появился в 40-е годы XX века в США, как метод поведенческого анализа человека, и с 1970-х годов стал применяться правоохранительными органами для выявления опасных лиц. Позднее данный метод поведенческого анализа стал использоваться и в других сферах.

[145] См.: Полякова Т. А., Минбалеев А. В., Бойченко И. С. Концептуальные подходы к правовому регулированию информационной безопасности в условиях цифровизации и трансформации права // Вестник УрФО. Безопасность в информационной сфере. 2019. № 3 (33). С. 64–68 (дата обращения: 17.11.23).
[146] См.: Что такое цифровой след? // АО «Лаборатория Касперского» : [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/definitions/what-is-a-digital-footprint (дата обращения: 25.11.23).
[147] Профайлинг представляет собой совокупность психологических методов оценки и прогнозирования поведения человека на основе анализа его наиболее информативных частных признаков, характеристик внешности, вербального и невербального поведения (Вереникина Н. А. Профайлинг как средство раскрытия и расследования преступлений // Актуальные проблемы российского права. — 2017. — № 9(82). — С. 203–209).

С развитием вычислительной техники и появлением технологии bigdata, а также широкого использования нейросетей для обработки больших массивов информации, профайлинг получил новые инструменты и возможности. А поскольку важным компонентом поведенческого анализа является обработка личной информации, то, как следствие, проблема повсеместного сбора таких сведений, даже в опосредованном виде, стала всё сильнее влиять на право личности защищать информацию о себе.

Общественные отношения, связанные с жизненным циклом персональных данных, претерпели определённые изменения в контексте автоматизации их обработки в рамках цифровизации экономии:

— персональные данные собираются постоянно;

— хранение, обработка, передача и анализ персональных данных значительно упростились;

— доступ к хранимым персональным данным стал практически мгновенным, вследствие чего получение несанкционированного доступа злоумышленников к ним упростилось;

— современные технологии позволяют в реальном времени идентифицировать физическое лицо, в том числе и с использованием биометрической и иной информации;

— объём собираемой информации о физических лицах постоянно увеличивается.

В современных условиях перед государством и юридической наукой возникла задача актуализации нормативно-правового регулирования обработки персональных данных, обусловленная трансформацией общественных отношений. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ был принят почти 20 лет назад, и, несмотря на все вносимые в него изменения, постоянно устаревает и во многом не учитывает развитие современных информационно-коммуникационных технологий и их влияние на сферу обработки персональных данных. Основная причина этой проблемы в том, что рассматриваемый Закон изначально был ориентирован на общественные отношения другого формата, когда

персональные данные обрабатываются и хранятся на бумажных, а не электронных носителях. Применение же автоматизированных информационных технологий произвело революцию и сделало информацию о физических лицах стратегически важным ресурсом, получение, обработка и анализ которого облегчились многократно.

Кроме этого, идентификация личности и подтверждение юридически значимых действий в сети стали играть важную роль во множестве сфер общественной жизни. Именно то, что при использовании цифровых сервисов, идентификация физического лица происходит в Интернете и является одной из ключевых особенностей современных социальных отношений в информационном обществе, и как следствие, в цифровой экономике.

Отечественное научное сообщество столкнулось с непростой задачей, связанной с необходимостью, как выработки технических решений, повышающих достоверность идентификации личности в цифровой среде, так и правового обеспечения этого процесса.

Традиционная верификация личности обычно проводится по удостоверению личности, собственноручная подпись физического лица подтверждает волеизъявление (ст. 160, п. 2 ст. 434 ГК РФ). В сети Интернет используются другие методы идентификации и фиксирования согласия, которые не всегда могут обеспечить достоверность, потому что:

— подтверждение личности осуществляется дистанционно, индивидуум не присутствует физически;

— точность дистанционной процедуры идентификации не всегда такая же, как если бы она происходила при личном присутствии идентифицируемого лица;

— важной особенностью сетевой идентификации физического лица является несовершенство регламентов и стандартов.

Отличительные особенности, относящиеся к электронной обработке персональных данных: возможность почти мгновенного несанкционированного доступа к хранимой личной информации, не всегда достоверная идентификация физических лиц. С этими проблемами столкнулись правительства многих

государств, что потребовало от них разработки правовых механизмов защиты, персональных данных, хранимых в различных информационных системах, а также выработки правовых подходов к дистанционной идентификации личности.

Широкое распространение определение личности с использованием сети Интернет послужило причиной появления «синтетических ID»[148] — никогда не существовавших, полностью виртуальных личностей, которые включают в себя персональные данные настоящих людей.

В США с использованием виртуальных личностей было получено кредитов более чем на 300 млн. долларов[149]. Дальнейший рост цифровизации социальных отношений будет способствовать росту числа мошенничеств с поддельными личностями, особенно, если процесс идентификации физического лица в сети Интернет не будет в достаточной степени достоверен. Помимо совершения мошеннических действий в финансовой сфере, несовершенство процедур онлайн-идентификации способствует росту числа угроз в сфере информационной безопасности. Виртуальные личности могут быть использованы нелегальными мигрантами. В нашей стране эта проблема не получила широкого распространения[150], но ускорение дальнейшего роста цифровизации экономики может актуализировать вопрос точности электронной идентификации физического лица.

Ущерб от несовершенства механизмов идентификации личности в Интернет-пространстве может быть не только финансовым, из-за изначально невозвратных кредитов, но и создавать напряжённость в обществе и недоверие к цифровым сервисам. Для повышения надёжности и достоверности процедуры подтверждения личности через Интернет следует рассмотреть обязательность считывания биометрических данных индивидуума в реальном времени, где уникальным

[148] См.: The New Face of Fraud: What You Need to Know About Synthetic ID Theft. // Safety.com : [Электронный ресурс]. URL: https://www.safety.com/synthetic-identity-theft/ (дата обращения: 28.11.23).
[149] См.: Есть ли шанс у цифровой идентификации в России. // EY Russia : [Электронный ресурс]. URL: https://www.ey.com/Publication/vwLUAssets/ey-digital-id-survey-rus/$FILE/ey-digital-id-survey-rus.pdf (дата обращения: 28.11.23).
[150] См.: What is Synthetic Identity Fraud? // Credit and Fraud Risk Solutions & Analitics — ID Analytics. : [Электронный ресурс]. URL: https://www.idanalytics.com/solutions-services/fraud-risk-management/synthetic-identity-fraud/ (дата обращения: 1.12.23).

критерием для подтверждения личности могут выступать дактилоскопические данные или другая аналогичная информация, а не только геометрия лица или сличение по голосу. Электронное считывание отпечатка пальца[151] за последние годы стало достаточно технически отработано, в том числе при помощи мобильных телефонов, также эта процедура может служить одним из инструментов проверки подлинности личности при совершении юридически значимых действий. Запрос на ввод дактилоскопической или иной биометрической информации, являющийся частью процедуры идентификации личности при удалённой идентификации, в значительной мере повысит её достоверность и надёжность.

Работа в этом направлении уже ведётся, принят Федеральный закон № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации»[152]. Документ задаёт правовые параметры регулирования отношений, складывающихся при использовании «Единой биометрической системы» (далее — ЕБС) для проведения процедуры биометрического установления личности. Основным функционалом системы на данный момент является использование её финансово-кредитными организациями для идентификации клиентов. Пока работа ЕБС не подразумевает хранения дактилоскопической информации, там хранится только изображение лица и образец голоса. Добавление дактилоскопической информации в такую систему позволило бы расширить перечень биометрических признаков, по которым можно проводить идентификацию физических лиц через биометрию.

Одним из инструментов идентификации личности в цифровую эпоху мог бы стать электронный паспорт гражданина Российской Федерации. Цифровое

[151] См.: Распознавание отпечатков пальцев. // Национальная библиотека им. Н. Э. Баумана : [Электронный ресурс]. Электронный ресурс URL: https://ru.bmstu.wiki/Распознавание_отпечатков_пальцев (дата обращения: 1.12.23).
[152] См.: Федеральный закон № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации // Собрание законодательства РФ, 02.01.2023, № 1 (часть I), ст. 19.

удостоверение личности позволило бы выстроить процесс идентификации личности на базе современных цифровых технологий в рамках цифровизации экономики. Внедрение электронного паспорта позволило бы выстроить достоверную и точную дистанционную идентификацию физических лиц.

Работа по его созданию уже началась в нашей стране: «В апреле в МВД раскрыли подробности механизма выдачи гражданам России паспортов нового образца в виде карты с электронным чипом (ПЭН). В ведомстве рассказали, что российское правительство поручило организовать выдачу ПЭН на территории Москвы начиная с 1 декабря 2021 года. При этом отмечалось, что замена бумажного паспорта смарт-картой не будет обязательной»[153]. Таким образом, нормативная база для введения цифровых удостоверений личности была практически готова. Но, к сожалению, летом 2022 года Министерство цифрового развития, связи и массовых коммуникаций заявило о заморозке проекта выдачи электронных паспортов[154]. Среди причин назывались сложности с технической документацией, с требованиями к безопасности и т.д. Таким образом, несмотря на острую необходимость во внедрении цифрового идентификатора личности, проект был заморожен и сроки его разморозки не озвучены. Однако весной 2023 года Минцифры предложило[155] «установить, что предъявление гражданином Российской Федерации (далее — гражданин) сведений в электронном виде из документов, удостоверяющих личность, либо из иных, выданных гражданину государственными органами, документов (далее — сведения) с использованием мобильного приложения федеральной государственной информационной системы "Единый портал государственных и муниципальных услуг (функций)" (далее — мобильное приложение) приравнивается к предъявлению указанных документов в

[153] См.: В МВД заявили о готовности к введению в России электронных паспортов // ИЗВЕСТИЯ : [Электронный ресурс]. URL: https://iz.ru/1228574/2021-09-29/v-mvd-zaiavili-o-gotovnosti-k-vvedeniiu-v-rossii-elektronnykh-pasportov (дата обращения: 3.12.23).
[154] См.: Минцифры заморозило проект электронного паспорта на неопределенный срок // ТАСС : [Электронный ресурс]. URL: https://tass.ru/obschestvo/14885335 (дата обращения: 1.12.23).
[155] См.: Минцифры предложило разрешить использовать приложение «Госуслуг» вместо паспорта // Ведомости : [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/news/2023/04/13/970836-mintsifri-predlozhilo-razreshit (дата обращения: 3.12.23).

случаях, определяемых Правительством Российской Федерации»[156]. Предлагаемый Министерством цифрового развития вариант идентификации физических лиц через специальный сервис, на данном переходном этапе развития информационного общества можно считать оптимальным, и наиболее эффективным по причине того, что для практической реализации такого механизма достаточно несколько расширить функционал имеющегося мобильного приложения для информационной системы «Госуслуг» и принять соответствующие изменения в законодательство. Таким образом, к имеющимся вариантам идентификации личности по бумажным документам, добавится возможность использовать для этой процедуры сведения из системы «Госуслуги». Это будет способствовать тому, что процедура идентификации физического лица получит цифровую составляющую, которую в дальнейшем можно будет дополнить другими методами, в том числе и разработкой цифрового паспорта гражданина.

Процесс реализации концептуальной идеи о цифровом сервисе для предъявления документов, удостоверяющих личность, занял несколько лет: практическая реализация последовала значительно позже выдвижения первоначальной инициативы, с принятием Федерального закон от 24.06.2025 № 156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации»[157]. Документ юридически устанавливает тождественность демонстрации удостоверения личности через такой сервис и предъявления оригиналов идентификационных документов. Появление такого сервиса с функцией определения личности физического лица станет отправной точкой на пути внедрения электронного паспорта в Российской Федерации. Такой подход позволит начать перестраивать всю систему идентификации физических лиц, не только в дистанционный формат, но и в реальном пространстве. С течением

[156] См.: О предъявлении документов с использованием информационных технологий // Федеральный портал проектов нормативных правовых актов. URL: https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=137532# (дата обращения: 3.12.23).
[157] См.: Федеральный закон от 24.06.2025 № 156-ФЗ "О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации". // Собрание законодательства РФ, 30.06.2025, № 26 (часть I), ст. 3486.

времени, когда система будет отлажена, гражданам потребуется всё меньше и меньше предоставлять ксерокопии своих идентификационных документов по месту требования; процесс хранения информации о них можно будет автоматизировать. Кроме того, сама процедура определения личности индивидуума при помощи многофункционального сервиса будет более безопасной и точной, чем при демонстрации бумажного удостоверения личности, которое можно подделать[158].

Резюмируя, можно сделать вывод о том, что обеспечение защиты персональных данных граждан и достоверной удалённой идентификации личности являются одними из приоритетных задач государства.

Проанализировав последствия повсеместного применения информационно-коммуникационных (цифровых) технологий, можно заключить, что её воздействие имеет сложный и многоуровневый характер, особенно это коснулось защиты персональных данных физических лиц. Значительное изменение общественных отношений потребовало пересмотра законодательства в области защиты персональных данных и идентификации личности. В последнее время стали появляться различные законодательные инициативы, призванные решить те или иные задачи, связанные с идентификацией личности в условиях повсеместного внедрения цифровых сервисов. Однако, несмотря на множество требующих внимания проблем и вызовов в этой области, работа по совершенствованию законодательства, связанного с идентификацией физических лиц и защитой их данных, даже учитывая принятие национального проекта «Цифровая экономика Российской Федерации» и внимание к этой области высшего руководства страны, ведётся фрагментарно, и не всегда системно. Значительное количество законодательных инициатив в рассматриваемой области не связано между собой и может не учитывать влияния друг друга на регулирование обработки персональных данных, а также не всегда учитывает интересы всех вовлечённых сторон: личности, государства и общества.

[158] См.: В 2023 году число случаев подделки доверенностей и судебных приказов выросло на 12% // Smart Engines : [Электронный ресурс]. URL: https://smartengines.ru/news/report-2023/ (дата обращения: 4.12.23).

Можно констатировать, что: «Несмотря на амбивалентность цифровых технологий, необходимо признать, как факт: тотальную цифровизацию общества и всех его систем, включая личную жизнь, нельзя остановить. Возможно, есть шанс замедлить развитие цифровых процессов в отдельных сегментах, например, в признании криптовалюты законным платёжным средством. Но, скорее всего, такое решение нужно лишь для того, чтобы выиграть время для создания систем контроля цифровой стихии и обеспечения хоть какой-то синхронизации эволюции человека и технологий»[159]. Поэтому государству необходимо интенсифицировать усилия по адаптации действующего законодательства к требованиям эпохи глобальной цифровизации.

Возможно, для решения этой проблемы следует организовать более тесное взаимодействие государства и общества. Исполнителем федерального проекта «Нормативное регулирование цифровой среды» являлось Министерство экономического развития Российской Федерации[160]. Кроме того, существует «Правительственная комиссия по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности»[161]. Также вопросами адаптации законодательства в области правового обеспечения цифровой экономики занимается «Комиссия по правовому обеспечению цифровой экономики» Ассоциации Юристов России. Объединение усилий всех заинтересованных сторон, в том числе и представителей «Совета по правам человека при Президенте РФ» и представителей Российской Академии Наук, на единой площадке, которая будет иметь статус экспертно-консультативного органа по вопросам цифровой трансформации отечественного права, позволит более системно и эффективно осуществлять адаптацию отечественного законодательства под новые реалии и

[159] См.: Шахрай С. М. Цифровая конституция. основные права и свободы личности в тотально информационном обществе // Вестник Российской академии наук. — 2018. — Т. 88, № 12. — С. 1075–1082.
[160] См.: «Нормативное регулирование цифровой среды». // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : [Электронный ресурс]. URL: https://digital.gov.ru/ru/activity/directions/862/ (дата обращения: 6.12.23).
[161] См.: Правительственная комиссия по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности. // Правительство России : [Электронный ресурс]. URL: http://government.ru/department/492/about/ (дата обращения: 6.12.23).

задачи. Повышенное внимание экспертов должно быть сосредоточено на сфере защиты персональных данных и идентификации личности в сети Интернет. Такой подход будет способствовать более детальной проработке законодательных инициатив в сфере обработки персональных данных, и позволит более системно выстроить законотворческую деятельность в рассматриваемой области.

§ 2.2 Воздействие цифровизации государственного управления на правовую защиту персональных данных

Динамика развития вычислительных систем обусловила трансформацию личности, общества и государственных институтов, при этом использование информационных технологий в повседневной деятельности становится всё более интенсивным[162]. Широкое распространение цифровых технологий стало затрагивать права человека[163]. Помимо этого, внедрение автоматизированных информационных технологий начало оказывать влияние и на сферу государственного управления; систем, используемых государственными организациями, государственных информационных систем (ГИС), становится всё больше. Некоторые исследователи предлагают рассмотреть в достаточной степени спорную идею о том, чтобы считать их одним из источников права[164]. В последнее время появляется всё больше информационных систем, имеющих статус государственных, а также используемых государственными органами и организациями, которые обрабатывают и хранят персональные данные[165].

Автоматизированная обработка персональных данных и использование сети Интернет[166] привели к тому, что злоумышленники получили возможность иметь

[162] См.: Корецкий А. С. Управление процессами трансформации предприятия в условиях цифровой экономики // Вестник Московского университета. Серия 21: Управление (государство и общество). — 2021. — № 1. — С. 48-63.
[163] См.: Бобунова С. А. Персональные данные и цифровизация. // Молодой ученый. — 2022. — № 36 (431). — С. 75–79.
[164] См.: Амелин Р. В. Использование государственных информационных систем как форм (источников) права: перспективы и проблемы // Вестник Московского университета. Серия 21: Управление (государство и общество). — 2021. — № 4. — С. 3–15.
[165] См.: Колюшин Е. И. Правовые проблемы электронизации (цифровизации) выборов // Вестник Университета имени О. Е. Кутафина. — 2019. — №. 9 (61). — С. 103–113.
[166] См.: Антонова В. В. Проблемы и решения правового регулирования защиты персональных данных // Учет и контроль. — 2022. — № 3. — С. 15–17.

практически мгновенный доступ к ним. В связи с этим, участились атаки на информационную инфраструктуру, в том числе и с целью завладения информацией о физических лицах; вопрос правовой защиты таких сведений должен являться одним из приоритетов государственной информационной политики[167]. Это обусловлено исключительной ценностью для государства персональных данных, а также чувствительностью такой информации к утечкам.

Становление Интернета как глобальной информационной инфраструктуры привело к тому, что множество привычных для обычного человека сервисов стали использовать её для взаимодействия с конечным потребителем. Помимо распространённых услуг, таких, как аренда машин, заказ еды, приобретение различных товаров, появилась возможность совершать юридически значимые действия используя технологию электронной подписи[168]. Теперь стало возможно, не посещая офис застройщика, приобрести квартиру, или получить кредит, не посещая банк, что, несомненно, удобно для потребителей, но порождает ряд проблем правовых проблем, связанных с защитой персональных данных[169].

Особенно на цифровизацию государственного управления повлияла пандемия COVID-19. По мнению иностранных исследователей, именно она стала тем фактором, который ускорил цифровизацию не только бизнеса, но и государства[170]; кроме этого, в своих работах они отмечают, что вынужденная цифровизация повлияла на отношение властей к применению новых технологий в государственном[171] и местном управлении[172]. Ещё одним вопросом, который зарубежные авторы рассматривают в своих научных работах, является проблема

---

[167] См.: Бочарникова А. Д. Модернизация государственного управления в условиях цифровизации общества // 25 лет конституционного развития России и проблемы государственного управления: материалы межвузовской научно-практической конференции, Краснодар, 12 декабря 2018 года. — Краснодар: Кубанский государственный университет. — 2018. — С. 246–249.

[168] См.: Применение электронной подписи // ФНС России : [Электронный ресурс]. URL: https://www.nalog.gov.ru/rn77/related_activities/el_doc/use_electronic_sign/.(дата обращения: 9.08.2023).

[169] См.: Сергеева Н. Ю. Защита персональных данных граждан Российской Федерации в сети Интернет: отдельные проблемы правового регулирования, Л. Т. Шарудинова // Гражданин и право. — 2021. — № 9. — С. 89–92.

[170] См.: Moser-Plautz B. COVID-19 and digitalization: The great acceleration. // Sciencedirect : [Электронный ресурс]. URL: https://www.sciencedirect.com/science/article/pii/S0148296321005725 (дата обращения: 9.08.2023).

[171] См.: Barrutia J. M. Effect of the COVID-19 pandemic on public managers' attitudes toward digital transformation // Technology in Society —2021 — Vol. 67 — P. 101776.

[172] См.: Черкасов А. И. Цифровизация местного управления и ее особенности в европейских странах // Сравнительное конституционное обозрение. 2024. № 1 (158). С. 90–109.

роста объёмов сбора медицинских данных физических лиц из-за использования цифровых технологий во время пандемии COVID-19. Это вызвало множество научных дискуссий относительно правового режима собираемой информации, как за границей[173], так и в нашей стране.

Применение новых технологий в значительной мере повлияло на государственное администрирование[174] и управление в субъектах Федерации[175], цифровизация которых идёт по многим направлениям[176] и последние годы всё сильнее набирает обороты[177]. Этот процесс не только повышает эффективность и является благом для системы публичного управления[178], но и несёт в себе различные риски, о чём пишут в своих работах отечественные учёные[179]. Они отмечают, что информационная безопасность должна стать важным приоритетом информационной политики государства[180]. В некоторых научных изысканиях указывается на недостаточность проработки вопросов цифровой трансформациии и на уровне бизнеса[181]. Подтверждается необходимость усиления внимания государства к этой области и её регулированию, по причине возникающих сложностей с саморегулированием.

---

[173] См.: Amankwah-Amoah J. COVID-19 and digitalization: The great acceleration // Journal of Business Research. — Vol. 2021 — № 136 — P. 602–611.

[174] См.: Николаева К. С. Цифровизация государственного управления как условие снижения транзакционных издержек в сфере публичного управления // Современный город: власть, управление, экономика. — 2021. — Т. 1. — С. 40–47.

[175] См.: Лясковская Е. А., Григорьева К. М., Халилова Г. Р.. Цифровизация государственного и муниципального управления в субъектах российской федерации. // Вестник Южно-Уральского государственного университета. Серия «Экономика и менеджмент». — 2023. — Том 17 № 4. — С.29–42.

[176] См.: Панина О. В., Красюкова Н. Л., Дорофеев А. Н., [и др.]. Выявление направлений совершенствования государственного управления за счет цифровизации государственного управления // Цифровизация государственного управления. — М.: "Издательство Прометей". — 2023. — С. 210–294.

[177]См.: Кудина М. В., Ишеков К. А., Ленков И. Н. Теории и практики государственного управления в современных условиях (итоги работы секции ежегодной научной конференции "Ломоносовские чтения" в 2021 Г.) // Вестник Московского университета. Серия 21: Управление (государство и общество). — 2021. — № 2. См.: — С. 67–102.

[178] См.: Заславская. Н. М. Пределы цифровизации государственного экологического управления // Правовое государство: теория и практика. — 2024. — № 4(78). — С. 44–54.

[179] Зубарев С. М. Правовые риски цифровизации государственного управления // Актуальные проблемы российского права. — 2020. №6 (115). — С 23–32.

[180] См.: Гринько С. Д. Противодействие посягательствам на информационную безопасность // Право и государство: теория и практика). — 2020. — № 3 (183). — С. 246–249.

[181] См.: Корецкий А. С. Управление процессами трансформации предприятия в условиях цифровой экономики / А. С. Корецкий // Вестник Московского университета. Серия 21: Управление (государство и общество). — 2021. — № 1. — С. 48–63.

Доступ к множеству государственных и муниципальных сервисов теперь можно получить через Интернет, с каждым годом их количество увеличивается[182]. Таким образом, появление цифровой составляющей у государственных и муниципальных услуг привело к тому, что они стали доступнее, их теперь можно получить дистанционно, но для этого необходимо предоставить свои персональные данные. Высокая доступность стала возможна за счёт организации межведомственного электронного взаимодействия, что, как отмечают некоторые исследователи в своих работах, требует обеспечения должного уровня информационной безопасности[183]. Это особенно важно в условиях интенсификации обмена персональными данными физических лиц между государственными органами. Т. А. Полякова пишет: «Также краткосрочным мероприятием по совершенствованию регуляторной среды обеспечения информационной безопасности является утверждение требований к устойчивости и безопасности сетей связи и оборудования органов государственной власти»[184]. Таким образом, цифровизация государственного управления требует всестороннего подхода, и адаптации действующего законодательства к изменениям в общественных отношениях в области обработки персональных данных.

Эффективность государственного управления зависит от множества различных факторов, но основополагающим и одним из ключевых, является то, сможет ли государство выстроить хорошо работающий непротиворечивый механизм обработки и защиты персональных данных, и своевременно осуществить актуализацию законодательства в этой области. Вот что об этом пишет А. А. Тедеев: «Возникает вопрос уже не о поиске юридических конструкций, которые бы позволили эффективно регламентировать отдельные особенности

[182] См.: Цацулин А. Н., Куприн А. А., Данилова Т. В., Сошников А. В. Потенциал модернизации государственного управления в эпоху цифровизации экономики // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 3: Экономические, гуманитарные и общественные науки. — 2019. — № 1. — С. 9–13.
[183] См.: Кнышоид М. З. Особенности правовой защиты персональных данных в рамках межведомственного электронного документооборота // Образование и право. — 2023. — № 2. — С. 151–158
[184] См.: Полякова Т. А., Бойченко И. С. "Информационная безопасность через призму национального проекта «цифровая экономика»: правовые проблемы и векторы решений" // Право и государство: теория и практика. — №. 2 (170). — 2019. — С. 97–100.

регулируемых соответствующей отраслью права общественных отношений, частично происходящих в киберпространстве (или отягощенных существенными информационными элементами), а о полной трансформации самих таких регулируемых общественных отношений, а значит, и внутренней организации соответствующей новым вызовам системы права»[185]. Важной особенностью такой трансформации права должен быть баланс между интересами государства и соблюдением прав граждан, особенно это относится к конституционным правам.

Важной вехой, связанной с цифровизацией государственного и муниципального управления, стало решение о создании «Единого федерального информационного регистра населения Российской Федерации» (далее — Регистр). Федеральный закон от 08.06.2020 № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации». Это событие ознаменовало собой начало централизации обрабатываемых государственными органами данных о населении. Современные информационно-коммуникационные технологии позволили решить важную проблему государственного управления, связанную со сбором, хранением и анализом информации о населении страны. Все государственные организации обрабатывают сведения о физических лицах, кто-то в большей степени, кто-то в меньшей. Во многих случаях эта информация дублируется, не обновляется, иногда искажается, теряется. Это выливается в чудовищные искажения статистических данных, которые могут обнаружиться через годы: «В марте 2013 г. полпред президента на Северном Кавказе А. Хлопонин вдруг заявил, что в регионе «потерялось» 110 тыс. детей: они по документам родились, но в школу не пошли… Материнский капитал введён в России с 2007 года, а значит, первые ”фиктивные дети“, придуманные ради получения средств, к 2013 г. как раз достигли школьного возраста. Системная проблема даже не в объёме маткапитала, который теоретически могли украсть (это всё равно капля в море других бюджетных трат).

[185] См.: Тедеев А. А. К вопросу о трансформации системы права в условиях развития информационно-коммуникационных технологий: постановка проблемы // Информационное пространство: обеспечение информационной безопасности и право. Сб. науч. трудов / под ред. Т. А. Поляковой, В. Б. Наумова, А. В. Минбалеева. М.: ИГП РАН, 2018. С.3.

Федеральный центр до сих пор имеет весьма приблизительную информацию о населении России, его численности, образовании, мобильности и половозрастном составе»[186]. Такое искажение статистических данных приводит к тому, что на основе недостоверной информации принимаются управленческие решения, которые не приводят к решению назревших проблем. Из-за недостоверности статистических данных страдает государственное планирование, в том числе и стратегическое. Кроме этого, слабая связность информационных систем обработки персональных данных, эксплуатируемых государственными органами, приводит к «недоступности персональных данных, размещаемых в отдельных автоматизированных системах учета, для заинтересованных органов государственной власти на межведомственном уровне и, как следствие, дублированию бюджетных расходов по сбору уже имеющихся в других ведомствах и организациях персональных данных; невозможности сопоставления и анализа персональных данных из различных автоматизированных систем учета для получения полной, достоверной и актуальной информации о населении»[187]. Таким образом, задача создания подобного Регистра назрела достаточно давно, его концепция разрабатывалась ранее[188], и была принята Правительством Российской Федерации[189]. Однако в то время до практической реализации, несмотря на все имеющиеся предпосылки, данный проект доведён не был.

По словам Председателя Комитета по информационной политике, информационным технологиям и связи А. Е. Хинштейна (в то время) осуществление проекта Регистра позволит «...более четко прогнозировать развитие страны, оперативно администрировать процессы. Это удобно в первую очередь для

[186] См.: Государство создаёт Единый регистр сведений о населении // Аргументы недели : [Электронный ресурс]. URL: https://yandex.ru/turbo/argumenti.ru/s/society/2023/09/858360 (дата обращения: 11.12.23).
[187] См.: Чудиновских О. С. К вопросу о создании регистра населения и использовании административных данных для нужд государственной статистики. Вопросы статистики, Т. 28, № 1, стр. 5–17.
[188] См.: Коллегия Минсвязи России рассмотрела проект Концепции создания автоматизированной системы «Государственный регистр населения (АС ГРН)» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : [Электронный ресурс]. URL: https://digital.gov.ru/ru/events/1513/ (дата обращения: 11.12.23).
[189] См.: Распоряжение Правительства РФ от 09.06.2005 № 748-р. «Об одобрении Концепции создания системы персонального учета населения Российской Федерации» Собрание законодательства РФ, 13.06.2005, № 24, ст. 2414.

граждан, потому что им не потребуется по кругу носить документы в случае каких-либо изменений, скажем смены паспорта. Сегодня, после того как ты меняешь паспорт, везде, где есть данные о нем, ты должен снова представить сведения о паспорте. После вступления закона в силу это будет происходить в автоматическом режиме».[190] Таким образом, единая информационная система, в которой будут храниться данные о населении, позволит решить множество задач, связанных с государственным управлением: централизация хранения информации о населении; поддержание в актуальном и непротиворечивом состоянии данных о физических лицах; повышение степени контроля за доступом к персональным данным населения; повышение защищённости хранимых данных за счёт консолидации усилий по защите на меньшем количестве защищаемых объектов; получение объективной статистической информации о населении; возможность ведомствам получать необходимую информации о физических лицах, используя межведомственные коммуникации; возможность более гибко разграничивать права на доступ к персональным данным населения; усложнение для злоумышленников возможностей по искажению информации о физических лицах; уменьшение времени на предоставление государственных услуг населению за счёт более оперативного доступа к нужной информации различных государственных органов; возможность централизованного исправления имеющихся некорректных данных о физических лицах (в частности, Регистр может помочь ФНС в борьбе с нелегальными налоговыми схемами с участием формально независимых лиц и компаний. При создании цепочек фирм-однодневок ключевой ресурс — люди). Регистр может быть полезен и для тендерных процедур, в частности, государственных, когда в конкурсе участвуют компании, формально зарегистрированные на независимых лиц. ФАС может использовать данные Регистра для целей расследования анти-конкурентных сговоров и т.д. «Регистр будет содержать сведения о населении России, которое представлено гражданами России, иностранными гражданами и лицами без гражданства, временно или

[190] См.: Что такое единый регистр сведений о населении и зачем он необходим // Государственная Дума Федерального Собрания Российской Федерации : [Электронный ресурс]. URL: http://duma.gov.ru/news/53118/ (дата обращения: 15.12.23).

постоянно проживающими в России, а также беженцами. Из реестра ЗАГС в новый Регистр будут предоставляться фамилия, имя и отчество, и их изменение, сведения о рождении и смерти, усыновлении и отцовстве, заключении и расторжении брака. Также Регистр будет содержать сведения об изменении пола физического лица. МВД предоставит сведения о документе, удостоверяющем личность, гражданстве, регистрации и миграционном учете, наличии у гражданина России права постоянно проживать в иностранном государстве, о выдаче иностранным работникам разрешений на работу и т.д.; Рособрнадзор — о документах об образовании и квалификации; Минобрнауки — об ученой степени и ученом звании; Минобороны — о постановке на воинский учет; ФНС — об учете в налоговом органе и о регистрации ИП; Роструд — об учете в службе занятости или в качестве безработного; ПФР, ФСС, ФОМС — о регистрации в системах обязательного пенсионного, медицинского и социального страхования; Минкомсвязь — об учетной записи лица в ЕСИА (в частности, через такую учетную запись происходит авторизация на сайте госуслуг). Помимо данных самого физического лица, регистр будет содержать сведения о его родителях, супруге и детях»[191]. Можно констатировать, что впервые в истории России сведения о населении будут храниться и обрабатываться в одном месте, что позволит значительно повысить эффективность государственного управления. Цифровизация обработки персональных данных населения позволит не только сократить время оказания государственных услуг физическим лицам, но и значительно повысить эффективность принимаемых управленческих решений, за счёт, как оперативного доступа к нужным сведениям, так и того, что государственные органы будут опираться на информацию, которая будет отвечать требованиям достоверности и непротиворечивости. Это позволит избежать принятия необоснованных управленческих решений.

Однако несмотря на все положительные стороны централизации учёта населения, эксперты высказывают ряд опасений, которые связаны с

[191] См.: Бардина П. На что повлияет регистр населения России // Ведомости : [Электронный ресурс]. URL: https://www.vedomosti.ru/opinion/articles/2020/06/19/833059-registr-naseleniya-rossii (дата обращения: 18.12.23).

информационной безопасностью этой стратегически важной системы — «Закон принят несмотря на определённые возражения со стороны отдельных представителей общественности и даже некоторых силовых структур. Например, аналогичный законопроект о “цифровом профиле гражданина” ранее был забракован в ФСБ. Специалисты Федеральной службы безопасности отмечали, что “обработка данных в рамках единой инфраструктуры значительно повысит риски утечек информации”»[192]. В коллективном открытом письме научного сообщества (которое подписали несколько десятков учёных), которое было направлено в высшие органы государственной власти Российской Федерации: Администрацию Президента, Правительство, Парламент были обозначены возможные риски внедрения такой системы. Не остались стороне и парламентарии — «Законопроект требует широкого обсуждения, парламентских слушаний, общественных слушаний, работы с экспертами... Член экспертного совета при комитете Государственной думы по развитию гражданского общества, вопросам общественных и религиозных объединений Игорь Понкин тоже считает, что законопроект, в числе прочего, создаёт предпосылки для утечек персональных данных. Во время последнего обсуждения глава ФНС Даниил Егоров пообещал максимальный уровень защиты базы и успокоил депутатов. В результате они проголосовали за принятие закона»[193]. Можно констатировать, что консолидация информации в одной информационной системе помимо решения множества важных задач государственного управления при помощи информационных (цифровых) технологий, порождает необходимость уделять пристальное внимание вопросам защиты разработанной информационной системы, как от внешних угроз, так и от внутренних. По данным исследований, в последнее время — «Почти каждая третья утечка конфиденциальной информации в России связана с компрометацией крупных баз данных (от 100 тыс. записей ПДн). Всего в первом

[192] См.: Эксперты рассказали о рисках централизованной системы хранения данных. // Рамблер-финансы : [Электронный ресурс].. URL: https://finance.rambler.ru/other/43154312-eksperty-rasskazali-o-riskah-tsentralizovannoy-sistemy-hraneniya-dannyh/ (дата обращения: 18.12.23).
[193] См.: Принят закон об электронных досье на жителей России. // HABR URL: https://habr.com/ru/news/503256/ (дата обращения: 18.12.23).

полугодии 2023 г. утекло 92 таких базы, тогда как в первом полугодии 2022 г. — 72 базы»[194], как видно интерес злоумышленников к информационным системам, содержащим большой объём персональных данных, постоянно растёт. Что во многом связано с изменившейся геополитической обстановкой и повышением интереса спецслужб недружественных государств, хакерских групп и террористических организаций к возможности получить конфиденциальную информацию о населении Российской Федерации. По этой причине риски, связанные с информационной безопасностью, на которые указывают некоторые эксперты, следует воспринимать всерьёз и уделять этому вопросу повышенное внимание. В связи с тем, что сохранность обрабатываемых в Едином регистре сведений о населении является вопросом национальной безопасности и требует постоянного внимания, компрометация хранимой информации может нанести государству огромный вред. Особенно это относится к персональным данным сотрудников правоохранительных органов, военных, и людей, имеющих доступ к государственной тайне. В соответствии с ч.5, ст.9 Федерального закона от 08.06.2020 № 168-ФЗ (ред. от 28.12.2022) «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации», поддержание необходимого уровня безопасности системы входит в зону ответственности её оператора. Наличие у Федеральной налоговой службы специализированных компетенций позволяет эффективно обеспечивать защиту обрабатываемых данных, однако, несмотря на отсутствие случаев громких утечек данных с их стороны, необходимо разработать дополнительные правовые механизмы защиты хранимой информации, поскольку безопасность информационной инфраструктуры, которая используется Регистром для функционирования, является вопросом национальной безопасности и должна быть обеспечена на высшем уровне. Для этого следует рассмотреть вопрос о необходимости проведения обязательного периодического (не реже одного раза в год) аудита инфраструктуры оператора «Единого регистра сведений о населении»

[194] См.: Утечки информации ограниченного доступа в мире и России, первое полугодие 2023 г. // INFOWATCH : [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-mire-i-rossii-za-pervoe-polugodie-2023-goda.pdf (дата обращения: 18.12.23).

на предмет соответствия всем требованиям информационной безопасности, а также следует рассмотреть вопрос обязательной аттестации персонала; такой аудит мог бы проводится силами межведомственной группы, которая имела бы соответствующие компетенции и, самое важное, соответствующий уровень допуска к государственной тайне. Аттестация и контроль сотрудников, имеющих доступ к информационным системам обработки персональных данных (особенно государственных), является важным элементом обеспечения информационной безопасности таких систем, по причине того, что это позволяет уменьшить возможные риски со стороны обслуживающего персонала, именно действия или бездействие персонала могут являться причиной несанкционированного доступа к обрабатываемой информации — «Примечательным является факт, что, согласно данным, 79% утечек персональных данных случились не в результате хакерских атак, а из-за внутренних нарушений. Доля утечек, вызванных умышленными действиями сотрудников, составляет 72%»[195]. Аудит должен проводится межведомственной группой, что позволит учесть интересы всех государственных органов в вопросе охраны данных. Особенно это актуально в свете увеличившегося числа утечек персональных данных и роста активности злоумышленников.

Ещё одной особенностью внедрения «Единого Регистра сведений о населении» является информационная составляющая его работы. Многие люди начали воспринимать появление такой системы, как элемент тотальной слежки, становление «цифрового ГУЛАга», и т.д. К сожалению, массовой истерии оказались подвержены даже некоторые политики — «”Англо-саксонцы будут контролировать каждого из нас…Это электронно-бытовой концлагерь, о котором фашисты даже не мечтали”, — заявил в связи с принятием закона лидер КПРФ Г. А. Зюганов»[196], что дополнительно дискредитирует в глазах населения создание такой стратегически важной для функционирования государства информационной системы. Можно констатировать, что государству необходимо своевременно

[195] См.: 72% утечек персональных данных происходят по вине сотрудников // Справочник секретаря : [Электронный ресурс]. URL: https://www.sekretariat.ru/news/214623-72-utechek-personalnyh-dannyh-proishodyat-po-vine-sotrudnikov (дата обращения: 19.12.23).
[196] См.: Закон о едином регистре населения окончательно принят Госдумой // РОСБАЛТ : [Электронный ресурс]. URL: https://www.rosbalt.ru/russia/2020/05/21/1844581.html (дата обращения: 19.12.23).

доносить свою точку зрения по общественно важным вопросам до населения с целью недопущения роста социальной напряжённости.

К сожалению, увеличение объёма автоматизированной обработки персональных данных стало причиной того, что злоумышленники всё чаще пытаются получить к ним доступ.

Известная компания, специализирующаяся на информационной безопасности[197] сообщает о ежегодном росте количества случаев, связанных с доступом злоумышленников к персональным данным[198]. Это происходит несмотря на все изменения[199], вносимые в законодательство[200] в последнее время[201].

В соответствии с Федеральным законом от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон ”О персональных данных”» был осуществлён ряд законодательных изменений[202]. Во-первых, были увеличены в 2 раза штрафы за нарушение требований к обработке персональных данных, во-вторых, такая санкция, как предупреждение теперь не применяется, в случае выявления нарушений выписывается штраф, размер которого при повторных пренебрежениях требованиями законодательства будет увеличиваться. Рост штрафов происходит впервые с 2017 года. Таким образом законодатель реагирует на значительное увеличение числа утечек. Для более эффективного воздействия экономических мер на тех, кто не уделяет достаточного внимания защите обрабатываемых персональных данных, следует выработать правовые механизмы выплаты компенсаций пострадавшим, со стороны того, кто допустил разглашение личной информации. Такая практика, к примеру, действует в США, где помимо выплаты

---

[197] См.: Капранов О. В. России прошла целая серия утечек персональных данных // Российская газета : [Электронный ресурс]. URL: https://rg.ru/2022/10/03/so-vzlomom-napereves.html (дата обращения: 19.12.23).
[198] См.: Утечки информации ограниченного доступа в России за 2022 год // InfoWatch : [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-god (дата обращения: 21.11.2023).
[199] См.: Как ужесточились требования к работе с персональными данными в 2021 году // Контур : [Электронный ресурс]. URL: https://kontur.ru/articles/4816 (дата обращения: 21.12.23).
[200] См.: Как изменится закон о персональных данных с 1 сентября 2022 года// Контур : [Электронный ресурс]. URL: https://kontur.ru/articles/1000 (дата обращения: 21.12.23).
[201] См.: Что изменится в работе с персональными данными с 1 марта 2023 года // Контур : [Электронный ресурс]. URL: https://kontur.ru/articles/1478 (дата обращения: 21.12.23).
[202] См.: Федеральный закон от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон "О персональных данных» // Собрание законодательства РФ, 04.01.2021, № 1 (часть I), ст. 58

больших штрафов, компании, допустившие утечки, вынуждены платить огромные компенсации тем, кто от них пострадал, а также, по решению суда[203], вкладывать деньги в свою информационную безопасность. Применительно к российскому законодательству такая правовая конструкция вынуждала бы компании и организации более качественно работать над сохранностью обрабатываемых персональных данных из-за опасности получить серьёзные убытки. Работа в этом направлении уже началась: «Правительство поддержало инициативу Минцифры о компенсации пострадавшим от утечек персональных данных в рамках закона об оборотных штрафах. Если компания, которая допустила утечку, обеспечит финансовое возмещение нанесённого пользователю вреда, это будет признаваться смягчающим обстоятельством. В этом случае к ней будут применяться пониженные оборотные штрафы»[204]. Внедрение такого п

авового механизма положительно скажется на защищённости прав физических лиц. Однако стимулирование выплат компенсаций за счёт снижения оборотных штрафов может привести к тому, что компании будут стараться занизить суммы выплачиваемых компенсаций и, тем самым, избегать высоких штрафных санкций. Это не будет способствовать вложению средств со стороны операторов персональных данных в обеспечение информационной безопасности хранимой информации. Кроме того, обязанность организаций выплачивать и оборотные штрафы, и компенсации физическим лицам за утечку данных, дополнительно побуждает операторов персональных данных вкладывать финансовые средства в информационную безопасность, чтобы не оказаться в ситуации, когда утечка данных, и последующие за ней санкции, приводят к банкротству. Именно перспектива больших финансовых потерь заставляет бизнес-структуры выступать против введения оборотных штрафов за утечки персональных данных — «РСПП, “Деловая Россия”, “Опора России” и ТПП РФ предлагают скорректировать

[203] См.: Deadline Passes on T-Mobile's $350 Million Settlement Days After Another Data Breach. // CNET : [Электронный ресурс]. URL: https://www.cnet.com/personal-finance/deadline-passes-on-t-mobiles-350-million-settlement-days-after-another-data-breach/ (дата обращения: 21.12.23).
[204] См.: В Правительстве одобрили компенсации пострадавшим от утечек // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : [Электронный ресурс]. URL: https://digital.gov.ru/ru/events/47423/ (дата обращения: 23.12.23).

положения законопроекта о введении оборотных штрафов за утечку персональных данных (ПДн), отсрочить его вступление в силу до 2026 года, говорится в письме этих организаций на имя председателя Госдумы РФ Вячеслава Володина, с которым ознакомился “Интерфакс”»[205]. Именно такие заявления являются маркером того, что правотворческая деятельность государства ведётся в правильном направлении, и несмотря на протесты бизнеса регулирование в этой области следует продолжать совершенствовать.

Также внесением изменений законодатель конкретизировал правовое понятие «персональные данные, разрешенные субъектом персональных данных для распространения», и в рамках нормативного регулирования закрепил правовая обязанность операторов персональных данных инициировать процедуру получения отдельного согласия субъекта на передачу его данных сторонним субъектам правоотношений. Правовая норма упразднила презумпцию автоматического распространения действия согласия субъекта на передачу данных третьим лицам при даче такового на их обработку. Теперь для передачи другим лицам необходимо получить отдельное согласие, в котором оператор обязан предоставить субъекту возможность выбора передаваемой сторонним лицам информации о себе, в случае отсутствия явного согласия передача данных не допускается, т.е. у субъекта персональных данных появляется возможность согласится на передачу оператору данных о себе, но запретить их передачу на сторону. Отдельным пунктом устанавливается, что «молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения»[206] (ст. 58). Такой подход минимизирует правовой риск расширительного толкования оператором волеизъявления субъекта: отсутствие несогласия более не может служить

[205] См.: Деловые объединения РФ предлагают доработать законопроект об оборотных штрафах за утечку ПДн, отсрочить его вступление // Деловая Россия : [Электронный ресурс]. URL: https://deloros.ru/press-centr/publikacii/delovye-obedineniya-rf-predlagayut-dorabotat-zakonoproekt-ob-oborotnykh-shtrafakh-za-utechku-pdn-ots/ (дата обращения: 23.12.23).

[206] См.: Федеральный закон от 30.12.2020 № 519-ФЗ "О внесении изменений в Федеральный закон «О персональных данных» // Собрание законодательства РФ, 04.01.2021, № 1 (часть I), ст. 58.

основанием для передачи данных. Этими изменениями в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» законодатель решил в первую очередь достаточно острую проблему навязывания субъекту персональных данных необходимости дать разрешение на передачу информации о нём другим лицам, вместе с согласием на обработку его персональных данных. Исследовательский анализ выявляет отсутствие нормативного регулирования механизма обратной связи: субъект персональных данных не всегда получает сведения о получателе и целях передачи данных, несмотря на факт его согласия на передачу. Например, в европейском «Общем регламенте по защите данных» (GDPR)[207], согласно ст.ст. 13 и 14, субъекта персональных данных необходимо информировать о том, кому передана информация о нём (получатели или категории получателей персональных данных). Подобный правовой подход позволяет более прозрачно для субъекта обрабатывать и передавать данные о нём. Применительно к российскому законодательству, информирование владельцев персональных данных о том, кому осуществлена их передача и с какими целями, позволило бы сделать эту процедуру более юридически прозрачной. При наличии такого способа информирования, субъект персональных данных сможет контролировать их передачу другим лицам. Это способствовало бы более взвешенному подходу операторов персональных данных к выбору тех, кому передаётся обрабатываемая информация, из-за возможного отзыва согласия на передачу или обработку со стороны владельцев личных данных, и компрометации деловой репутации.

В 2022 году были внесены новые важные изменения[208] в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», часть из которых вступила в силу с 1 сентября 2022, а часть — с 1 марта 2023 г. Положения, вступившие в силу с 1 сентября 2022 г., впервые в истории российского законодательства, связанного с регулированием обработки персональных данных, расширили действие

[207] См.: Общий регламент защиты персональных данных (GDPR) Европейского союза // GDPR TEXT : [Электронный ресурс]. URL: https://gdpr-text.com/ru/read/article-14/ (дата обращения: 1.12.23).
[208] См.: Федеральный закон от 14.07.2022 № 266-ФЗ "О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности» // Собрание законодательства РФ, 18.07.2022, № 29 (часть III), ст. 5233.

федерального законодательства в области защиты информации о физических лицах, теперь его положения будут распространяться в том числе, и на иностранных операторов персональных данных, которые осуществляют их обработку на основании договора с гражданином России или с его согласия; в этом появилась схожесть с общеевропейским законодательством. Принятый документ оговаривает обязательное, с марта 2023 года, уведомление государственного регулятора операторами персональных данных, в случае передачи этой информации иностранному оператору для обработки. Кроме того, регламентируются требования для трансграничной передачи. Регулятор, получив уведомление о желании оператора персональных данных осуществить их трансграничную передачу, может ограничить или запретить её, для достижения тех или иных целей, например, если они связаны с безопасностью государства.

Таким образом, государство усиливает контроль за трансграничными информационными потоками информации о своих гражданах, что будет способствовать улучшению информационной безопасности государства и защищённости данных.

Однако данная мера работала бы более эффективно в случае, если помимо уведомления государственных органов, владелец персональных данных также получал бы уведомление о трансграничной передаче своих данных явным способом. Это позволило бы физическим лицам более полно контролировать передачу информации о себе и положительным образом сказалось бы на реализации права человека на защиту частной жизни.

Ещё одним нововведением, в соответствии с Приказом Роскомнадзора от 28.10.2022 № 179[209], стало то, что оператор персональных данных при уничтожении обрабатываемой информации о физических лицах обязан составлять об этом акт в соответствии с требованиями регулятора. Эта мера позволит лучше контролировать процедуру уничтожения персональных данных.

[209] См.: Приказ Роскомнадзора от 28.10.2022 № 179 «Об утверждении требований к подтверждению уничтожения персональных данных» // Министерство Юстиции Российской Федерации : [Электронный ресурс]. URL: https://minjust.consultant.ru/special/documents/document/33515 (дата обращения: 26.12.23)

Теперь оператор персональных данных, с 1 марта 2023 года, обязан уведомлять Роскомнадзор о возникшем инциденте, повлекшем утечку информации о физических лицах через государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы (ГосСОПКА), а также определять степень вреда, который может быть причинён утечкой охраняемой информации (законодатель выделяет три степени потенциального вреда из-за утечки персональных данных: высокий, средний и низкий, в зависимости от того какие виды охраняемой информации обрабатывались)[210]. Важно отметить, что оценка производится на основании критериев, представленных в приказе регулятора, силами сотрудников оператора персональных данных. С одной стороны, такой подход позволяет оператору понимать степень важности хранимых данных. Однако это же может привести к тому, что в случае, если потенциальный ущерб от утечки невелик, у того, кто обрабатывает персональные данные, есть риск возникновения обманчивой иллюзии, что можно уделять меньше внимания обеспечению безопасности охраняемых сведений, чем в случае, когда возможный ущерб более высок. Такое категорирование возможного вреда от разглашения информации о физических лицах является достаточно неоднозначным. И может в будущем спровоцировать увеличение числа утечек персональных данных из-за снижения качества их защиты. Методика определения вреда от утечек информации о физических лицах безусловно нужна, но она не должна влиять на мотивацию оператора защищать персональные данные. Эта оценка должна осуществляться профильными сторонними организациями или же регулятором. Такой подход позволит исключить ситуацию с возможным занижением последствий утечки информации со стороны оператора персональных данных. Следовательно, эта правовая новелла требует доработки, по причине ее неоднозначности и возможной неэффективности.

[210] См.: Приказ Роскомнадзора от 27.10.2022 № 178 "Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных" // Официальное опубликование правовых актов : [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202211290004 (дата обращения: 27.12.23).

Федеральный закон от 30.11.2024 № 420-ФЗ[211] внёс правки в «Кодекс Российской Федерации об административных правонарушениях», который ужесточил санкции в отношении операторов персональных данных при утечках обрабатываемых ими персональных данных. Впервые введён штраф, как для юридических, так и должностных лиц, за несообщение о факте неправомерного доступа к обрабатываемой информации о физических лицах; повышен размер штрафа за подтверждённый случай утечки персональных данных с 60-100 тыс. руб. до 3-5 млн. рублей. Кроме этого, впервые за повторную компрометацию обрабатываемой оператором персональных данных информации, введён обратный штраф в размере 1-3 % годовой выручки (не менее 20 млн. руб. и не более 500 млн. руб.). Ранее размер штрафа составлял 100-300 тыс. руб. Однако, в случае если организация тратила ежегодно не менее 0.1 % от выручки на информационную безопасность и при доказанном соблюдении всех требований законодательства возможно снижение размера оборотного штрафа. Введённые регуляторные меры призваны ликвидировать ситуацию, при которой финансовая целесообразность склоняется в пользу уплаты штрафов вместо инвестирования в системы защиты персональных данных. Также ведены штрафы за не уведомление регулятора о намерении обрабатывать сведения о физических лицах. Следует так же отметить, что Федеральный закон от 30.11.2024 № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»[212], криминализировал распространение персональных данных, добытых незаконным путём, и за создание информационных ресурсов для получения таких данных, которая предусматривает наказание до 4 лет; этот срок увеличивается, если преступные действия связаны с информацией о несовершеннолетних.

[211] См.: Федеральный закон от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // Собрание законодательства РФ, 02.12.2024, № 49 (часть IV), ст. 7411.
[212] См.: Федеральный закон от 30.11.2024 № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // Собрание законодательства РФ, 02.12.2024, № 49 (часть IV), ст. 7412.

В 2025 году осуществлено ужесточение[213] нормативных требований, регламентирующих географическое размещение баз данных, содержащих персональные сведения. Согласно новым изменениям, массивы данных, включающие персональную информацию российских граждан, должны располагаться на территории Российской Федерации. Действующий регламент обработки персональных данных дополнен[214] обновлёнными требованиями к оформлению согласия на обработку данных. Правовая модель требует, чтобы волеизъявление субъекта в отношении обработки его персональных данных было зафиксировано в отдельном документе, не объединённом с иными договорными положениями. Это позволит исключить ситуации, когда согласие включалось в состав иных документов, подписываемых субъектом персональных данных. Теперь у операторов будет меньше возможностей для злоупотреблений при оформлении согласий, что сделает процедуру более прозрачной для субъекта персональных данных.

Рассматривая последние изменения в законодательстве, направленные на защиту персональных данных, можно сделать вывод о том, что трансформация права идёт полным ходом, государство продолжает выстраивать современный правовой механизм регулирования обработки персональных данных в условиях цифровизации. Цифровые технологии позволяют консолидировать обрабатываемую государственными органами информацию о населении, что и позволило организовать «Единый федеральный информационного регистр населения Российской Федерации». Его создание стало требованием времени, поскольку разрозненность и фрагментация собираемых данных стала отрицательно сказываться на эффективности принимаемых государственными органами решений. Консолидация учёта населения стала важным этапом в цифровизации государственного управления. Поскольку централизация хранения и обработки

[213] См.: Федеральный закон от 28.02.2025 № 23-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ, 03.03.2025, № 9, ст. 852.
[214] См.: Федеральный закон от 24.06.2025 № 156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ, 30.06.2025, № 26 (часть I), ст. 3486.

данных о населении подтолкнёт все органы государственной власти, включённые в обработку информации о физических лицах к внедрению новых технологий для решения повседневных задач. Это позволит повысить эффективность государственного управления и будет способствовать повышению качества оказания государственных услуг, сведя к минимуму необходимость сбора данных у заявителя, благодаря получению этой информации в рамках межведомственного электронного взаимодействия. Однако функционирование такой информационной системы требует обеспечения высокого уровня информационной безопасности, поскольку обеспечение хранящихся данных становится вопросом государственной безопасности, что накладывает на оператора Регистра дополнительные обязанности по обеспечению сохранности обрабатываемой информации.

Цифровизация социальных отношений стала причиной множества изменений, которые коснулись не только общественной жизни, но и затронули управление государством. Значительное влияние на государственное управление оказала возможность построения больших автоматизированных информационных систем. Это позволило начать работу над централизацией обработки и хранения данных о населении. Данная задача является одной из важнейших для государственного управления, поскольку позволяет точнее и эффективнее на основе этих сведений о физических лицах осуществлять государственное планирование во всех сферах. Кроме этого, централизованное хранение данных о населении позволяет выстроить систему качественного и быстрого оказания государственных услуг для населения и бизнеса, что повышает качество и эффективность государственного управления за счёт достоверности и непротиворечивости данных о населении. Но немаловажным остаётся вопрос обеспечения информационной безопасности централизованного хранения данных о населении.

Постоянные утечки информации о физических лицах привели к тому, что происходит ужесточение законодательства и усиление роли контролирующих органов в этой области. Однако, для повышения эффективности трансформации права в области обработки персональных данных, следует не только ужесточать санкции и усиливать роль контролирующих органов, но и расширять

информирование владельцев персональных данных: как о различных инцидентах, связанных с информацией о них, так и о том, кому и куда передаются их данные, с какими целями и для чего. Кроме этого, дальнейшей проработки требует вопрос, связанный с проблемой выплат компенсаций пострадавшим от утечек личной информации, как и создание правовых механизмов принуждения нарушителей к повышению эффективности защиты персональных данных. Обязанность выплачивать компенсации пострадавшим от компрометации личной информации будет дисциплинировать операторов персональных данных на соблюдение всех требований информационной безопасности. Существенным элементом процедуры получения согласия на обработку персональных данных должно стать заблаговременное уведомление субъекта о ранее зафиксированных случаях утечки персональных данных у данного оператора. Введение такого обязательного информирования об операторах, которые допустили несанкционированный доступ к обрабатываемой информации о физических лицах, также будет побуждать операторов персональных данных защищать персональные данные более качественно и эффективно.

Разрешение выявленных проблем способно выступить катализатором повышения для субъектов прозрачности обработки и передачи сведений о них, надёжнее гарантировать конституционное право на неприкосновенность частной жизни, укрепить систему информационной безопасности государства и повысить эффективность управленческих механизмов в данной области.

Можно констатировать, что основным направлением системного совершенствования правового регулирования персональных данных в Российской Федерации должна выступить регламентация порядка функционирования механизма правовой защиты информации о физическом лице на электронном носителе. Систему защиты такой информации можно определить как совокупность правовых средств, направленных на защиту информации, документированной (электронно и\или неэлектронно) информации, относящейся прямо или косвенно, к определенному или определяемому физическому лицу (субъекту персональных данных), позволяющей его (субъект) идентифицировать полностью или частично,

в том числе с применением автоматизированных и неавтоматизированных информационных технологий**.** В настоящее время в Российской Федерации назрела необходимость изменения действующей модели правового регулирования персональных данных, которая ориентирована на регламентацию отношений по поводу обработки информации о физических лицах, документированной преимущественно на бумажных, а не электронных носителях. Решение этой задачи позволит выстроить актуальную систему правовой защиты персональных данных в Российской Федерации соответствующую реалиям и задачам информационно-правового регулирования обработки персональных данных, что положительно скажется на эффективности государственного управления в нашей стране.

§ 2.3 Организационные основы правовой защиты персональных данных как фактор обеспечения национальной безопасности России

Впервые понятие «национальная безопасность» появилось в США, оно было употреблено в одном из посланий президента Т. Рузвельта Конгрессу в 1904 году. В дальнейшем под этим термином стало пониматься обеспечение безопасности граждан, общества и государства — «“традиционная концепция национальной безопасности фокусируется на выживании государства”: аспекты физической безопасности государства от внешних угроз (преимущественно военного реагирования) включают национальную оборону, национальную целостность и национальный суверенитет»[215]. В английском языке понятие «national security» — обозначает именно государственную безопасность.

В России понятие «национальная безопасность» было впервые использовано в Федеральном законе № 24-ФЗ от 20 февраля 1995 г. «Об информации, информатизации и защите информации»[216] (п.2 ст.3), а позднее его определение прозвучало в послании Президента Российской Федерации Федеральному Собранию 13 июля 1996 года: «состояние защищенности национальных интересов

[215] См.: Khan E. M. Comprehensive national security:contemporary discourse // Margalla Papers-2022 (Issue-I) p.1-17.
[216] См.: Федеральный закон от 20.02.1995 № 24-ФЗ "Об информации, информатизации и защите информации" // "Российская газета", № 39, 22.02.1995.

от внутренних и внешних угроз, обеспечивающее прогрессивное развитие личности, общества и государства»[217], позднее была принята «Концепция национальной безопасности 1997 года»[218]. Для России эта дефиниция была новой, в то время она только начала постепенно замещать понятие «государственная безопасность», которое использовалось для характеристики безопасности государства в СССР.

В основе долгосрочного обеспечения национальной безопасности лежит стратегическое планирование[219]. Базовым актом, регулирующим эту деятельность, является Федеральный закон от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации», нормативное обеспечение в этой области также включает более 20 иных нормативных актов различного уровня[220].

В постоянно меняющемся мире именно стратегическое планирование позволяет государству на необходимом уровне определять систему взглядов на те или иные проблемы с целью защиты своих национальных интересов. Важность стратегического планирования не раз подчёркивалась в юридической литературе — «документы стратегического планирования играют ключевую роль в управлении, так как именно посредством их реализуются на практике принятые управленческие решения. По сути, такого рода документы — это и способ и, одновременно, форма передачи управляющего воздействия от одного субъекта стратегического планирования к другому»[221]. Ключевая роль документов стратегического планирования связана с тем, что они определяют: приоритеты,

---

[217] См.: Послание Президента Российской Федерации Федеральному Собранию «О национальной безопасности» от 13 июля 1996 г. // Российская газета, № 17, 14.07.1996.

[218] См.: Указ Президента РФ от 17.12.1997 № 1300 "Об утверждении Концепции национальной безопасности Российской Федерации" // "Российские вести", № 239, 25.12.1997.

[219] См.: Молчанов Н. А. Новые аспекты правового регулирования государственного стратегического планирования в Российской Федерации / Н. А. Молчанов, В. П. Егоров, Е. К. Матевосова // Актуальные проблемы российского права. — 2015. — № 2(51). —С. 28-34.

[220] См.: Нормативное обеспечение стратегического планирования // Минэкономразвития РФ : [Электронный ресурс]. URL:https://www.economy.gov.ru/material/directions/strateg_planirovanie/normativnoe_obespechenie_strategicheskogo_planirovaniya/ (дата обращения: 27.12.23).

[221] См.: Полякова Т. А. Роль стратегического планирования в совершенствовании системы государственного управления в Российской Федерации / Т. А. Полякова, Д. А. Афиногенов // Вестник Академии права и управления. — 2016. — № 4(45). — С. 11–18.

принципы, цели, задачи и, что немаловажно, угрозы и риски в определённой области.

Эволюция стратегического планирования в области национальной и информационной безопасности сопровождалась принятием ряда основополагающих документов, среди которых: «Доктрина информационной безопасности 2000 года»[222], «Стратегия национальной безопасности Российской Федерации 2009 года»[223], «Стратегия национальной безопасности Российской Федерации 2015 года»[224], «Доктрина информационной безопасности 2016 года»[225] (далее: Доктрина), «Стратегии национальной безопасности Российской Федерации 2021 года»[226] (далее: Стратегия национальной безопасности) и «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы»[227] (далее: Стратегия информационного общества).

Развитие и становление информационного общества привели к тому, что различные сведения и данные стали ресурсом, который является критически важным для достижения целевых показателей социально-экономического развития [228]. В контексте развития цифровой экономики персональные данные физических лиц и их надёжная защита приобрели стратегическое значение для государства ввиду их ключевой роли в формировании информационного общества[229].

Анализ массивов данных, содержащих сведения о населении, позволяет осуществлять планирование (в т.ч. стратегическое) не только государственным органам, но и всем заинтересованным лицам; «в эпоху “больших данных” и

---

[222] См.: Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // "Российская газета", № 187, 28.09.2000.
[223] См.: Указ Президента РФ от 12.05.2009 № 537 "О Стратегии национальной безопасности Российской Федерации до 2020 года" // Собрание законодательства РФ, 18.05.2009, № 20, ст. 2444.
[224] См.: Указ Президента РФ от 31.12.2015 № 683 "О Стратегии национальной безопасности Российской Федерации" // Собрание законодательства РФ, 04.01.2016, № 1 (часть II), ст. 212.
[225] См.: Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" // "Собрание законодательства РФ", 12.12.2016, № 50, ст. 7074.
[226] См.: Указ Президента РФ от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации"// Собрание законодательства РФ, 05.07.2021, № 27 (часть II), ст. 5351.
[227] См.: Указ Президента РФ от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы". // "Собрание законодательства РФ", 15.05.2017, № 20, ст. 2901
[228] См.: О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года (утв. Указом Президента РФ от 07.05.2024 № 309) // "Собрание законодательства РФ", 13.05.2024, № 20, ст. 2584.
[229] См.: Войниканис Е. А. Большие (персональные) данные: проблема баланса интересов*// Журнал Суда по интеллектуальным правам. — № 4 (34). — 2021 г. — с. 19–27.

машинного обучения возможности по преобразованию данных в полезную информацию многократно увеличились, что актуализировало важность правового регулирования отношений в сфере обработки данных. Объектом охраны в отношении данных является не конкретная смысловая единица (либо совокупность таких смысловых единиц), а массивы данных, представленные, как правило, в цифровом виде и обрабатываемые в компьютерных информационных системах»[230], например, данные операторов сотовой связи (геоаналитика) могут использоваться городскими властями для планирования застройки, маршрутов транспорта, и многого другого[231].

Появление сети Интернет и развитие информационных технологий позволило находить личную информацию практически любого человека; особенно на это повлияли утечки персональных данных. Комбинируя сведения, полученные из открытых источников «социальные сети значительно упростили различным сообществам и группировкам первичную оперативную разработку кандидатов»[232]. Используя информацию, украденную у операторов персональных данных, заинтересованные лица (в т.ч. разведки иностранных государств, террористические и экстремистские организации) могут планировать и осуществлять свою деятельность по нанесению ущерба интересам Российской Федерации в различных областях. Например, даже, казалось бы, такая бесполезная информация как данные о росте заказов пиццы, в определённых условиях, может представлять достаточную важность[233].

Становление информационного общества и цифровизация социальных отношений привели к тому, что сведения о населении превратились в один из ключевых ресурсов, который повышает эффективность стратегического

[230] См.: Регулирование данных в Российской Федерации: текущее состояние, проблемы, перспективы // НИУ ВШЭ: [Электронный ресурс]. URL: https://www.hse.ru/mirror/pubs/share/480910412.pdf.
[231] См.: Трегубов В. Н. Использование информации сотовых операторов в городских транспортных исследованиях // Транспортные системы и технологии. — 2020. — Т. 6, № 2. — С. 20–33.
[232] См.: Климашин А. Г. Утрата государственной монополии на персональные данные как риск национальной безопасности // Журнал Белорусского государственного университета. Социология. — 2019. — № 3.— С. 107–112.
[233] См.: Валагин А. NI: Заказы в пиццериях у Пентагона позволяют предсказывать войны. // Российская газета : [Электронный ресурс]. URL: https://rg.ru/2025/06/23/ni-zakazy-v-picceriiah-u-pentagona-pozvoliaiut-predskazyvat-vojny.html

планирования[234] практически во всех сферах общественной жизни. Персональные данные стали не только информацией для идентификации физического лица, но и его социально-экономической характеристикой. На основании этих данных можно строить различные прогнозы, относящиеся к населению, определять лиц для вербовки или проведения в отношении них различных акций, вплоть до террористических актов. Кроме этого, эта информация позволяет выстраивать психологический и поведенческий портрет человека, а также может быть использована для совершения в отношении индивида не только мошеннических действий, но и принуждения его к выполнению тех или иных инструкций, с целью достижения необходимых результатов для злоумышленников.

Таким образом, правовое регулирование обработки и защиты персональных данных приобретает стратегическое значение для государства и защиты его интересов в информационной сфере, кроме этого «одной из целей на пути достижения финансового и информационного суверенитета является защита данных»[235].

«Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы» это один из ключевых документов стратегического планирования, определивший цели, задачи, а также меры реализации внутренней и внешней политики Российской Федерации в сфере применения информационно-коммуникационных технологий. Раздел, посвящённый развитию информационно-коммуникационной инфраструктуры РФ, включает положение о необходимости противодействия противоправному сбору и обработке персональных данных (пп. "е", п. 31), свидетельствующее о высокой значимости этой сферы в современном обществе. Рассматриваемый документ стратегического планирования устанавливает взаимосвязь между правомерным использованием персональных данных и интересами государства в области цифровой экономики (пп. "ж", п.42), что на стратегическом уровне подчёркивает влияние защиты

[234] См.: Медведев В. В. Роль цифрового стратегического планирования в государственном регулировании экономики. // Университет им. В.И. Вернадского. № 2(92). 2024 г. С. 88–105

[235] См.: Клименко С. А. Обеспечение защищённости персональных данных как основа национальной безопасности России в условиях цифровизации // Право и государство: теория и практика. — 2024. — № 6(234). — С. 216–221.

персональных данных на государственные интресы. Регламентация доступа к информации о населении и порядок обработки этих сведений, а также государственная защита персональных данных, в соответствии с этим документом стратегического планирования оказывают влияние на интересы государства (пп. "и", п.42). Всё это говорит о том, что «наряду с несомненными преимуществами информационного общества, особого внимания заслуживают новые угрозы, которые появляются. Вопросы отстаивания национальных интересов, обеспечения национальной безопасности, а также тесно связанные с ними вопросы международного сотрудничества постоянно остаются в центре внимания государства»[236].

Однако, внимание, уделённое такой важной составляющей информационного общества как правовая защита персональных данных, в Стратегии развития информационного общества видится недостаточным; содержание документа не в полной мере учитывает особую роль сбора и обработки персональных данных в современном обществе. Одним из основополагающих элементов стратегии являются приоритеты. «Правовой приоритет можно определить как правовые установления, правоположения, правовые позиции, предопределяющие в силу их важности первоочередность реализации в процессе решения конкретных задач и достижения общественно значимых целей»[237]; именно правильно определённый приоритет является залогом успешности стратегии, «поскольку это начальная и основная часть стратегирования, которая и дает “магистральное направление” внедряемой стратегии»[238]. Исходя из чего, в п. 22 рассматриваемого документа, предлагается добавить пп. "е" следующего содержания «обеспечение национальных интересов в области защиты персональных данных и сведений о населении»; это позволит на стратегическом

[236] См.: Чубукова С. Г. Стратегии развития информационного общества и направления развития законодательства // Правовая информатика: теория и опыт. — М.: Научный центр правовой информации при Министерстве юстиции Российской Федерации.—2018.— С. 247–252.
[237] См.: Морозова Л. А. Роль правовых приоритетов в формировании стратегии законотворчества в России // Юридическая техника.— №. 9.— 2015.— С. 485–487.
[238] См.: Гринев С. А. Формирование стратегических приоритетов промышленного развития РФ как инновационный фактор преодоления кризисных периодов / Гринев С. А, Квинт В. Л. // Экономика промышленности. — 2023. — Т. 16.— № 3.—С. 275–283.

уровне определить в качестве одного из ключевых направлений построения информационного общества в Российской Федерации — обеспечение безопасности информации о населении. Поскольку стратегические приоритеты признаются главными среди прочих, то предложенные дополнения будут способствовать концентрации на данном важнейшем направлении большего количества ресурсов: финансовых, политических, материальных и людских. Это положительно скажется не только на достижении целей развития информационного общества, но и окажет определённое влияние на сферу национальной безопасности нашей страны, а также зафиксирует на стратегическом уровне важность защиты персональных данных для государства.

Противостояние в информационной сфере сопровождает человечество с древнейших времён, о чём писал ещё Сунь Цзы[239], однако «результаты эволюции, которую прошел процесс становления различных способов воздействия на противника небоевыми средствами, свидетельствует о том, что искусство информационного противоборства к началу XX в. достигло весьма высокого уровня»[240]. Дальнейшее развитие информационных технологий привело к тому, что конец XX века стал временем активного развития теории и практики «информационного противостояния» (англ. information warfare). Проникновение новых технологий во множество сфер общественной жизни привело к тому, что повседневная деятельность личности, общества и государства стала во многом зависима от уровня защищённости информационной среды. «Меры по предотвращению угроз, возникающих в информационном пространстве, выступают в качестве важных факторов для обеспечения национальной и международной безопасности. Рассматривая влияние современного информационного пространства на обеспечение национальной безопасности необходимо отметить, что в настоящее время такое пространство представляет собой не просто доступ к определенной информации, а оно превратилось в

[239] См.: См.:Сунь-цзы. Искусство войны / Пер. с кит. Н. И. Конрада. — М.: Издательство АСТ, 2019. — 256 с.
[240] См.: Касюк А. Я. Информационное противоборство: генезис и первые шаги // Вестник Московского государственного лингвистического университета. Общественные науки.— 2019.— №3 (836).—С. 157–172.

информационное поле, которое используется для обеспечения процессов жизнедеятельности во всех основных сферах общества»[241], именно поэтому, учитывая возросшую роль информационной сферы и её влияние на обеспечение национальной безопасности, у государства возникла необходимость на уровне документов стратегического планирования отразить систему своих взглядов на безопасность в информационной сфере. Эти документы служат основой для государственной политики регулирования социальных отношений в информационной сфере и обеспечения информационной безопасности личности, общества и государства. Впервые такой документ был принят в 2000 году[242], в дальнейшем быстрое развитие информационно-коммуникационных технологий, а также появление новых угроз и вызовов в глобальном масштабе, потребовало уточнений и актуализации национальных интересов Российской Федерации в этой области. В результате, в 2016 году была принята новая версия «Доктрины информационной безопасности Российской Федерации»[243] (далее: Доктрина). Указанный правовой акт выступает в качестве нормативного основания для постановки оперативных и стратегических задач по обеспечению информационной безопасности Российской Федерации; А. А. Стрельцов по этому поводу отмечает: «В новом документе отражены основные национальные интересы в информационной сфере, основные информационные угрозы и состояние информационной безопасности, стратегические цели и основные направления обеспечения информационной безопасности, организационные основы информационной безопасности России»[244].

Важной особенностью Доктрины является то, что она «перестала носить общий и декларативный характер и стала конкретной и направленной в сторону

---

[241] См.: Кучерявый М. М. Основные факторы влияния политики информационной безопасности на национальную безопасность современной России // Евразийская интеграция: экономика, право, политика. — 2013. — № 14. — С. 164–168.

[242] См.: Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // "Российская газета", № 187, 28.09.2000.

[243] См.: Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" // "Собрание законодательства РФ", 12.12.2016, № 50, ст. 7074.

[244] См.: Стрельцов А. А. Новая доктрина информационной безопасности Российской Федерации: информационно-правовые основы обеспечения безопасности информационных угроз // Труды по интеллектуальной собственности. — 2017. — Т. 28, № 1. — С. 116–123.

совершенствования национальной безопасности… в новой доктрине были сформулированы взаимоувязанные основные направления деятельности в сфере информационной безопасности, которые должны быть осмыслены и детализированы в конкретных задачах»[245]. Рассматриваемый документ устанавливает, что сфера информационной безопасности государства является одним из элементов национальной безопасности; впервые на стратегическом уровне эти две области были юридически связаны в непротиворечивую иерархическую систему (п.1 Доктрины). В документе можно выделить несколько основных блоков, составляющих ключевые направления интересов Российской Федерации в информационной сфере. Среди них можно особо отметить относящиеся в той или иной степени к защите персональных данных. В первую очередь, это приоритет защиты конституционных прав граждан как составного элемента информационной безопасности государства и влияние информационных технологий на безопасность личности, общества и государства. Об этом говорится в юридической литературе: «совершенствование информационно-коммуникационных технологий сопровождается расширением возможностей их недобросовестного использования, которое создает угрозы информационной безопасности и может приводить к нарушениям прав человека»[246]. В рамках рассматриваемого документа обозначенная проблематика получила соответствующее отражение, при этом приоритетное внимание уделено вопросам обеспечения и защиты конституционных прав граждан и свобод личности в информационной сфере (пп. "а", п.8), что на стратегическом уровне подчёркивает важность этого вопроса для государства и национальной безопасности соответственно.

Цифровизация социальных отношений не только придала новый импульс развитию экономики и народного хозяйства, но и привела к тому, что «вся

[245] См.: Минзов А. С. О новой доктрине информационной безопасности России (размышления о совершенствовании системы профессионального образования в сфере информационной безопасности) / А. С. Минзов, А. Ю. Невский, О. Ю. Баронов // ИТНОУ: Информационные технологии в науке, образовании и управлении. — 2017. — № 3(3). — С. 80–85.

[246] См.: Туликов А. В. Обеспечение информационной безопасности как гарантия прав человека // Право. Журнал Высшей школы экономики. — 2015. — № 2. — С. 50–60.

информация о пользователях сети сохраняется и анализируется. Постоянно совершенствуются алгоритмы обработки “больших данных” и извлечения из них значимой информации. В условиях идеологического противостояния активизировалась деятельность иностранных разведок с использованием разнообразных технологий несанкционированного доступа и несанкционированного воздействия на информационные ресурсы, а также съема информации по техническим каналам»[247]. Это стало причиной значительного изменения общественных отношений, связанных с обработкой и защитой персональных данных в нашей стране, из-за роста объёмов автоматизированной обработки информации о физических лицах и появления множества угроз информационной безопасности для личности, общества и государства. Поэтому эффективность правовой защиты персональных данных стала влиять не только на конституционные права личности, но начала затрагивать и национальную безопасность, что нашло своё отражение на стратегическом уровне в действующей «Доктрине информационной безопасности Российской Федерации».

Однако с течением времени роль защиты персональных данных всё больше возросла, «с ростом объема цифровых данных увеличивается и уровень киберугроз. Хакерские атаки, вирусы, фишинг, и другие формы киберпреступности становятся все более изощренными и распространенными. Организации и частные лица подвергаются риску утечек данных, финансовых потерь, утраты репутации и других негативных последствий… Многие организации не обеспечивают должного уровня защиты для хранящихся у них данных. Уязвимости в сетевых системах, слабые пароли, недостаточное шифрование данных — все это делает персональную информацию уязвимой для кибератак и утечек. Недостаточная защита данных может привести к серьезным нарушениям безопасности и утечкам конфиденциальной информации»[248]. Из-за малого внимания к защите информации

[247] См.: Ищенко А. Н. Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности России в информационной сфере / А. Н. Ищенко, А. Н. Прокопенко, А. А. Страхов // Проблемы правоохранительной деятельности. — 2017. — № 2. — С. 55–62.
[248] См.: Гаджиев Г. К. Защита персональных данных и приватности в эпоху цифровизации: вызовы и решения // Международный журнал информационных технологий и энергоэффективности. — 2024. — Т. 9, № 10(48). — С. 38–41

о физических лицах возникают случаи получения чувствительных данных злоумышленниками[249]; особенно такая проблема стала актуальной в последнее время, когда на информационные системы различных организаций, в том числе государственных, осуществляются целенаправленные атаки с целью получения злоумышленниками критически важных для национальной безопасности данных[250]. В действующей Доктрине этому уделено особое внимание: «в числе основных направлений обеспечения информационной безопасности в области государственной и общественной безопасности называются повышение эффективности профилактики правонарушений с использованием информационных технологий, противодействия таким правонарушениям, защите информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения»[251]. Влияние защищённости персональных данных граждан на национальную безопасность многократно возросло, и для решения этой проблемы необходимо на уровне документов стратегического планирования обеспечить установление повышенной важности защиты персональных данных физических лиц при их электронной обработке. Именно автоматизация обработки персональных данных стала одной из предпосылок трансформации[252] общественных отношений в этой области. Теперь ключевой особенностью, связанной с обработкой информации о физических лицах, стало появление возможности удалённого и практически мгновенного доступа к ней, и её моментальная трансграничная передача, что имеет одно из ключевых значений для национальной безопасности. Этот важный вопрос поднимается в находит своё отражение в научной литературе: «персональные данные — очень ценный ресурс в условиях современного мира. Их легальная обработка позволяет

[249] См. подробнее: Сапронов Д. Ю. Об основных направлениях совершенствования правового регулирования обработки персональных данных (информационно-правовой аспект) // Вестник Московского университета. Серия 26: Государственный аудит. – 2025. – № 3. – С. 136-151.
[250] См.: Хакеры провели инвентаризацию // КОММЕРСАНТ : [Электронный ресурс]. URL: https://www.kommersant.ru/doc/6147895?ysclid=llgwmtxzp9332474382 (дата обращения: 28.12.23).
[251] См.: Дикаев, С. У. Право безопасности и доктрина информационной безопасности России // Криминология: вчера, сегодня, завтра. — 2017. — № 1(44). — С. 37–39.
[252] См.: Тедеев А. А. К вопросу о трансформации системы права в условиях развития информационно-коммуникационных технологий: постановка проблемы // Информационное пространство: обеспечение информационной безопасности и право. Сб. науч. трудов / под ред. Т. А. Поляковой, В. Б. Наумова, А. В. Минбалеева. М.: ИГП РАН, 2018.

коммерческим компаниям производить более адаптированные под интересы целевой аудитории товары, создавать таргетированную рекламу, привлекая новых клиентов и увеличивая прибыль… Одновременно с этим персональные данные интересны и для злоумышленников, поскольку предоставляют им возможность реализовать различного рода хищения, дискредитировать конкретную личность в медиапространстве, шифровать собственную личность при реализации противоправных действий и т. д.»[253]. Превращение личной информации в ресурс с высоким уровнем спроса не только для легальной обработки, но и для нелегальной, потребовало от законодателя выработки новых подходов к обеспечению информационной безопасности личности, общества и государства. Множество услуг и сервисов стало доступно практически из любого местоположения, но и доступ к персональным данным физических лиц для злоумышленников стал менее трудозатратным и, соответственно, количество случаев несанкционированного доступа к ним увеличивается. Цифровизация общественных отношений поставила перед юристами непростую задачу по адаптации имеющихся стратегических документов в области обеспечения национальной безопасности к новым вызовам. «Сегодня процесс формирования цифровой среды создает запрос на развитие системы организационных и правовых механизмов взаимодействия субъектов информационного и цифрового обмена, оборота цифровых данных в различных сферах нашей жизни»[254], отмечает Т. А. Полякова.

Повсеместное использование цифровых технологий актуализировало необходимость пересмотра подходов к обеспечению информационной безопасности по причине постоянного увеличения количества утечек персональных данных[255], причём иногда достаточно минимального набора сведений о физическом лице для того, чтобы злоумышленник мог получить результат — «в последние годы многие клиенты банков пострадали от действий

[253] См.: Бахтеев Д. В. Преодоление нелегальной трансграничной передачи персональных данных / Д. В. Бахтеев, А. М. Сосновикова, Е. В. Казенас // Journal of Digital Technologies and Law. — 2024. — Т. 2, № 4. — С. 943–972.
[254] См.: Полякова Т. А, Бойченко И. С. Особенности взаимодействия и правового обеспечения информационной безопасности в единой биометрической системе в Российской Федерации // Правовая политика и правовая жизнь. — 2023. — № 3. — С. 26-34.
[255] См.: В Сбербанке крупнейшая утечка в истории российского банковского сектора. // CNEWS : [Электронный ресурс]. URL: https://www.cnews.ru/news/top/2019-10-03_sberbank_dopustil_krupnejshuyu (дата обращения: 28.12.23).

мошенников, которые по телефону обманным путем вынуждали граждан переводить деньги со своих счетов. Поскольку преступниками использовался минимальный объем информации о гражданине (фамилия, имя, отчество и номер телефона), вероятно, утечка персональной информации произошла не из кредитных организаций, поскольку они владеют значительно большим объемом сведений о своих клиентах»[256]. В 2023 году ЦБ РФ фиксирует что количество «...утечек баз персональных данных в России в I полугодии 2023 года выросло в четыре раза в сравнении с аналогичным периодом 2022 года. С начала 2023 года случилось уже 76 таких инцидентов против 19 в первые месяцы 2022»[257]. Изменение геополитической обстановки стало причиной того, что всё больше государственных организаций становятся целями злоумышленников, желающих добраться до обрабатываемых ими персональных данных[258], в том числе и для передачи сведений разведкам недружественных государств. Автоматизация хранения и обработки личной информации стала источником не только положительных изменений во всех сферах общественной жизни, но и фактором появления новых вызовов и угроз для государства. А. В. Морозов пишет: «В центре внимания всех мероприятий по обеспечению ИБ, прежде всего, должна находиться информационная среда системы органов государственной власти. Это объясняется тем, что их деятельность по управлению государством и обществом обеспечивает создание реальных гарантий свобод и прав человека, защиту интересов граждан страны и их социально значимых ассоциаций»[259]. Украденная информация о физических лицах может быть использована при совершении правонарушений, «всего в 2022 году злоумышленникам удалось украсть у банковских клиентов 14,1 млрд руб. Это рекордно высокий показатель минимум с 2019 года…За год объем

[256] См.: Горячева Е. В. Проблемы защиты персональных данных в банковской сфере // Юридическая наука и практика. — 2023. — Т. 19, № 3. — С. 23–29.
[257] См.: Роскомнадзор сообщил о росте утечек данных в четыре раза в I полугодии // ТАСС : [Электронный ресурс]. URL: https://tass.ru/obschestvo/18333157 (дата обращения: 28.12.23).
[258] См.: Хакеры взломали сайт МосгорБТИ // Forbes : [Электронный ресурс]. URL: https://www.forbes.ru/tekhnologii/494123-hakery-vzlomali-sajt-mosgorbti (дата обращения: 28.12.23).
[259]См.: Малюк А. А., Морозов А. В. Формирование цифровой экономики и проблемы совершенствования нормативно-правового регулирования в области обеспечения информационной безопасности. // Безопасность информационных технологий. — 2019. — Т. 26, № 4. — С. 21–36.

хищений вырос на 4,29% на фоне активного развития новых дистанционных платежных сервисов и роста объема денежных переводов с применением электронных средств платежа»[260]. Полученные злоумышленниками персональные данные используются для совершения противоправных действий; это не только затрагивает сферу безопасности физических лиц, но и создаёт в обществе социальную напряжённость, которая отрицательным образом сказывается на имидже государства, и на защищённости его интересов в информационной сфере, и, как следствие, на национальной безопасности. Полученные мошенниками денежные средства могут использоваться террористическими и экстремистскими группировками, а также иностранными спецслужбами для финансирования своей деятельности. В последнее время участились случаи принуждения мошенниками своих жертв к совершению противоправных действий[261], в том числе, и против государственных органов[262]. Таким образом, получение несанкционированного доступа к большим объёмам персональным данным физических лиц напрямую угрожает безопасности государства из-за того, что злоумышленники, имея доступ к ним, могут не только наносить отдельным обманутым гражданам финансовый ущерб, но и за счёт использования социальной инженерии и иных методов, принуждать своих жертв к выполнению различных противоправных действий с целью нанесения ущерба государству; к примеру, в последнее время участились случаи атак на логистическую инфраструктуру[263].

Можно сделать вывод о том, что ущерб от утечек персональных данных становится многокомпонентным и затрагивает не только безопасность личности, но и влияет на сферу национальной безопасности. Это требует выработки новых подходов к регулированию обработки персональных данных, что предполагает, в частности, признание на уровне стратегического планирования критической

[260] См.: Чернышева. Е. Россияне сдали мошенникам рекордные ₽14 млрд. // РБК : [Электронный ресурс].. URL: https://www.rbc.ru/newspaper/2023/02/15/63eb5da89a794701b759621f (дата обращения: 28.12.23).
[261] См.: Мошенники убедили россиянку отдать им 750 тысяч рублей и поджечь гостиницу. // Газета.ру : [Электронный ресурс]. URL https://www.gazeta.ru/social/news/2023/11/02/21630997.shtml (дата обращения: 28.12.23)
[262] См.: Фроленко В. На Урале зафиксировали случаи принуждения жертв мошенников к поджогам военкоматов. // ТАСС. URL: https://tass.ru/proisshestviya/17567183 (дата обращения: 1.12.23).
[263] См.: Иванова В. По статье «диверсия» // Гудок : [Электронный ресурс]. URL https://gudok.ru/zdr/173/?ID=1637772 (дата обращения: 28.12.23).

значимости сведений о населении для национальной безопасности и формирование целостной системы мер по предотвращению их несанкционированного доступа.

Предлагается также рассмотреть внесение ряда дополнений в «Доктрину информационной безопасности Российской Федерации», связанных с защитой персональных данных. Например, в п. 8, посвящённый национальным интересам в информационной сфере, стоит внести следующее дополнение: «Обеспечение всесторонней защиты персональных данных физических лиц, особенно при обработке которых используются автоматизированные информационные технологии; кроме этого, особое внимание должно быть уделено обеспечению информационной безопасности автоматизированных систем в которых производится обработка персональных данных». В пп "ж" п. 23 Доктрины следует, после слов «иной информации ограниченного доступа и распространения», добавить фразу «…а также персональных данных», таким образом, подпункт приобретёт следующий вид «обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, а также сведений о населении (персональных данных физических лиц), путём повышения уровня защищённости соответствующих информационных систем и технологий в соответствии с установленными требованиями». В п. 25 Доктрины целесообразно акцентировать внимание на необходимости снижения числа мошенничеств в информационной сфере. Данные дополнения позволят сконцентрировать внимание на защите персональных данных, и способствовать улучшению безопасности обработки и хранения персональных данных на системном уровне.

Итак, в современных условиях становления информационного общества, роль персональных данных изменилась, и они превратились в социально-экономическую характеристику. Из-за чего их защищённость стала оказывать влияние не только на права личности, но и на сферу национальной безопасности. Для поддержания требуемого уровня защищённости интересов государства в области информационной безопасности важно на уровне документов стратегического планирования зафиксировать значимость персональных данных

для национальной безопасности, и важную роль их защиты для противодействия угрозам информационной безопасности в целях защиты интересов государства.

ГЛАВА 3 Отличительные черты совершенствования информационно-правового регулирования на протяжении жизненного цикла персональных данных при использовании «сквозных технологий»

§ 3.1 Информационно-правовое регулирование обработки персональных данных при использовании технологий искусственного интеллекта

Нейросети (искусственный интеллект) оказали значительные влияние на различные сферы жизни: «Согласно исследованию перспектив развития технологий искусственного интеллекта и возможностей их интеграции в различные сферы деятельности консалтинговой компании PricewaterhouseCoopers (далее — PwC), 72% топ-менеджеров компаний уверены, что уже в ближайшем будущем технологии искусственного интеллекта будут ключевым фактором формирования конкурентоспособности и устойчивости бизнеса на рынке. Более 60% участников исследования выразили уверенность, что искусственный интеллект помогает решать сложные задачи, стоящие перед бизнесом и социумом в целом, а 59% респондентов считают технологии искусственного интеллекта инструментом более полного раскрытия возможностей человека»[264].

До недавнего времени автоматизированные системы были жёстко ограничены заложенными в них при создании алгоритмами действий. Концепция обучаемых машин на основе нейронных сетей основана на понятиях и принципах математической логики, основы которой были заложены в начале XX века в работах учёных: Б. Рассела и А. Уайтхеда, позднее в 1943 году в науке появился термин «искусственный интеллект», впервые употреблённый трудах У. Мак-Коллока и У. Питтса. В 1951 году А. Тьюринг разработал свой знаменитый тест для определения «сильного» искусственного интеллекта. В дальнейшем концепция нейросетей развивалась, однако вычислительные мощности по-прежнему не позволяли в полной мере реализовать потенциал идеи «думающей машины» на практике. Лишь к началу 2020-х годов человечество получило возможность

[264] См.: Ступин Р. С. Искусственный интеллект в системе статистического анализа. // Цифровой регион: опыт, компетенции, проекты: Сборник трудов IV Международной научно-практической конференции, приуроченной к Году науки и технологий в России, Брянск, 25 ноября 2021 года. — Брянск: Федеральное государственное бюджетное образовательное учреждение высшего образования "Брянский государственный инженерно-технологический университет". — 2021. — С. 575–590.

производить мощные вычислительные процессоры и хранить большие объёмы информации для реализации концепции «обучаемых» нейронных сетей и применения их в промышленных масштабах. Актуализировался и вопрос правового регулирования общественных отношений, в том числе и в сфере обработки персональных данных.

Ключевая особенность, отличающая нейросети от других автоматизированных информационных систем состоит в том, что ИИ-системы способны к обучению и требуют меньше контроля со стороны оператора. «…Данные системы, в большинстве своем, пока еще нуждаются в управлении и поддержке человеком, хотя и максимально считаются приближенными к полностью автономным системам, работающим на основе своего “мозга” — нейронной сети. Особую роль в искусственном интеллекте имеет такое направление как обработка персональных данных»[265].

Применение нейросетей в сфере персональных данных позволяет решить множество различных задач, которые связаны с общественной безопасностью[266], медициной[267], банковской и финансовой сферой. «Искусственный интеллект в банках уже давно перестал быть только инструментом скоринга, как это было на начальном этапе, и стал всеобъемлющей технологией, которая коренным образом перестраивает все бизнес-процессы внутри финансовых институтов и организаций и, как следствие, повышает безопасность и комфорт сервисов, считают в Дом.РФ»[268]. Применение технологии нейросетей стало важным фактором повышения эффективности бизнес-процессов в различных сферах хозяйственной

[265] См.: Денисенко В. В., Евтеева К. С., Савченко И. И., Скрыпников А. А. Использование искусственного интеллекта для обработки персональных данных // Международный журнал гуманитарных и естественных наук. 2020. №7–1. с. 110–114.
[266] См.: Нейросеть в городе: как исскуственный интеллект помогает москвичам. // Ведомости : [Электронный ресурс]. Город. URL: https://www.vedomosti.ru/gorod/ourcity/articles/neiroset-v-gorode-kak-iskusstvennii-intellekt-pomogaet-moskvicham (дата обращения: 29.12.23).
[267] См.: 2023 Аналитический отчет "Система государственного стимулирования использования сервисов искусственного интеллекта в здравоохранении на основе анализа российского и зарубежного опыта", НЦРИИ. // Искусственный интеллект Российской Федерации : [Электронный ресурс]. URL: https://ai.gov.ru/knowledgebase/investitsionnaya-aktivnost/2023_analiticheskiy_otchet_sistema_gosudarstvennogo_stimulirovaniya_ispolyzovaniya_servisov_iskusstvennogo_intellekta_v_zdravoohranenii_na_osnove_analiza_rossiyskogo_i_zarubeghnogo_opyta_ncrii/ (дата обращения: 29.12.23).
[268] См.: Искусственный интеллект становится искусным поставщиком услуг. // Ведомости.Капитал : [Электронный ресурс]. URL: https://www.vedomosti.ru/kapital/trends/articles/2024/07/24/1051936-iskusstvennii-intellekt-stanovitsya-iskusnim-postavschikom-uslug (дата обращения: 29.12.23).

деятельности, как в бизнесе, так и в государственном управлении. Большое влияние оказало применение искусственного интеллекта и на сферу персональных данных — «по мере развития искусственного интеллекта он все больше увеличивает вовлеченность личной информации, тем самым увеличивая количество случаев утечки данных. Генеративные модели нейросетей могут быть использованы в противоправной деятельности, для создания поддельных профилей или манипулирования изображениями. Киберпреступления затрагивают безопасность 80% предприятий по всему миру, и мы понимаем, что личные данные в чужих руках могут иметь чудовищные последствия. Нам необходимо принять активные меры для защиты конфиденциальности информации наших клиентов с помощью аутентификации с использованием платформ данных»[269].

Технологическая доступность нейросетей породила новый вектор угроз: зафиксированы случаи применения данных алгоритмов злоумышленниками для реализации противоправных сценариев: «Использование интеллектуальных систем повышает эффективность, снижает издержки, минимизирует риски и позволяет повысить охват преступной деятельности. Преступный результат достигается без активного вовлечения преступника. Обучив и запустив систему, можно, не прилагая усилий, пользоваться результатами её работы»[270]. Применение такой многообещающей технологии в преступных целях является элементом наступившей цифровой реальности, при этом правонарушения во многих случаях затрагивают и сферу персональных данных.

Информационные брокеры активно стали использовать нейросети: «Брокеры данных — это компании, продающие персональную информацию. Они собирают данные из различных источников, составляют подробную картину о пользователе, а затем продают эту информацию. Продажа такой информации — это крупный бизнес: отрасль оценивается в 200 миллиардов долларов в год, а по всему миру

[269] См.: AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data. // The Economic Times : [Электронный ресурс]. URL ¨https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms?from=mdr (дата обращения: 29.12.23).

[270] См.: Дремлюга Р. И. "Использование искусственного интеллекта в преступных целях: уголовно-правовая характеристика" // Азиатско-Тихоокеанский регион: экономика, политика, право, том l. 23, №. 3, 2021, С. 153–165.

насчитывается до 4000 брокерских компаний… Деятельность брокеров данных критикуют за непрозрачность: брокеры данных не заинтересованы во взаимодействии с людьми, данные которых они собирают, анализируют и продают с целью получения прибыли. Брокеры данных не связаны прямыми отношениями с людьми, о которых они собирают данные. Большинство пользователей вообще не знает, что происходит сбор данных. Пользователи, часто не задумываясь, выбирают вариант “Я согласен” для политик конфиденциальности и условий использования. Однако не всегда очевидно, какой уровень контроля данных предоставляет брокеру такое согласие и каков совокупный эффект от согласия, предоставленного на большом количестве веб-сайтов. Сайты брокеров данных получают информацию несколькими способами, как онлайн, так и офлайн, постепенно выстраивая детализированные профили потребителей»[271]. Такие компании, имея огромные массивы данных, и получив в своё распоряжение мощный аналитический инструмент, стали применять его для получения новой личной информации физических лиц из имеющихся у них массивов данных, для того, чтобы повысить стоимость предлагаемого на продажу информационного продукта. Д. П. Десмонд отмечает: «Эта отрасль существовала до того, как ИИ стал массовым явлением, а теперь ИИ облегчает работу брокеров данных. В недавнем указе президента Байдена об искусственном интеллекте признается, что искусственный интеллект позволяет брокерам данных с большей легкостью “извлекать, повторно идентифицировать, связывать, делать выводы и действовать на основе конфиденциальной информации о личности, местонахождении, привычках и желаниях людей”»[272]. Применение ИИ-аналитики, и использование её, в том числе и брокерами данных, ставит перед государством задачу наращивания усилий по совершенствованию правовой защиты персональных данных из-за существенного изменения структуры общественных отношений в сфере персональных данных под влиянием масштабов применения нейросетей.

[271] См.: Как запретить брокерам данных продажу своей личной информацию // Лаборатория Касперского : [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-stop-data-brokers-from-selling-your-personal-information (дата обращения: 29.12.23).
[272] См.: AI Enables Data Brokers to Create “Detailed Dossiers”. // AI in Business : [Электронный ресурс]. URL: https://aiinbusiness.substack.com/p/ai-enables-data-brokers-to-create (дата обращения: 29.12.23).

Рассматривая применение ИИ-систем в сфере персональных данных, отметим два основных результата использования этой технологии, а именно: высокая эффективность анализа данных и генерация различной информации и данных.

Нейросеть может получать на основе анализа больших массивов информации новые знания и информацию, которые в некоторых случаях содержат персональные данные. Особенно эффективно ИИ-аналитика работает в связке с другой современной технологией, которая получила название «bigdata» или «большие данные» (подробнее влияние этой технологии на сферу персональных данных будет рассмотрено в п.3.2.) Е. С. Раздьяконов отмечает: «В последнее время большие данные широко используются для получения знаний во многих сферах деятельности. Однако это создает очень серьезную проблему безопасности, поскольку подобные данные могут содержать информацию, которая позволяет прямо или косвенно узнать и идентифицировать того или иного человека»[273]. Иностранные исследователи, также делают вывод о том, что развитие и применение технологии ИИ-аналитики может привести к невозможности для индивида осуществить своё право на тайну частной жизни[274]. Проблемой обеспокоены, в том числе и в Организации Объединённых Наций: Верховный комиссар ООН по правам человека в своём докладе в 2018 году выражал тревогу в том, что применение новых технологий, которые всё глубже проникают во все сферы человеческой жизни, начинает угрожать фундаментальному праву индивидуума на тайну частной жизни. В докладе отмечалось: «Аналитический потенциал технологий, основанных на использовании данных, продолжает расти в геометрической прогрессии. Методы анализа больших объёмов данных и нейросети расширяют возможности государств и компаний получать точную информацию о жизни людей, делать выводы об их физических, и психических, и иных характеристиках, что позволяет создавать подробные личные досье. Многие

[273] См.: Раздьяконов Е. С. Поиск персональных данных в неструктурированных текстах с использованием нейронных сетей. // Инженерный вестник Дона, №7 (2023) : [Электронный ресурс]. URL: http://ivdon.ru/uploads/article/pdf/IVD_86__6y23_razdyakonov.pdf_47d75621b4.pdf (дата обращения: 29.12.23).
[274] См.: Lee T. Tracing surveillance and auto-regulation in Singapore: «smart» responses to COVID-19 / T. Lee, H. Lee // Media International Australia. — 2020. — Vol. 177 (1). — P. 47–60.

системы, используемые правительствами и компаниями, создаются именно для этой цели — сбор максимального объема информации о физических лицах в целях анализа, профилирования, оценки, классификации и, в конечном итоге, принятия решений о них, причем зачастую автоматических. В результате создается среда, порождающая угрозы для людей и обществ, которые трудно переоценить»[275]. Влияние применения ИИ-аналитики на сферу персональных данных не подлежит сомнению.

Нейросети могут на основе проанализированных данных, в том числе и личной информации, получать новые персональные данные об индивидууме, о чём пишет А. В. Минбалеев: «Наиболее проблемным является вопрос о создании новых данных, полученных в результате самообучения нейронной сети… Всё это требует особого подхода с позиции выработки новых персональных данных… В связи с этим нам представляется, что в законодательстве о персональных данных должно быть закреплено, что обработка персональных данных с использованием нейронных сетей должна производиться только при условии письменного согласия субъекта персональных данных»[276]. Возможность применения нейросетей для анализа собираемых персональных данных вызвала насущную потребность включения в текст согласия на обработку персональных данных специальных положений о возможности запрета на обработку собираемой информации ИИ-системами.

Существенное воздействие на обеспечение конфиденциальности персональных данных оказала способность ИИ-решений в режиме реального времени осуществлять генерацию различной информации, в том числе аудио- и видеоформата. В последнее время достаточно широкое распространение получила технология подделки аудиовизуальной информации (далее deepfake, дипфейки). С её помощью, используя специальные алгоритмы нейросетей, можно в реальном

[275] См.: Право на неприкосновенность частной жизни в цифровой век. Доклад Верховного комиссара Организации Объединенных Наций по правам человека (A/HRC/39/29) // Сайт ООН : [Электронный ресурс]. URL: https://documents.un.org/doc/undoc/gen/g18/239/60/pdf/g1823960.pdf? (дата обращения: 29.12.23).
[276] См.: Минбалеев А. В., Сторожакова Е. Э. Проблемы правовой охраны персональных данных в процессе использования нейронных сетей // Вестник Университета имени О. Е. Кутафина. — 2023. — №2 (102) . — с. 71–79.

времени генерировать и подменять аудиовизуальный ряд в соответствии с задумкой оператора такой системы[277], в результате чего, получается реалистичный аудиовизуальный ряд подмены лица и\или голоса человека. Эта технология стала набирать популярность у злоумышленников, которые используют её для свершения различных противоправных действий, и таких случаев регистрируется всё больше и больше[278]. Дипфейки, помимо введения в заблуждение людей, используются и для обхода механизмов защиты, которые применяются, в том числе и при дистанционном банковском обслуживании, и другими сервисами, где необходима идентификация личности, также опирающаяся и на биометрические данные. «Больше всего в банках опасаются, что мошенники смогут использовать дипфейки для прохождения голосовой аутентификации, применяемой для проверки клиентов и предоставления им доступа к их учетным записям. Именно поэтому сотрудники стали задавать клиентам больше вопросов, чтобы убедиться, что звонят именно они “Людям всегда поступали мошеннические звонки. Но способность ИИ имитировать реальный голос человека, дающего указания что-то сделать, — это совершенно новые риски”»[279]. В нашей стране всё чаще стали фиксироваться случаи применения технологии подмены аудио- и\или видеоданных для совершения мошеннических действий в отношении физических лиц. Центральный Банк России сообщает: «…злоумышленники для хищения денег стали чаще использовать новый инструмент обмана — дипфейк-технологии. С помощью нейросети мошенники создают реалистичное видеоизображение человека. Затем сгенерированный образ рассылают его друзьям или родным через мессенджеры или социальные сети... Чтобы создать цифровую копию конкретного человека, злоумышленники используют фото и видео, а также запись голоса,

[277] См.: Обзор технологий создания Deepfake и методов его выявления. // ФГУП «ГРЧЦ : [Электронный ресурс]. URL: https://rdc.grfc.ru/2020/06/research-deepfake/ (дата обращения: 03.03.24).
[278] См.: Кузнецов М. Эффект зловещей долины: как распознать дипфейк и не дать себя обмануть. // FORBES : [Электронный ресурс]. URL: https://www.forbes.ru/finansy/439601-effekt-zlovesej-doliny-kak-raspoznat-dipfejk-i-ne-dat-seba-obmanut (дата обращения: 03.03.24).
[279] См.: Фролова М. Рост на 700%: мошенники стали чаще использовать дипфейки в сфере финансов. // Известия : [Электронный ресурс]. URL: https://iz.ru/1679621/mariia-frolova/rost-na-700-moshenniki-stali-chashche-ispolzovat-dipfeiki-v-sfere-finansov (дата обращения: 03.03.24).

полученные, в основном, в результате взлома его аккаунта в социальных сетях или мессенджерах»[280].

Способность нейросетей быстро осуществлять генерацию новой информации, в том числе и биометрической, которая используется для идентификации личности, как другими людьми, так и автоматизированными системами, оказала ощутимое влияние на отношения, которые связаны с идентификацией личности, и эта сложная проблема имеет межотраслевой характер; этот вопрос поднимается в юридической литературе «…требуется правовое регулирование не только в отрасли уголовного права, но и в гражданско-правовой отрасли, а также и административной. Нейросети позволяют создавать образы политиков, которые несут ответственность перед всем миром. Дипфейк позволяет синтезировать не только внешность, но и голос, именно по этой причине в США дипфейки признали на государственном уровне угрозой национальной безопасности. Ведь Deepfake может стать новой “ядерной бомбой” для преступников»[281]. Подменяя аудиовизуальный образ собеседника, злоумышленники могут вводить свою жертву в заблуждение с целью получения наживы; во многих случаях мошенники стараются втереться в доверие к пожилым людям, которые в силу возраста оказываются более внушаемы[282].

Обобщая, можно сказать о том, что широкое распространение технологии дипейков оказало значительное влияние на отношения, которые связаны с обработкой персональных данных, причём оно оказалось настолько существенным, что затронуло фундаментальные права человека, что нашло отражение в докладе 2021 года Верховного Комиссара ООН по правам человека[283]. Аналогичного мнения придерживаются и органы Европейского Союза, например в

[280] См.: Мошенники обманывают людей с помощью дипфейков. // Центральный Банк России : [Электронный ресурс]. URL: https://cbr.ru/information_security/pmp/15082024/ (дата обращения: 03.03.24).
[281] См.: Данилова В. А., Левкин Д. М. Правовые аспекты регулирования "deepfake" технологии в россии // Право и государство: теория и практика. 2022. №7 (211), стр. 88–91.
[282] См.: Бобрышев Е. Экс-командующий сухопутными войсками РФ и его жена стали жертвами мошенников. // РИАМО : [Электронный ресурс]. URL https://riamo.ru/news/proisshestviya/eks-komandujuschij-suhoputnymi-vojskami-rf-i-ego-zhena-stali-zhertvami-moshennikov/ (дата обращения: 03.07.24).
[283] См.: Artificial intelligence risks to privacy demand urgent action – Bachelet // ООН, Офис Верховного комиссара по правам человека : [Электронный ресурс]. URL: https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet?LangID=E&NewsID=27469 (дата обращения: 03.07.24).

докладе об «Artificial Intelligence Act»[284], где высказывают мнение, что идентификация физических лиц, проводимая удалённо, посредством биометрических данных, с высокой степенью вероятности будет вторжением в частную жизнь человека, а также автоматическая идентификация и классифицирование могут нарушать право на достоинство личности. Эти принципы позднее выразились в нормах «EU AI Act»[285], среди которых в контексте персональных данных отметим следующие запреты применения ИИ-решений: удалённая идентификация и категоризация по биометрии в реальном времени (с исключениями для правоохранительных органов); применение нейросетей для поведенческого анализа, применение ИИ-алгоритмов для манипулирования человеком и воздействия на его поведение, а также для эксплуатации слабостей; запрещены системы сбора и агрегации фото- и видеоинформации в сети Интернет, не ограниченные конкретной целью. Всё это подтверждает тезис о необходимости урегулирования применения нейросетей в сфере персональных данных. Однако, учитывая сложность и многогранность отношений, которые возникают при использовании нейросетей во время обработки персональных данных необходимо выработать такие подходы, которые бы не только защищали права и свободы личности, но и обеспечивали защиту интересов всего общества и государства. Применение ИИ-систем в некоторых областях позволяет значительно сократить время реакции на события, которые затрагивают безопасность общества или государства. В Российской Федерации уже создан ИИ-комплекс, задача которого оказывать помощь в выявлении поддельных документов у приезжих[286]. Использование такого инструмента позволит увеличить эффективность работы контролирующих органов, а также положительно скажется не только на качестве миграционных процедур, но и позволит снизить их коррупциогенность, за счёт

[284] См.: EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). // EDPИ : [Электронный ресурс]. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en (дата обращения: 12.07.24).
[285] См.: The AI Act. // Future of Life Institute. URL: https://artificialintelligenceact.eu/ai-act-explorer/ (дата обращения: 12.07.24).
[286] См.: В России разработали нейросеть, выявляющую террористов среди мигрантов. // РИА Новости : [Электронный ресурс]. URL: https://ria.ru/20240413/neyroset-1939738693.html (дата обращения: 12.07.24).

уменьшения роли человека. А поскольку на стратегическом уровне применение технологии ИИ-систем будет способствовать достижению цели обеспечения национальной безопасности и правопорядка, то применение нейросетей будет расширяться, в том числе и для обработки и персональных данных физических лиц. Однако, до тех пор, пока технология и алгоритмы не будут в достаточной степени отлажены и отработаны, конечное решение, должно оставаться за человеком. Это позволит уменьшить риск возникновения ошибок из-за несовершенства технологии. Кроме того, применение нейросетей для обработки рутинных и объёмных задач позволит решать их быстрее и более качественно.

Два основных результата использования искусственного интеллекта для обработки информации о физических лицах — высокая эффективность анализа данных и генерация новой информации. Способность нейросетей осуществлять генерацию биометрической информации, которая используется для идентификации личности, как другими людьми, так и автоматизированными системами, оказала ощутимое воздействие на отношения, связанные с обработкой и защитой персональных данных и идентификацией личности. В первую очередь изменения коснулись аналитики, которую искусственный интеллект вывел на качественно новый уровень. Правовой режим генерируемой новой информации, содержащей персональные данные физических лиц, до сих пор в отечественном законодательстве не определён. Применение нейросетей в сфере работы с персональными данными в целом позитивно и позволяет решить множество задач. Однако злоумышленники уже начали использовать нейросети для достижения противозаконных, в том числе преступных, целей. Генеративные алгоритмы нейросетей породили проблему, но и поставили перед юристами и государством задачу по выработке новых процедур и алгоритмов идентификации личности по биометрическим данным, которые были бы устойчивы к неправомерному применению технологий.

Важным фактором, влияющим на отношения в сфере обработки персональных данных, является отсутствие в законодательстве процедуры фиксации согласия или несогласия субъекта персональных данных на обработку

информации о нём искусственным интеллектом. Кроме этого, государство сталкивается с необходимостью формирования нормативно-правовых подходов к обеспечению защиты биометрических процедур идентификации личности, с учётом новых угроз и вызовов, в том числе связанных и с фальсификацией биометрических данных при помощи разных технологий.

Разработка нормативного регулирования применения нейросетей в сфере безопасности осложняется тем, что необходимо соблюсти баланс между защитой прав субъектов персональных данных и эффективностью применения ИИ-аналитики для прогнозирования правонарушений. Именно обеспечение такого баланса позволит максимально эффективно и продуктивно использовать весь потенциал этой многообещающей технологии. Особенно это актуально в сфере безопасности, где применение нейросетей может предотвратить совершение, как мошенничеств, так и террористических атак.

Появление ИИ-решений вывело на новый уровень применение аналитических систем, в том числе и для противодействия правонарушениям и обеспечения безопасности; благодаря применению этой технологии стало возможно прогнозировать различные правонарушения[287]. Важной особенностью применения нейросетей является не только обработка ими персональных данных для анализа обстановки, но и получение при этом новой личной информации в процессе работы. Правовой режим применения ИИ-аналитики в сфере безопасности в нашей стране ещё не выстроен, что ставит перед государством и юридическим сообществом задачу, в том числе и по урегулированию отношений в этой области. Разработка нормативного регулирования применения нейросетей в сфере безопасности осложняется тем, что необходимо соблюсти баланс между защитой прав субъектов персональных данных и эффективностью применения На фоне повышения эффективности ИИ-аналитики в прогнозировании событий актуализируется задача формирования критериев и методологического инструментария для оценки воздействия на права человека (далее — ОВПЧ) при

[287] См.: Дроздов В. Ю. Использование искусственного интеллекта для предупреждения преступности. // Закон и право. — 2021. — № 9. — С. 114–117.

внедрении нейросетей, включая сферу правоохранительной деятельности. В документе Комиссара Совета Европы по правам человека сообщается: «Нормативно-правовая база по ОВПЧ должна предусматривать самостоятельную оценку государственными органами существующих и предлагаемых систем ИИ. В ходе проведения такой оценки необходимо рассматривать потенциальное воздействие систем ИИ на права человека, учитывая характер, контекст, сферу применения и задачи таких систем. В случаях, когда государственный орган еще не приобрел или не разработал предлагаемую систему ИИ, такая оценка должна предшествовать приобретению/разработке системы ИИ. ОВПЧ также должна включать в себя содержательный внешний анализ системы ИИ, проводимый либо независимым контролирующим органом, либо внешним экспертным лицом/аудитором с соответствующими компетенциями. Такой анализ призван помочь в обнаружении, количественной оценке и (или) описании воздействия и рисков в области прав человека, которые могут возникнуть с течением времени»[288]. Концептуальной основой правового регулирования ИИ-систем должна стать методология, ориентированная на анализ степени воздействия данных технологий на реализацию фундаментальных прав и свобод человека. Применение нейросетей для обработки информации о физических лицах напрямую затрагивает конституционное право человека на невмешательство в частную жизнь. Включение Совета по правам человека при Президенте РФ в процесс формирования законодательства по вопросам обработки персональных данных и информационной безопасности представляется методологически оправданным: это позволит создать дополнительные институциональные гарантии защиты конституционных прав и свобод граждан. Кроме этого, в рекомендациях, подготовленных Комиссаром Совета Европы по правам человека, акцентируется внимание на необходимости независимого контроля за соблюдением прав человека на всех этапах жизненного цикла ИИ-систем, а также независимости таких контролирующих органов от государства, и расширения в этой области

[288] См.: Рекомендации раскрытие искусственного интеллекта: 10 шагов для защиты прав человека. // Council of Europe : [Электронный ресурс]. URL: https://rm.coe.int/-10-/16809a42e4 (дата обращения: 12.07.24).

полномочий национальных структур по правам человека. Выстроенная система независимого аудита за разработкой и применением ИИ-алгоритмов позволит не только осуществлять контроль уже действующих и применяемых систем искусственного интеллекта, но и тех, которые находятся на стадии проектирования и разработки. Такой подход даст возможность предотвращать появление ИИ-решений, сама логика работы которых оказывает отрицательное влияние на защищённость прав человека, в том числе и связанных с защитой персональных данных.

Требуется комплексное обновление правового регулирования: совершенствование существующих норм защиты персональных данных и разработка отдельной правовой концепции для регламентации применения нейросетей при обработке таких данных. Достижение устойчивого равновесия интересов в данной предметной области является комплексной задачей, решение которой не может быть реализовано в сжатые временные рамки. Вместе с тем требуется непрерывное развитие регуляторных механизмов, обеспечивающих правомерное применение нейросетях контексте обработки персональных данных.

Принятая «Национальная стратегия развития искусственного интеллекта на период до 2030 года» и дополненная[289] в 2024 году (далее — Стратегия) содержит принципы, приоритетные направления, цели и задачи развития технологии ИИ-систем в нашей стране. Ключевой принцип (пп. "а" п. 19 Стратегии) развития и использования нейросетей гласит: «защита прав и свобод человека: обеспечение защиты прав и свобод человека, гарантированных законодательством Российской Федерации, международными договорами Российской Федерации и общепризнанными принципами и нормами международного права, в том числе права на труд, и предоставление гражданам возможности получать знания и приобретать навыки для успешной адаптации к условиям цифровой экономики»[290].

[289] См.: Указ Президента РФ от 15.02.2024 № 124"О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490 "О развитии искусственного интеллекта в Российской Федерации" и в Национальную стратегию, утвержденную этим Указом" // "Собрание законодательства РФ", 19.02.2024, № 8, ст. 1102

[290] См.: пп. "а" п. 19 Указ Президента РФ от 10.10.2019 № 490 "О развитии искусственного интеллекта в Российской Федерации" (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года") // Собрание законодательства РФ, 14.10.2019, № 41, ст. 5700..

Институционализация данного принципа в системе стратегического планирования знаменует собой важный этап в развитии правового регулирования нейросетевых технологий: впервые приоритет прав и свобод человека закрепляется как доминирующий критерий. Обоснованность рассматриваемого подхода определяется способностью ИИ-систем воздействовать на конституционные права граждан, в особенности при работе с персональными данными. Данный тезис находит подтверждение во втором принципе применения нейросетей (пп. “б” п. 19 Стратегии), предусматривающем соблюдение требований к конфиденциальности такой информации. Однако документ не учитывает того, что при обработке различных наборов данных нейросеть может получить новые персональные данные о человеке. Правовой режим этой информации на данный момент не определён, кроме этого, отсутствует законодательное установление принципов обработки персональных данных при помощи технологии нейросетей; данный вопрос является стратегически важным, и его решение позволит повысить эффективность правовой защиты персональных данных физических лиц при обработке такой информации искусственным интеллектом. Для решения этой задачи предлагается установить следующие принципы применения ИИ-систем для обработки персональных данных:

1) Добровольность согласия на обработку персональных данных ИИ-системами (далее Первый принцип);
2) Приоритет защиты прав личности в случае, если это не создаёт угрозу безопасности других людей и\или государства (Второй принцип);
3) Контроль влияния на права человека применения ИИ-систем (Третий принцип);
4) Повышенные стандарты безопасности ИИ-систем, обрабатывающих персональные данные (Четвёртый принцип);
5) Прозрачность обработки персональных данных для физического лица (Пятый принцип);
6) Обеспечение безопасности конституционного строя Российской Федерации при создании информационных систем искусственного

интеллекта, их эксплуатации и реализации комплекса мер по защите персональных данных, содержащихся в этих системах. (Шестой принцип);

Первый принцип опирается на конституционную норму, гарантирующую право граждан на неприкосновенность частной жизни как одну из базовых гарантий прав человека (п.1 ст.23 ч.2 Конституции Российской Федерации) и недопустимости сбора такой информации без согласия человека (п.1 ст.24 ч.2 Конституции Российской Федерации), а также на принципе неприкосновенности частной жизни граждан, установленном в п.7 ст.3 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Необходимость *второго принципа* обоснована положениями Конституции Российской Федерации, гарантиями государственной защиты прав и свобод человека и гражданина (п.1 ст.45 ч.2 Конституции Российской Федерации);

Третий принцип связан с потребностью в отслеживании того, как влияет применение нейросетей на права и свободы человека и гражданина, при обработке его персональных данных, что находит своё основание в положениях Главы 2 Конституции Российской Федерации, норм Федерального конституционного закона от 26.02.1997 № 1-ФКЗ «Об Уполномоченном по правам человека в Российской Федерации» и соотноситься с ст. 2 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», которая требует обеспечить защиту конституционных прав и свобод человека. Контроль за влиянием на эти права является важной составляющей механизма зашиты конституционных прав; в комментариях к Конституции Председатель Конституционного суда Российской Федерации В. Д. Зорькин замечает: «Право на частную жизнь, в том числе на информационное невмешательство в нее, основывается на идее самоопределения и автономности личности, свободе индивида в приватной, интимной сфере его жизни от внешнего контроля со стороны государства и общества… Между тем существует другая проблема. Множество государственных и муниципальных органов, юридических и физических лиц в силу своей компетенции или характера и целей деятельности накапливают у себя, хранят и используют данные, в том числе в виде компьютерных баз и информационных систем, которые содержат

сведения, относящиеся к частной жизни граждан, а в определенных случаях обязывают их предоставлять им информацию такого рода»[291].

Четвёртый принцип обусловлен тем, что обеспечение безопасности таких информационных систем затрагивает не только права физических лиц, но и интересы государства в области национальной безопасности. Кроме этого, защита конституционных прав граждан гарантирована Конституцией Российской Федерации, что выражается, в том числе и в предупреждении возникновения нарушений в этой области, о чём пишет В. Д. Зорькин: «Исполнение государством соответствующей обязанности не только требует наличия необходимых социально-экономических и политических условий, обеспечивающих реализацию прав и свобод человека и гражданина, но и предполагает функционирование государственно-правового механизма, предназначенного для предупреждения нарушений в этой сфере, а также восстановления прав и свобод в случаях их нарушения»[292]. Таким образом, установление этого принципа будет соотноситься с положениями Конституции Российской Федерации.

Пятый принцип способствует осуществлению конституционного права, установленного в п.2 ст.45 ч.2 Конституции Российской Федерации, а именно позволяет человеку контролировать обработку его данных системами искусственного интеллекта и обнаруживать угрозу или нарушение своих конституционных прав и своевременно реагировать на такие факты, используя законные средства. Мнение В. Д. Зорькина касательно права личности контролировать информацию о своей частной жизни: «Как указывается в Определении КС РФ от 9 июня 2005 г. № 248-О, право на неприкосновенность частной жизни означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера»[293].

[291] См.: Комментарий к Конституции Российской Федерации / Под ред. проф. В. Д. Зорькина — 3-е изд., пересмотр. — Москва: Норма: НИЦ ИНФРА-М, 2013. — 1040 с. ISBN 978-5-91768-441-3.
[292] См.: Там же.
[293] См.: Там же.

Шестой принцип согласуется с п.5 ст.5 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Помимо этого, результаты проведённого исследования демонстрируют, что защита персональных данных оказывает многоаспектное влияние: она затрагивает как индивидуальную безопасность личности, так и сферу национальной безопасности государства. Данный факт необходимо принимать во внимание при разработке и внедрении ИИ-систем. В рамках анализа Конституции Российской Федерации В. Д. Зорькин затрагивает этот вопрос: «Иными словами, права и свободы нельзя рассматривать в отрыве от конституционного строя государства, социальной, политической и экономической системы общества, так как именно в них коренятся гарантии прав человека, которые он имеет в силу принадлежности к роду человеческому. Отсюда следует, что категория прав человека выступает теперь в качестве основы идеологии и практики демократического переустройства общества»[294]. Таким образом, применение ИИ в сфере обработки персональных данных оказывает влияние и на конституционный строй нашей страны.

Правовое регулирование использования нейросетевых технологий в Российской Федерации пока ещё только выстраивается, и общефедеральный закон, который бы охватывал применение этой технологии, пока отсутствует. Вместо этого законодатель использовал точечное регулирование, через введение экспериментальных правовых режимов. Их можно разделить по направлениям, а именно: беспилотный автомобильный транспорт, беспилотный воздушный транспорт, медицина, государственное управление, промышленное производство и сельское хозяйство, а также строительство и капитальный ремонт. Экспериментальные правовые режимы применения ИИ в этих областях уже применяются в следующих городах и регионах нашей страны: в Москве, Иннополисе, Томской области, Самарской области и др. Организация экспериментальных правовых режимов позволяет в тестовом режиме изучить

[294] См.: Комментарий к Конституции Российской Федерации / Под ред. проф. В. Д. Зорькина — 3-е изд., пересмотр. — Москва: Норма: НИЦ ИНФРА-М, 2013. — 1040 с. ISBN 978-5-91768-441-3.

действенность правовых подходов к регулированию использования систем искусственного интеллекта в различных условиях. Корректировки в этом случае в соответствующие нормативно-правовые акты вносятся значительно более оперативно, чем при действующем общефедеральном законодательстве.

Защите персональных данных при их обработке в системах искусственного интеллекта уделено недостаточно внимания. В условиях становления информационного общества такой изъян в правовой защите персональных данных недопустим, о чём говорится в юридической литературе: «по мере развития глобального информационного общества вопросы защиты персональных данных становятся все более актуальными и требуются решительные действия законодателя»[295]. Следовательно, помимо принципов обработки персональных данных нейросетями, которые изложены выше, необходимо на законодательном уровне установить и требования к обработке такой информации ИИ-системами. Это позволит в значительной степени повысить защищённость личной информации физических лиц в условиях распространения ИИ-решений и устранить дефекты регулирования, пусть на данный момент и экспериментального, в сфере применения этой технологии.

Требования к применению нейросетей, в том числе и в работе с персональными данными, должны соответствовать сформулированным выше принципам применения ИИ-систем для обработки личной информации. Предлагается следующий перечень требований:

1. Субъект персональных данных должен быть проинформирован о том, что его данные будут собираться и обрабатываться ИИ-системой (далее Первое требование);
2. Обработка персональных данных ИИ-системой осуществляется только с разрешения субъекта персональных данных или уполномоченного им лица (Второе требование);

[295] См.: Чеботарева А. А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе // Юридический мир. — 2016. — № 8. — С. 63–66. — Библиогр.: с. 66 (6 назв.). — ISSN 1811-1475.

3. ИИ-алгоритмы, обрабатывающие персональные данные в коммерческих целях, подлежат обязательной регистрации уведомительным порядком у уполномоченного государственного органа. (Третье требование);

4. К ИИ-решениям, которые обрабатывают специальные категории персональных данных, должны предъявляться повышенные требования безопасности (Четвёртое требование);

5. ИИ-системы, которые обрабатывают специальные категории персональных данных, подлежат независимому аудиту не реже раза в 2-3 года и учёт таких систем должен осуществляться в особом порядке уполномоченной организацией (Пятое требование);

Первое требование необходимо для того, чтобы индивидуум, чьи данные планируется обрабатывать с помощью ИИ-алгоритма, был об этом явно проинформирован и чётко осознавал, какой именно системой будут обрабатываться информация, которую он о себе предоставит;

Второе требование согласовывается с необходимостью зафиксировать волеизъявление субъекта персональных данных персональных данных на их обработку (пп. 1 п. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»), различия в архитектуре и функционале систем искусственного интеллекта по сравнению с традиционными системами обработки персональных данных служат достаточным основанием для выдвижения данного требования;

Третье требование позволит регулятору иметь сведения о ИИ-системах, обрабатывающих персональные данные, это согласуется с необходимостью уведомлять регулятора о начале обработки персональных данных (п.1 ст. 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

Четвёртое требование связано с тем, что специальные категории персональных данных затрагивают личную сферу человека, поэтому требуют особого отношения, разглашение такой информации, не только нарушит права человека, но и может иметь негативные последствия для субъекта персональных данных.

Пятое требование связано с тем, что безопасность обработки специальных категорий персональных данных должна обеспечиваться на высоком уровне; периодический аудит же таких ИИ-решений позволит уменьшить риск нарушения конституционных прав граждан и своевременно выявлять недобросовестных операторов персональных данных.

Законодательное установление этих требований при регулировании общественных отношений, связанных с обработкой информации о физических лицах ИИ-системами, будет способствовать повышению защищённости персональных данных в условиях изменяющихся социальных отношений в нашей стране.

В достаточной мере очевидно, что применение нейросетей в определённой степени повлияло на изменение общественных отношений в этой области. Важной особенностью воздействия ИИ-систем на социальные отношения стало то, что и их использование начало затрагивать область защиты персональных данных. Поэтому государства, лидирующие в области создания и внедрения ИИ-систем начали разрабатывать законодательство, регулирующее применение таких систем. Особое место в котором, занимают нормы, относящиеся к защите персональных данных при их обработке нейросетями. В нашей стране всё ещё ведётся работа по разработке такого законодательства. Имеющаяся нормативно-правовая база в сфере регулирования применения ИИ-систем не всегда уделяет достаточное внимание проблематике защиты персональных данных. Решению этой проблемы будет способствовать установление на законодательном уровне принципов обработки персональных данных системами искусственного интеллекта. Также необходимо установить ряд требований к ИИ-системам, которые обрабатывают личную информацию физических лиц. Это конкретизирует правила применения нейросетей при сборе, хранении и обработке персональных данных, что будет способствовать улучшению правовой защиты персональных данных при их обработке ИИ-системами.

§ 3.2 Взаимосвязь и взаимовлияние технологии «больших данных» и организационно-правовой защиты персональных данных

Появление глобальной сети Интернет стало одним из факторов, который привёл к тому, что в автоматизированных информационных системах стали скапливаться огромные массивы информации, в том числе и, на первый взгляд, не не содержащие персональные данные. Технология агрегации и хранения больших и разрозненных информационных массивов получила название bigdata, что переводится на русский язык как «большие данные» и которые можно охарактеризовать как: «большие массивы данных, отличающиеся главным образом такими характеристиками, как объем, разнообразие, скорость обработки и/или вариативность, которые требуют использования технологии масштабирования для эффективного хранения, обработки, управления и анализа»[296].

Появление этой технологии оказало влияние на многие стороны общественной жизни[297]. «Умные города» генерируют огромное количество различной информации и данных[298] в процессе своей жизнедеятельности, эти данные позволяют значительно повысить эффективность управления городской инфраструктурой и улучшить жизнь проживающих в таких городах людей. Bigdata также применяется в медицине[299] и здравоохранении[300], в образовании[301], в банковском и финансовом секторах. Центральный Банк России сообщает: «В последние годы становится все более распространенным применение технологий обработки больших данных в финансовом секторе. Данные технологии

[296] См.: ГОСТ Р ИСО/МЭК 20546-2021 // Федеральное агентство по техническому регулированию и метрологии : [Электронный ресурс]. URL: https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=4&month=4&year=-1&search=&id=240981 (дата обращения: 16.05.25).
[297] См.: Денисова А. Б., Сенюшина В. Г. Влияние информационной реальности на существование человека // Современные проблемы науки и образования. — 2012. — № 6 с. 347.
[298] См.: Слагаемые успеха: технологии умного города. // CNEWS : [Электронный ресурс]. URL: http://smartcity.cnews.ru/articles/2018-08-09_slagaemye_uspeha_tehnologii_umnogo_goroda (дата обращения: 16.05.25).
[299] См.: Овчинникова М. А. Применение big data в лабораторной медицине / М. А. Овчинникова, Ю. И. Жиленкова, Н. Ю. Черныш // Российский журнал персонализированной медицины. — 2023. — Т. 3, № 4. — С. 77–87.
[300] Полубинская С. В. Big Data в здравоохранении: информационная безопасность и правовая охрана персональных данных / С. В. Полубинская, М. И. Галюкова // Государство и право. – 2023. – № 6. – С. 149-160
[301] См.: Большие данные и их применение в образовании / М. В. Алиева, З. Б. Батчаева, З. М. Муцурова, М. З. Исаева // Журнал прикладных исследований. — 2023. — № 6. — С. 140–146.

потенциально способствуют повышению качества предоставляемых услуг, помогают финансовым организациям снизить издержки и повысить эффективность деятельности. Большие данные используются практически всеми крупными финансовыми организациями, а также консалтинговыми и технологическими компаниями, оказывающими услуги в финансовом секторе»[302]. Таким образом, широкое применение технологии bigdata с целью повышения эффективности различных услуг, в достаточной степени доказано.

Однако существует и другая сторона применения этой технологии, а именно — большая вероятность получения доступа к таким данным различного рода злоумышленниками, террористическими или разведывательными структурами. Анализ находящихся в открытом доступе больших объемов информации существенно облегчает и повышает эффективность разведывательных мероприятий. Теперь для того, чтобы обнаружить военную базу достаточно получить доступ к данным сотовых операторов или производителя фитнес-браслетов. Так, в начале 2018 года, благодаря данным с фитнес-браслетов американских военнослужащих, были обнаружены военные базы на территории Сирии и Ирака.

Кроме этого, такие информационные массивы могут содержать сведения, относящиеся к частной жизни граждан[303]. Исследование массивов информации, собираемых через социальные сети, позволяет оперативно выявлять и управлять реакцией пользователей социальных сетей[304] на различные события. Например, анализ реакции пользователей социальных сетей на различные действия власти позволяет определить стратегию поведения в отношении оппозиции, протестный потенциал или реакцию общества на те или иные события. Так, социальные сети использовались для организации масштабных протестов во многих странах Ближнего Востока и некоторых странах СНГ.

---

[302] См.: Использование больших данных в финансовом секторе и риски финансовой стабильности. // ЦБ РФ. URL: https://cbr.ru/Content/Document/File/131359/Consultation_Paper_10122021.pdf (дата обращения: 18.06.25).
[303] См.: Расследование: как обезличенные данные становятся персональными и продаются на сторону. // ХАБР : [Электронный ресурс]. URL: https://habr.com/ru/post/518458/ (дата обращения: 18.06.25).
[304] См.: Развитие методов анализа социальных явлений с использованием больших данных соцсетей. // ВШССН МГУ : [Электронный ресурс]. URL: https://nosh.msu.ru/math/tpost/zxkjfmab31-razvitie-metodov-analiza-sotsialnih-yavl (дата обращения: 12.07.24).

Упомянем о тесной связи с bigdata с персональными данными. Казалось бы, две, не связанные друг с другом сущности, такие как персональные и «большие данные», что может быть между ними общего? Ответ на этот вопрос заключается в том, что при анализе массивов информации можно получить новые знания. Которые могут содержать персональные данные конкретных физических лиц. В юридической научной литературе отмечается: «В отсутствие общепризнанного определения больших данных их признаки описаны в современной литературе. Обработка больших данных пока находится вне правового поля, поэтому наиболее значимую юридическую проблему представляет “соприкосновение” с персональными данными, в отношении которых правила уже установлены. Любые нарушения в этой сфере напрямую затрагивают права человека, особенно право на частную жизнь»[305]. И в связи с этим обстоятельством, а также по причине того, что происходит кардинальная трансформация общественных отношений под влиянием широкомасштабного использования различных информационно-коммуникационных технологий, в том числе и технологии bigdata, перед государством и юридическим сообществом возникла задача, связанная с совершенствованием правового регулирования отношений по обработке больших массивов информации с применением новых технологий.

Единых подходов к правовому регулированию «больших данных» международное сообщество ещё не выработало, по этому вопросу идут оживлённые дискуссии.

В Европейском союзе обработка информации о физических лицах с помощью технологии bigdata подпадает под регулирование общеевропейского законодательства, принятого в 2016 году. В Китае основные принципы регулирования изложены в законе о кибербезопасности (2016 г.), подзаконных актах и стандартах к нему, где установлены требования к хранению данных и запрет на их трансграничную передачу. В КНР широкое применение получило использование технологии больших данных со стороны государства в различных

[305] См.: Талапина Э. В. Большие данные и права человека: на пути к правовому регулированию // Государство и право. 2023. № 7. С. 129–138.

сферах экономики и национальной безопасности. В январе 2018 года был представлен новый проект стандарта по защите данных, который во многом копирует законодательство Европейского Союза. В США использование этой технологии регулируется множеством как федеральных законов, так и законов штатов. В Японии bigdata подпадают под действие норм закона от 2017 года «О защите персональных данных»: структурно правовое регулирование включает два взаимосвязанных блока, нормы анонимизации данных, а также нормы, закрепляющие правовой статус больших данных как потенциально охраняемого объекта интеллектуальных прав компаний.

Помимо регулирования персональных данных в условиях цифровизации социальных отношений, важным правовым аспектом является регламентация отношений, связанных с технологией bigdata, которая базируется на правовом определении этого понятия. Важность урегулирования этой сферы связана с тем, что такие наборы информации являются интегрированным «цифровым следом», который оставляют как физические, так и юридические лица, в условиях цифровизации всех сфер общественной жизни. Выработка легального определения термина bigdata представляет собой достаточно неординарную задачу, стоящую перед юристами, из-за того, что эта технология является достаточно сложной[306], и даже её техническое определение насчитывает несколько[307] вариантов[308].

В 2017 году. Указом Президента Российской Федерации была утверждена «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы». Введение в стратегический документ первого в отечественной практике правового определения технологии bigdata знаменует институционализацию подхода к её регулированию и переход от фрагментарного к системному правовому оформлению сферы: «Обработка больших объемов

[306] См.: Что такое Big Data — большие данные. // Сайт корпорации Oracle : [Электронный ресурс]. URL: https://www.oracle.com/ru/big-data/what-is-big-data/ (дата обращения: 12.06.25).
[307] См.: Что такое big data: зачем нужны большие данные, как их собирают и обрабатывают. // Журнал Mail.ru : [Электронный ресурс]. “Cloud Solutions об IT-бизнесе, технологиях и цифровой трансформации”. URL: https://mcs.mail.ru/blog/big-data-vse-govoryat-no-malo-kto-shchupal (дата обращения: 16.06.25).
[308] См.: Что такое Big data. // Rusbase : [Электронный ресурс] URL: https://rb.ru/howto/chto-takoe-big-data/ (дата обращения: 16.06.25).

данных — совокупность подходов, инструментов и методов автоматической обработки структурированной и неструктурированной информации, поступающей из большого количества различных, в том числе разрозненных или слабосвязанных, источников информации, в объемах, которые невозможно обработать вручную за разумное время»[309].

Помимо «Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» при определении правовых подходов к регулированию использования bigdata также обращает на себя внимание «Доктрина информационной безопасности Российской Федерации».

Большие данные отличает от персональных неструктурированность, в некоторых случаях обезличенность, и невозможность без дополнительных усилий определить их отношение к тому или иному физическому лицу. Применение технологии bigdata может не подпадать под действие Федерального закона № 152-ФЗ «О персональных данных», поскольку такие данные могут быть обезличены. В Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» есть понятие «информация», однако отсутствуют понятия «большие данные», «обработка больших данных», «оператор больших данных». Следовательно, нормы действующего законодательства, которое регулирует обращение персональных данных, к социальным отношениям, связанным с технологией bigdata, не всегда применимы. Это влечёт за собой снижение уровня защищённости персональных данных. В 2018 году была предпринята первая попытка включить в правовое поле сферу обработку массивов больших данных. В Государственную Думу Федерального Собрания Российской Федерации был внесён законопроект № 571124-7 о регулировании больших (пользовательских) данных, на который в ноябре 2018 года были получены отрицательные заключения Правого управления Государственной Думы и Комитета Государственной Думы по информационной политике, информационным технологиям и связи.

[309] См.: Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы. // Собрание законодательства Российской Федерации, № 20, 15.05.2017, ст.2901.

Проект предусматривал внесение изменений в Федеральный закон № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», должен был внести понятия «большие пользовательские данные», «оператор больших данных», «обработка больших пользовательских данных»: «большие пользовательские данные — совокупность не содержащей персональных данных информации о физических лицах и (или) их поведении, не позволяющая без использования дополнительной информации и (или) дополнительной обработки определить конкретное физическое лицо, собираемой из различных источников, в том числе сети «Интернет», количество которых превышает тысячу сетевых адресов»[310], как следует из определения, с точки зрения юристов bigdata это совокупность данных, которая не содержит персональные данные физических лиц, также разработчики законопроекта считали, что информация, собираемая с менее чем тысячи сетевых адресов, не является большими данными.

С технической точки зрения большие данные определяются следующим образом: «Большие данные — это разнообразные данные, которые поступают с постоянно растущей скоростью и объем которых постоянно растет»[311]. Технологию bigdata характеризуют три ключевые свойства — разнообразие, высокая скорость поступления и большой объем, которые авторы законопроекта не учли. Кроме этого, существуют и другие технические определения: «Большие данные обычно определяют с точки зрения проблематики управления такими объёмами данных, которые не удается решить в рамках традиционных баз данных из-за объема, их разнообразия и требований к скорости. Существуют разные определения больших данных, но большинство из них базируется на концепции “трех V” больших данных. Объем (Volume): исчисляется в терабайтах и петабайтах. Разнообразие (Variety): данные поступают из самых разнообразных источников в различных форматах (это могут быть сетевые журналы, взаимодействие в социальных сетях, интернет-коммерция и транзакции в режиме онлайн или финансовые, и т.д.).

[310] См.: Законопроект № 571124-7 Статья 1, п.2. стр. 3 // Система обеспечения законодательной деятельности: [Электронный ресурс]. URL: https://sozd.duma.gov.ru/bill/571124-7 (дата обращения: 19.06.25).
[311] См.: Что такое Big Data — большие данные. // Сайт корпорации Oracle : [Электронный ресурс]. URL: https://www.oracle.com/ru/big-data/what-is-big-data/ (дата обращения: 20.06.25).

Скорость (Velocity): компании все чаще предъявляют очень строгие требования к тому, за какое время с момента возникновения данные должны превращаться в аналитические результаты, на основании которых пользователи могут принимать решения. Таким образом, необходимо обеспечить сбор, хранение, обработку и анализ данных за довольно короткое время: от одного дня вплоть до режима реального времени»[312]. Как видно из представленных определений, специалисты в области информационных технологий не проводят границу между персональными и «большими данными». Однако при рассмотрении определения, которое попытались дать юристы, у технических специалистов возникает недоумение, по причине того, что точное количество источников массива bigdata не является определяющим критерием, как, впрочем, и отсутствуют общепринятые нижние пороговые значения для этого. Источниками bigdata могут быть не только устройства, имеющие сетевые адреса, но и различные датчики, камеры видеонаблюдения, фитнес-браслеты, автомобили, и т.д. — что-то, что собирает какие-либо данные и передаёт их в какую-либо базу данных, но не всегда имеет привычный сетевой адрес. Следовательно, привязка правовой дефиниции к количеству сетевых адресов, да и в принципе к сетевым адресам, технически не верна. Так же в определении отсутствует такая важная характеристика, связанная с технологий bigdata, как получение новых знаний.

Среди положений законопроекта следует отметить создание единого федерального реестра «операторов больших данных»: «Федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке, установленном Правительством Российской Федерации, создается и ведется федеральная государственная информационная система “Реестр операторов больших пользовательских данных” (далее — реестр операторов больших пользовательских данных), устанавливается порядок

[312] См.: Определение больших данных. // Сайт корпорации Amazon : [Электронный ресурс]. URL: https://aws.amazon.com/ru/big-data/what-is-big-data/ (дата обращения: 20.06.25).

контроля и надзора за обработкой больших (пользовательских) данных»[313]. Проект предполагал обязательность информирования оператором пользователей о проведении сбора данных: «Оператор больших пользовательских данных до начала обработки больших пользовательских данных, за исключением случая, если в рамках такой обработки предполагается на безвозмездной основе или за плату передача больших пользовательских данных третьим лицам и (или) получение больших пользовательских данных у третьих лиц, и (или) иная обработка больших пользовательских данных для третьих лиц (далее — обработка больших пользовательских данных для целей третьих лиц), размещает на своем сайте в сети «Интернет» информационное сообщение, а при отсутствии такого сайта иным доступным способом информирует в электронной форме пользователя абонентского терминала (пользовательского оборудования) о своем намерении осуществлять такую обработку (далее — информационное сообщение)»[314]. Разработчики законопроекта вменяли в обязанность Операторов больших пользовательских данных информировать пользователя о сборе и обработке больших данных. Данная мера перекликается с необходимостью информировать субъекты персональных данных об условиях их обработки. Кроме этого, по аналогии со сбором персональных данных, авторы законопроекта предполагали, что оператор должен получить согласие на обработку данных от их владельца: «Оператор больших пользовательских данных до начала обработки больших пользовательских данных для целей третьих лиц обязан получить информированное согласие в электронной форме пользователя абонентского терминала (пользовательского оборудования) об идентификации сетевого адреса (далее — информированное согласие). Требования к информированному согласию и его форма устанавливаются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой

[313] См.: п.3 ст.1 Законопроект № 571124-7 // Система обеспечения законодательной деятельности : [Электронный ресурс]. URL: https://sozd.duma.gov.ru/bill/571124-7 (дата обращения: 22.06.25).
[314] См.: п.2 ст.1 Законопроект № 571124-7 // Система обеспечения законодательной деятельности : [Электронный ресурс]. URL: https://sozd.duma.gov.ru/bill/571124-7 (дата обращения: 22.06.25).

информации, массовых коммуникаций, информационных технологий и связи»[315]. С юридической точки зрения данная мера призвана сделать сбор и обработку больших данных добровольной, и исключить случаи, когда такие данные собираются без ведома и согласия владельца таких данных. Среди положений законопроекта следует отметить создание единого федерального реестра «операторов больших данных»: «Федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке, установленном Правительством Российской Федерации, создается и ведется федеральная государственная информационная система “Реестр операторов больших пользовательских данных” (далее — реестр операторов больших пользовательских данных), устанавливается порядок контроля и надзора за обработкой больших (пользовательских) данных»[316]. Данное положение было призвано упорядочить информацию об операторах больших данных по аналогии с операторами персональных данных.

С технической точки зрения, предложение регистрировать всех операторов больших данных выглядит весьма неоднозначно, по причине того, что количество таких операторов будет достаточно велико, и, к тому же, любое физическое лицо, имея в своём распоряжении достаточный объём дискового пространства, может организовать сбор больших данных для личных целей. И обнаружить такого «домашнего» оператора bigdata будет весьма сложно. А уж задача обязать всех операторов bigdata регистрироваться, представляется весьма непростой, местами фантастической. Итак, первый законопроект не был принят по вполне понятным причинам, связанным с низким качеством содержания законопроекта.

[315] См.: п.3. ст.1 Законопроект № 571124-7 // Система обеспечения законодательной деятельности : [Электронный ресурс]. URL: https://sozd.duma.gov.ru/bill/571124-7 (дата обращения: 22.06.25).
[316] См.: п.3. ст.1 Законопроект № 571124-7 // Система обеспечения законодательной деятельности : [Электронный ресурс]. URL: https://sozd.duma.gov.ru/bill/571124-7 (дата обращения: 22.06.25).

Несмотря на то, что законопроект был отклонён[317], некоторые идеи можно использовать в дальнейшем при разработке документов, регламентирующих использование технологии bigdata.

14 февраля 2020 года на портале правовой информации был опубликован текст законопроекта[318] о внесении изменений в законодательство. Авторы законопроекта постарались дать правовое определение понятию большие данные: «большие данные — совокупность неперсонифицированных данных, классифицирующая по групповым признакам, в том числе информационные и статистические сообщения, сведения о местоположении движимых и недвижимых объектов, количественные и качественные характеристики видов деятельности, поведенческие аспекты движимых и недвижимых объектов, полученных от различных владельцев данных либо из различных структурированных или неструктурированных источников данных, посредством сбора с использованием технологий, методов обработки данных, технических средств, обеспечивающих объединение указанной совокупности данных, ее повторное использование, систематическое обновление, форма представления которых не предполагает их отнесение к конкретному физическому лицу»[319]. Как видно из определения, авторы исходили из того, что bigdata это неперсонифицированная информация, однако они не рассматривали применение этой технологии исключительно в сети Интернет, и включили в это понятие множество различных признаков, в том числе и поведенческие аспекты. Изучая это определение, стоит отметить, что оно уже в большей степени соответствует техническому толкованию понятия «большие данные», однако данное определение слишком широкое, что влечёт за собой соответствие ему большой части общедоступной информации. Кроме этого,

[317] См.: Решение профильного комитета (Комитет Государственной Думы по информационной политике, информационным технологиям и связи). // Система обеспечения законодательной деятельности : [Электронный ресурс].. URL: https://sozd.duma.gov.ru/download/C9C4EF85-CACE-4956-8C21-FFDF8EFCE15D (дата обращения: 22.06.25).
[318] См.: Проект 04/13/02-20/00099581 «О внесении изменений в Федеральный закон Об информации, информационных технологиях и о защите информации». // Портал правовой информации : [Электронный ресурс].. URL: https://regulation.gov.ru/p/99581 (дата обращения: 22.06.25).
[319] См.: Проект 04/13/02-20/00099581 п.1 «О внесении изменений в Федеральный закон Об информации, информационных технологиях и о защите информации». // Портал правовой информации : [Электронный ресурс]. URL: https://regulation.gov.ru/p/99581 (дата обращения: 25.06.25)

участники Российской Ассоциации «Больших данных» считают, что положения законопроекта противоречат Конституции, в контексте нарушения свободы экономической деятельности и ограничения распространения информации. Также, в определении отсутствует такая важная составляющая технологии bigdata, как получение новых знаний[320]. Эта особенность анализа bigdata является одной из ключевых для этой технологии. Проведённый анализ определений больших данных показывает, что рассматриваемый аспект остаётся вне рамок существующих трактовок.

В законопроекте предлагалось установить: «1. Принципы, правовые основания, права и обязанности операторов больших данных, порядок и условия оборота обработки больших данных, а также контроль за обработкой и оборотом больших данных устанавливаются Правительством Российской Федерации. 2. Федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке, установленном Правительством Российской Федерации, создается и ведется реестр операторов больших данных, а также осуществляется контроль за обработкой и оборотом больших данных»[321]. Эти положения выглядели неоднозначно, потому что оператором больших данных может выступать любой, кто имеет техническую возможность сбора большого объёма информации и умеет обращаться с программным обеспечением, предназначенным для сбора, обработки и хранения bigdata. Таким образом, необходимость регистрации всех операторов больших данных является весьма спорной.

Определение обязанностей операторов bigdata, в отличие от документа 2018 года, в соответствии законопроектом изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации», отнесено к

[320] См.: Big Data: что это такое простыми словами — характеристики технологии больших данных и методы их обработки. // Cleverence : [Электронный ресурс]. URL: https://www.cleverence.ru/articles/auto-busines/big-data-chto-eto-takoe-prostymi-slovami-kharakteristiki-tekhnologii-bolshikh-dannykh-i-metody-ikh-o/ (дата обращения: 25.06.25)
[321] См.: Проект 04/13/02-20/00099581 п.2. «О внесении изменений в Федеральный закон Об информации, информационных технологиях и о защите информации». // Портал правовой информации : [Электронный ресурс]. URL: https://regulation.gov.ru/p/99581 (дата обращения: 27.06.25)

компетенции Правительства Российской Федерации. Такая норма позволяет в случае необходимости более гибко вносить изменения в нормы, регулирующие обязанности и права операторов больших данных, условия и порядок обработки массивов больших данных, не изменяя текст федерального закона, но при таком подходе существует риск того, что принятие нормативного акта Правительства Российской Федерации будет затянуто или не будет принято вовсе. В законопроекте была установлена необходимость организации федерального реестра операторов больших данных, что указывает на то, что законотворцы руководствовались, в том числе и принципами, на которых базируется регулирование персональных данных.

Сравнивая два законопроекта, можно прийти к выводу о том, что юристы иногда при разработке норм, которые призваны урегулировать общественные отношения, связанные с родственными, но разными понятиями, пытаются перенести принципы регулирования с одних отношений на другие. Юристы по-разному воспринимают одни и те же явления, что иллюстрируется определениями, которые дали авторы законопроектов. Остаётся открытым вопрос том, в каких случаях целесообразно использовать бланкетные нормы, а в каких такое использование повредит. Возможно, государственным органам следует вести учёт крупных операторов, которые применяют рассматриваемую технологию, собирающих значимый объём этих данных.

В марте 2020 года Правительство Российской Федерации отклонило законопроект. «Представитель Минкомсвязи не стал комментировать судьбу законопроекта. Он лишь сказал, что работа над совершенствованием законодательства в области больших данных продолжается»[322]. Однако, несмотря на это, часть подходов предложенных в документе, может быть использована в дальнейшем.

Необходимость нахождения общественных отношений, касающихся обработки bigdata, внутри правового поля связана с тем, что бесконтрольное

[322] См.: Правительство отклонило законопроект Минкомсвязи о больших данных». // Сайт газеты Ведомости : [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/articles/2020/03/27/826513-pravitelstvo-otklonilo-zakonoproekt (дата обращения: 27.06.25).

использование этой технологии может стать причиной нарушения тайны частной жизни (ст.ст. 23 и 24 Конституции Российской Федерации), которая будет защищена не в достаточной степени из-за того, что аналитика массивов bigdata нацелена на получение новых знаний, которые могу включать персональные данные физических лиц. Анализ огромных массивов информации может помочь в определении того, что женщина готовится стать матерью, и способствовать разглашению этой информации до того, как будущая мать захочет об этом кому-то рассказать[323]. Рассматриваемая технология может также применяться для комплексной оценки человека; вот что об этом пишут в юридической литературе: «Однако в реализуемой сегодня программе речь идёт не просто о системе оценки платёжеспособности заёмщика, а о создании индивидуального социального рейтинга китайского гражданина на основе объединения всех баз данных, содержащих какую-либо информацию о физических и юридических лицах, и их анализа с помощью технологий bigdata»[324]. Всё это в совокупности требует того, чтобы использование технологии bigdata регламентировалось нормами права, что положительным образом скажется на повышении защищённости конституционных прав граждан и защите их персональных данных.

В первую очередь, для достижения этой цели необходимо дать практически применяемое правовое определение рассматриваемой технологии. Ранее разбирались попытки со стороны законодателей дать такое определение. Ключевой особенностью bigdata является то, что, во-первых, их источником может быть не только сеть Интернет, но и огромное количество различных устройств и механизмов, которые собирают и хранят какие-либо данные. Ещё одной немаловажной деталью, связанной с пониманием сущности технологии bigdata, является то, что её использование может способствовать получению новых данных, в том числе персональных. Сами по себе массивы больших данных представляют из себя нагромождение не связанной, на первый взгляд, друг с другом информации.

[323] См.: Страшное лицо больших данных. // Сайт Лаборатории Касперского : [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/scary-big-data/8676/ (дата обращения: 27.06.25).
[324] См.: Шахрай С. М. Цифровая конституция. основные права и свободы личности в тотально информационном обществе. // Вестник Российской академии наук. — 2018. — Т. 88, № 12. — С. 1075–1082.

Правовое определение технологии больших данных могло бы выглядеть следующим образом: *большие данные* — совокупность массивов информации (которые характеризуются объемом, скоростью обработки, разнообразием и вариативностью данных), содержащих, как персональные, так и не персональные, данные физических лиц, обрабатывая которые, при помощи искусственного интеллекта (нейросетей), можно получить новую информацию, в том числе и персональные данные физических лиц.

Влияние применения технологии bigdata на сферу обработки персональных данных можно обозначить как достаточно весомое, особенно, в случае если их анализом занимается специальная нейросеть. Даже обезличенные массивы данных после их анализа в соответствии с определёнными алгоритмами могут предоставить новую информацию об индивидууме, относящуюся к его частной жизни. В связи с этим, для повышения качества защиты персональных данных, требуется урегулировать использование этой технологии нормами права, что особенно важно в условиях трансформации социальных отношений и их переходе на цифровые рельсы. Этот процесс имеет множество последствий, среди которых можно выделить накопление больших объёмов данных буквально обо всём; именно поэтому технология bigdata в национальном проекте «Цифровая экономика Российской Федерации» являлась, наряду с искусственным интеллектом — сквозной[325]. Это актуализирует задачу по разработке методов и способов её информационно-правового регулирования, что, в первую очередь, требует выработки правового толкования определения понятия «большие данные». Предложенное толкование этого понятия позволит выделить предмет правого регулирования, который связан с рассматриваемой технологией, что положительным образом скажется на эффективности правового регулирования жизненного цикла и защиты персональных данных.

[325] См.: Как трансформировались «сквозные технологии». // КоммерсантЪ : [Электронный ресурс]. URL: https://www.kommersant.ru/doc/5925906 (дата обращения: 27.06.25).

§ 3.3 Общественный контроль как элемент механизма правовой защиты персональных данных в Российской Федерации

Идея связи между гражданским обществом и государством является фундаментом на котором базируется демократическое государство. Она основывается на том, что государственные органы и должностные лица должны быть подотчётны и подконтрольны обществу, общественные объединения выполняют не только важную координирующую функцию[326], но и могут заниматься общественным контролем. Демократические государства, на практике реализующие доктрину правового государства, с особым вниманием относятся к соблюдению законодательства, регулирующего общественный контроль. Такое внимание к этому вопросу и его регулированию связано с тем, что данный институт представляет собой, в достаточной степени, не только действенный и эффективный механизм выявления злоупотреблений и коррупции со стороны государственных органов, но и со стороны негосударственных организаций. Поддержка и развитие гражданского общества и его институтов являются важной задачей государства, решение которой позволяет обеспечить социально-правовой характер государства.

В отечественной правовой науке проблематика, связанная с гражданским обществом и его институтами, рассматривалась в работах следующих исследователей: В. В. Гриба[327], С. М. Зубарева[328], В. Т. Кабышева[329], Г. Н. Комкова[330], Е. В. Бердниковой[331] и др.

---

[326] См.: Пешин Н. Л. Муниципальная власть: продолжение государства или институт самоорганизации общества / Вестник Воронежского государственного университета. Серия: Право. — 2019. — № 2(37). — С. 38–50

[327] См.: Гриб В. В. Общественный контроль: учебник; Московский государственный университет имени М.В. Ломоносова Высшая школа государственного аудита (факультет) Центр общественного контроля. — Москва: Издательская группа "Юрист", 2017. — 656 с. — ISBN 978-5-94103-417-8.

[328] См.: Зубарев С. М. Понятие и сущность общественного контроля за деятельностью государственных органов // Административное право и процесс. — 2011. — № 5. — С. 7–13., Зубарев С. М. Новые технологии общественного контроля: реальность или иллюзия? // Вестник Пермского университета. Юридические науки. 2019. № 1.

[329] См.: Кабышев В. Т. Народовластие в системе конституционного строя России: конституционно-политическое измерение // С Конституцией по жизни: Избранные научные труды. — М.: Формула права, 2013. — 320 с., Кабышев В. Т. Человек и власть: конституционные принципы взаимоотношений // С Конституцией по жизни: Избранные научные труды. — М.: Формула права, 2013. — 320 с.

[330] См.: Комкова Г. Н. Проблемы обеспечения равенства и справедливости на современном этапе конституционного развития России // Вестник Саратовской государственной юридической академии. — 2018. — № 2 (121), Комкова, Г. Н., Бердникова, Е. В. Содержание объекта и предмета общественного контроля в Российской Федерации: теоретико-правовые вопросы // Российское право: образование, практика, наука. — 2019. — № 4 (112).

[331] См.: Бердникова Е. В. Общественный контроль в конституционно-правовом взаимодействии публичной власти и институтов гражданского общества в Российской Федерации: специальность 12.00.02 "Конституционное право;

Характеристика Российской Федерации как правового государства закреплена в Конституции (п.1 ст.1), однако воплощение данной нормы на практике, вот уже более четверти века, сталкивается с рядом трудностей: высокие показатели коррупции[332], множественные злоупотребления должностных лиц[333] и др. Важным фактором, который влияет на преодоление коррупции, является соблюдение принципа законности государственными органами в своей деятельности и должностными лицами при исполнении своих обязанностей. Контрольная функция государства играет ведущую роль в борьбе с коррупцией и злоупотреблениями, однако её практического применения не всегда достаточно для эффективного решения проблемы злоупотреблений полномочиями должностных лиц. Ещё одним инструментом, позволяющим выстроить эффективный механизм борьбы, со злоупотреблениями властными и должностными полномочиями, является привлечение к решению этой проблемы неравнодушных граждан. Объединение таких активных членов общества в группы, должно всячески поддерживаться и стимулироваться государством, поскольку этот процесс позволяет наладить механизм сбора и передачи достоверной информации о различных нарушениях. Общественный контроль является тем информационным контуром, который при полноценном развёртывании не позволяет информации о злоупотреблениях затеряться на пути к адресату, в роли которого выступают соответствующие органы; особенно такой инструмент контроля важен в формирующемся информационном обществе, и в области защиты персональных данных. В своих работах отечественные исследователи характеризуют институт общественного контроля как одну из фундаментальных конструкций гражданского общества и правового государства[334]. Применение инструментария общественного контроля снижает вероятность «замыливания» информации о нарушении, и, что

конституционный судебный процесс; муниципальное право": диссертация на соискание ученой степени доктора юридических наук, 2022. — 482 с.

[332] См.: Сапожников А. Россия опустилась на 137-е место в рейтинге восприятия коррупции. // КоммерсантЪ : [Электронный ресурс]. URL: https://www.kommersant.ru/doc/5797806 (дата обращения: 5.07.25).

[333] См.: Злоупотребление должностными полномочиями — самые громкие приговоры 2023 года // Адвокат Саркисов : [Электронный ресурс]. URL: https://www.advokat-sarkisov.ru/blog/zloupotreblenie-dolzhnostnymi-polnomochiyami-samye-gromkie-prigovory-2023-goda.html (дата обращения: 5.06.25).

[334] См.: Гриб В. В. Роль и место общественных палат в системе общественного контроля в Российской Федерации // Конституционное и муниципальное право. — 2015. — № 5. — С. 33.

немаловажно, в некоторых случаях общественный контроль позволяет предупреждать нарушения за счёт своевременной фиксации фактов злоупотреблений.

В современном мире развитие информационных технологий стало всё чаще затрагивать права и свободы человека. Особенно новые технологии повлияли на сферу обработки персональных данных, и, как следствие, на конституционно закреплённое право человека на невмешательство в его частную жизнь. Среди всех современных технологий, которые оказали наиболее значительное воздействие на сферу персональных данных, можно выделить стремительно развивающиеся системы искусственного интеллекта и системы управления большими массивами данных (bigdata). Ю. М. Батурин замечает: «Широкое использование в практике организаций и компаний информационных технологий — от компьютерных баз данных до искусственного интеллекта (ИИ) увеличило риски нарушения прав. Мелкие, на первый взгляд, погрешности или неточная информация могут вызвать достаточно серьезные последствия для контрагентов, клиентов и пользователей. Многие могут оказаться затронуты, если алгоритмы выполняются, используя неточную информацию»[335]. Именно две эти технологии, работающие в связке друг с другом, оказывают существенное влияние на социальные отношения, связанные с обработкой персональных данных физических лиц.

Общественный контроль как институт, призван сделать работу государственных органов более прозрачной для общества, что положительно сказывается на степени вовлечённости граждан в деятельность государства; политолог Б. Пейдж говорил про доступность информации о деятельности государственных организаций для общества: «Для того, чтобы общество имело возможность реально контролировать действия правительства, оно должно быть в целом хорошо информированным, а граждане должны принимать активное участие в обсуждении всех важнейших проблем страны»[336]. Доступность информации является ключевым фактором для эффективной работы общественного контроля.

[335] См.: Батурин Ю. М. Аудит алгоритмов. // Вестник Московского университета. Серия 26. Государственный аудит. — 2024. — №4. — с.147.
[336] См.: Page B. Who deliberates? // Mass media in modern democracy. — Chicago, 1996. — P.5.

Впервые в истории на законодательном уровне обязательное предоставление официальных документов государственных органов по запросу, было установлено законом Швеции «О свободе изданий» (The Freedom of the Press Act)[337], принятом в 1766 году. Позднее, принцип открытости деятельности государственных органов перед гражданами, стал применяться и в других странах, например, в Конституции Финляндии, которая была принята в 1919 году, была закреплена норма о свободе информации[338]; позднее в 1951 году в Финляндии был принят закон «О гласности официальных документов»[339], который в дальнейшем несколько раз изменялся. Именно принятие этого документа стало отправной точкой для Финляндии в вопросе формирования института общественного контроля. В дальнейшем, в середине прошлого века, аналогичные документы были приняты и в других демократически развитых странах: в США закон «О свободе информации» (The Freedom of Information Act)[340] был принят в 1966 году, в Британии аналогичный нормативный акт[341] был принят в 2000 году. Несмотря на приверженность принципу открытости, доступ к некоторой информации о деятельности государственных органов в этих документах ограничен; к таким сведениям относится информация о деятельности разведывательных структур, национальной безопасности и др. Можно сделать вывод, что не вся информация о деятельности государственных органов может быть доступна для общественного контроля.

Обратим внимание, в том числе и на Соединённые Штаты Америки, где контроль со стороны общества является одним из важных элементов поддержания эффективной работы государства и негосударственных организаций. В США с 1992 года действует общественная организация «Privacy Rights Clearinghouse»,

---

[337]См.: The Freedom of the Press Act. // Campaign for Tobacco-Free Kids: [Электронный ресурс]. URL: https://assets.tobaccocontrollaws.org/uploads/legislation/Sweden/Sweden-Freedom-of-Press-Act.pdf (дата обращения: 5.07.25) (пер.: Яндекс-переводчик).

[338] См.: Finland Constitution 1919. // International Constitutional Law (ICL) : [Электронный ресурс]. URL: https://www.servat.unibe.ch/icl/fi01000_.html (дата обращения: 5.07.25) (пер.: Яндекс-переводчик).

[339] См.: Act on the Publicity of Official Documents. // Finlex: [Электронный ресурс]. URL: https://www.finlex.fi/fi/laki/smur/1951/19510650 (дата обращения: 5.07.25) (пер.: Яндекс-переводчик).

[340] См.: The Freedom of Information Act. // U.S. Department of Justice: [Электронный ресурс]. URL: https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/foia-final.pdf (дата обращения: 5.07.25).

[341] См.: Freedom of Information Act 2000. // Legislation.gov.uk : [Электронный ресурс]. URL: https://www.legislation.gov.uk/ukpga/2000/36/contents (дата обращения: 5.07.25).

деятельность которой сфокусирована на защите конфиденциальности потребителей.

Ещё одним, не менее интересным, зарубежным опытом представляется то, как подошли к решению задачи общественного контроля в Польше. С 2003 года в Польше действует гражданская сеть «Watchdog Poland»[342]. Это организация объединяет неравнодушных граждан, которые хотят участвовать в общественном контроле; чаще всего такими гражданами оказываются представители средств массовой информации или блогеры.

Активисты гражданской сети «Watchdog Poland» проводят мониторинг деятельности различных органов власти или конкретных организаций, в тех сферах, которые их интересуют. В ситуации, когда член сети обнаруживает нарушение, у него есть ряд способов эскалации выявленной проблемы, которые можно разделить на следующие группы: юридические, общественные и политические. К юридическим относятся подготовка и передача материалов в надзорные органы или же в суд, общественные представляют собой различные формы массовых мероприятий, такие как: митинги, шествия, демонстрации или раздача листовок и иных информационных материалов, или публикация информации в сети Интернет. К политическим методам, которые находятся в распоряжении активистов можно отнести организацию конференций, симпозиумов, встреч, а также проведение экспертизы законопроектов. Поскольку активисты гражданской сети являются экспертами в одной или нескольких областях, их часто приглашают на различные мероприятия, которые организуют те или иные государственные органы; например, парламент привлекает членов организации к публичным слушаниям, или для работы в парламентских комиссиях. Кроме этого, экспертов из гражданской сети периодически привлекают министерства Польши. Помимо активистов в «Watchdog Poland» состоят и те, кого можно назвать информаторами. Это граждане, которые работают в различных государственных организациях, и, когда они в ходе своей работы сталкиваются со

[342] См.: Watchdog Poland. // Citizens Network Watchdog Poland : [Электронный ресурс]. URL: https://siecobywatelska.pl/?lang=en (дата обращения: 6.07.25).

злоупотреблениями, то сообщают об этом в «Watchdog Poland». Выстроенная таким образом система общественного контроля позволяет осуществлять мониторинг деятельности предприятий и организаций не только снаружи, но и, с помощью сознательных граждан, изнутри; всё это делает деятельность государственных органов в достаточной степени прозрачной для общественного контроля.

Рассматривая становление гражданского общества и общественного контроля в России, нужно учитывать всё богатство истории нашей великой страны, и соответственно рассмотрение только периода после 1991 года, не является методологически верным. История становления института общественного контроля в России насчитывает не одно десятилетие, и начинает своё существование с появления в Российской Империи в 1819 году «Попечительного общества тюрем». Задачей этой организации была работа над улучшением быта и содержания заключённых. В дальнейшем либерализация политической ситуации привела к тому, что в результате реформ 1860–1870 годов в Российской Империи появились Земские учреждения, которые стали прообразом общественных объединений гражданского общества, решавших задачу по участию представителей общественности в решении некоторых вопросов государственного управления. Таким образом, в Российской Империи имелись зачатки гражданского общества, которые не получили дальнейшего развития из-за революции 1917 года.

Крах государства и революция 1917 года привели к тектоническим изменениям во всех сферах; изменение общественно-политической формации стало причиной ликвидации не только государственных, но и общественных институтов. Новой власти пришлось выстраивать их практически с нуля, а учитывая её ярко выраженный внеклассовый характер, приходилось создавать совсем другие механизмы. В 1917 году было принято положение ВЦИК о рабочем контроле[343]. Одним из ключевых норм принятого документа была норма о выборном формировании контрольных учреждений. В дальнейшем «рабочий контроль» стал приобретать характер государственного, и к 1918 году с принятием

[343] См.: Положеніе о рабочемъ контроле. // "СУ РСФСР", 1917, № 3, ст. 35.

Конституции РСФСР, окончательно трансформировался в государственный, с образованием Народного комиссариата государственного контроля РСФСР. И только в 1965 году был принят «Закон об органах народного контроля в СССР», который утвердил переход от партийно-государственного контроля к формам народного участия в контрольных функциях, возложенный на Комитет народного контроля СССР, после принятия Конституции СССР 1977 года[344], с появлением в 1978 году Закона СССР № 1158-X «О народном контроле в СССР»[345], институт общественного контроля обрёл законную основу. Последним этапом существования общественного контроля советского периода можно считать период с 1990 по 1991 гг. На этом этапе органы народного контроля РСФРС были упразднены[346].

В постсоветский период, когда страна встала на путь демократического развития, идея формирования гражданского общества и его институтов стала особенно актуальной и значимой для эффективной работы государства. Общественный контроль, будучи одним из элементов гражданского общества, решает важную задачу ретранслятора информации от общества к государству в тех ситуациях, когда прохождение сведений о злоупотреблениях и нарушениях к конечному адресату затруднено, или они искажаются. Первый Президент Российской Федерации Б. Н. Ельцин учредил[347] Общественную палату в рамках Конституционного совещания в 1993 году. Позднее, после принятия Конституции Российской Федерации, данный орган был трансформирован[348] в Общественную палату при Президенте Российской Федерации. Главной задачей этой общественной организации стало предоставление экспертной оценки деятельности государственных органов, выработка предложений и рекомендаций по совершенствованию законодательства. Позднее Общественная палата

[344] См.: Конституция (Основной Закон) Союза Советских Социалистических Республик (принята ВС СССР .07.10.1977) // "Ведомости ВС СССР", 1977, № 41, ст. 617.
[345] См.: О народном контроле в СССР // Ведомости ВС СССР, 1979, № 49, ст. 840..
[346] См.: Ведомости СНД РСФСР и ВС РСФСР, 1990, № 3, ст. 28.
[347] См.: Об образовании Общественной палаты Конституционного совещания. // "Собрание актов Президента и Правительства РФ", 27.09.1993, № 39, ст. 3674.
[348] См.: Распоряжение Президента РФ от 16.02.1994 № 78-рп "Об Общественной палате при Президенте Российской Федерации". // "Собрание актов Президента и Правительства РФ", 21.02.1994, № 8, ст. 592.

преобразовывается[349] в Политический консультативный совет. Однако в 2000 году данный орган был упразднён[350]. В дальнейшем тема развития и становления гражданского общества всё сильнее актуализировалась, и всё чаще оказывалась в фокусе внимания руководства Российской Федерации; так в Послании Федеральному собранию Российской Федерации в 2004 году, Президент обозначил развитие гражданского общества как одну из важнейших целей для России: «Наши цели абсолютно ясны. Это высокий уровень жизни в стране, жизни безопасной, свободной и комфортной. Это — зрелая демократия и развитое гражданское общество»[351]. Позднее данный приоритет получил своё воплощение в сформулированном на расширенном заседании Правительства тезисе Президента Российской Федерации о необходимости привлечения общества к решению тех или иных задач «…считаю продуманной идею образования общественной палаты как площадки для широкого диалога, где могли бы быть представлены и подробно обсуждены гражданские инициативы, и, что не менее важно, такая палата должна стать местом проведения общественной экспертизы тех ключевых государственных решений и прежде всего законопроектов, которые касаются перспектив развития всей страны, которые имеют общенациональное значение»[352]. Данная инициатива руководства воплотилась в Федеральном законе № 32-ФЗ «Об Общественной палате Российской Федерации»[353] от 04.04.2005 г. Данный документ заложил правовую основу для развития института общественного контроля в нашей стране. Закон закрепил цели и задачи данного органа, этический кодекс членов Общественной Палаты, порядок её формирования, состав Палаты и многое другое.

---

[349] См.: Указ Президента РФ от 25.06.1996 № 989 "О Политическом консультативном совете". // Собрание законодательства РФ, 01.07.1996, № 27, ст. 3232.
[350] См.: Указ Президента РФ от 08.08.2000 № 1461 "О Политическом консультативном совете. // Собрание законодательства РФ, 14.08.2000, № 33, ст. 3351.
[351] См.: Послание Федеральному Собранию Российской Федерации. 26 мая 2004 года // Президент России : [Электронный ресурс]. URL: http://archive.kremlin.ru/text/appears/2004/05/71501.shtml (дата обращения: 6.07.25).
[352] См.: Вступительное слово на расширенном заседании Правительства с участием глав субъектов Российской Федерации. // Президент России: [Электронный ресурс]. URL: http://www.kremlin.ru/events/president/transcripts/22592 (дата обращения: 6.07.25).
[353] См.: Федеральный закон от 04.04.2005 № 32-ФЗ (ред. от 13.06.2023) "Об Общественной палате Российской Федерации". // Собрание законодательства РФ, 11.04.2005, № 15, ст. 1277.

В дальнейшем приоритет развития институтов гражданского общества был закреплён и на стратегическом уровне[354], в «Стратегии государственной национальной политики Российской Федерации на период до 2025 года». Анализируемый документ, среди прочих аспектов, выделяет общественный контроль в качестве ключевого механизма обеспечения прозрачности и эффективности национальной политики.

Дальнейшее развитие нормативно-правовой базы общественного контроля привело к необходимости установления на правовом уровне общих подходов к общественному контролю России. Это привело к принятию в 2014 году Федерального закона от 21.07.2014 № 212-ФЗ «Об основах общественного контроля в Российской Федерации», где было дано определение понятия «общественный контроль»: «Под общественным контролем в настоящем Федеральном законе понимается деятельность субъектов общественного контроля, осуществляемая в целях наблюдения за деятельностью органов государственной власти, органов местного самоуправления, государственных и муниципальных организаций, иных органов и организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, а также в целях общественной проверки, анализа и общественной оценки издаваемых ими актов и принимаемых решений»[355]. Таким образом, впервые в истории современной России в правовом поле появилось определение понятия «общественный контроль». Положения рассматриваемого закона охватывают цели, задачи, принципы деятельности, правовой статус и компетенцию субъектов общественного контроля (включая их права и обязанности). В рамках закона осуществлено нормативно-правовое оформление правового режима общественных наблюдательных комиссий и инспекций, а также объединений типа ассоциаций и союзов. Важным элементом общественного контроля, который нормативно закрепил документ, являются общественные (публичные) слушания. Одним из

[354] См.: Указ Президента РФ от 19.12.2012 № 1666 (ред. от 15.01.2024) "О Стратегии государственной национальной политики Российской Федерации на период до 2025 года" // Собрание законодательства РФ, 24.12.2012, № 52, ст. 7477.
[355] См.: п.1 ст. 4, Федеральный закон от 21.07.2014 № 212-ФЗ "Об основах общественного контроля в Российской Федерации" // Собрание законодательства РФ, 28.07.2014, № 30 (Часть I), ст. 4213.

важнейших положений рассматриваемого документа является закрепление ответственности за нарушение законодательства в сфере общественного контроля. Важность этих норм связана с тем, что процесс формирования института общественного контроля ещё продолжается, и общественные активисты и их объединения могут сталкиваться с препятствованием своей деятельности по ряду причин: непонимание, и, в отдельных случаях, нежелание понимать роль института общественного контроля в государственном управлении, смещение приоритета на собственное обогащение некоторых должностных лиц, и, как следствие, желание воспрепятствовать общественным контролёрам в выявлении таких случаев. Следовательно, наличие норм, связанных с ответственностью за нарушения в сфере общественного контроля, является важным инструментом в повышении эффективности работы данного, чрезвычайно важного для государственного управления, института.

Например, подходы к общественному контролю в пенитенциарной сфере, которые были заложены в Российской Империи (о которых писалось выше), нашли своё продолжение в статье 23 Уголовно-исполнительного кодекса Российской Федерации[356] и Федеральном законе от 10.06.2008 № 76-ФЗ «Об общественном контроле за обеспечением прав человека в местах принудительного содержания и о содействии лицам, находящимся в местах принудительного содержания»: «Созданные в 21 веке Общественные наблюдательные комиссии и общественные советы при ФСИН и его территориальных органах являются уже, по меньшей мере, 5-м поколением институтов общественного контроля за тюремной системой»[357]. Общественный контроль за исправительными учреждениями, учитывая важность для общества этой области, позволяет бороться с нарушением законодательства и прав человека в этой сложной и неоднозначной сфере, и помогает уменьшить воспроизводство антисоциальных элементов среди граждан, отбывающих наказания за свои преступления в исправительных учреждениях. В регламентации

[356] См.: Уголовно-исполнительный кодекс Российской Федерации от 08.01.1997 № 1-ФЗ. // Собрание законодательства РФ, 13.01.1997, № 2, ст. 198.
[357] См.: 199 лет общественному контролю за тюрьмами: история, проблемы, перспективы. // Блог Андрея Бабушкина: [Электронный ресурс]. URL: https://an-babushkin.livejournal.com/830553.html (дата обращения: 6.07.25).

работы наблюдательных комиссий можно выделить то, что посещение мест принудительного ограничения свободы общественными комиссиями является уведомительным, а также то, что они обладают достаточно широкими правами ознакомления с необходимой им информацией. «Члены общественной наблюдательной комиссии при осуществлении общественного контроля вправе посещать места принудительного содержания в уведомительном, а не разрешительном порядке, беседовать с содержащимися там лицами, принимать и рассматривать их жалобы, запрашивать у администраций мест принудительного содержания и получать от них сведения и документы, необходимые для проведения общественного контроля и подготовки заключений, предложений или обращений общественной наблюдательной комиссии, обращаться к соответствующим должностным лицам»[358]. Руководство страны, понимая важность для государства и общества такого важного инструмента как общественный контроль пенитенциарной системы, старается всячески поддерживать общественные организации в этой области. «С каждым годом возрастает роль НКО и различных фондов, у которых накоплен опыт ресоциализации и адаптации заключенных. Преуспела в этой сфере региональная общественная организация Правовой центр “Право на защиту”, проект которой поддержан Фондом президентских грантов»[359]. Таким образом, можно констатировать признание на высшем уровне важности института общественного контроля. Эта оценка результатов работы говорит о том, что выстроенный нормативно-правовой контур мониторинга общественными организациями пенитенциарной системы достаточно высок и заслуживает внимания как возможный объект рецепции модели правового регулирования общественного контроля в других сферах, например в сфере контроля за применением технологии искусственного интеллекта и bigdata.

[358] См.: Общественный контроль за работой органов и учреждений уголовно-исполнительной системы со стороны гражданского общества. // Прокуратура Владимирской области: [Электронный ресурс]. URL: https://epp.genproc.gov.ru/ru/web/proc_33/activity/legal-education/explain?item=23019822 (дата обращения: 6.07.25).
[359] См.: Общественный контроль в тюрьмах: реальность и перспективы. // Общественная палата Российской Федерации: [Электронный ресурс]. URL: https://www.oprf.ru/news/obshchestvennyy-kontrol-v-tyurmakh-realnost-i-perspektivy (дата обращения: 6.07.25).

В современных условиях становления информационного общества государству потребовалось актуализировать законодательство во многих областях, в том числе и в сфере обработки и защиты персональных данных. Нагрузка на государственные органы, занимающиеся контролем над соблюдением требований законодательства о защите персональных данных, постоянно увеличивается. Помимо государственных механизмов контроля, существуют и иные институциональные инструменты обеспечения соблюдения правового режима персональных данных. Ещё одной стороной, заинтересованной в том, чтобы правила обработки информации о физических лицах неукоснительно соблюдались, является общество. В демократически развитых странах активную роль в контроле над соблюдением законодательства в различных сферах жизни играет именно общество. Общественный контроль является тем инструментом, который позволяет повысить эффективность государственного управления за счёт повышения прозрачности работы не только государственных, но и частных организаций. Особенно актуально привлечение общественности к соблюдению законодательства в сфере защиты персональных данных, в связи с тем, что в 2022 году количество утечек персональных данных выросло в 40 раз[360], за следующий 2023 год аналогичный рост составил 60%[361], и, наконец, за 2024 год рост утечек продемонстрировал новый рекорд, превысив показатели предыдущего года на 70%[362]. Очевидно, что система правовой защиты персональных данных требует совершенствования, и общественный контроль операторов персональных данных может стать одним из механизмов, который повысит эффективность всей системы защиты личной информации о физических лицах.

[360] См.: Объём утечек персональных данных россиян в 2022 году вырос в 40 раз по отношению к 2021 году, демонстрирует отчёт компании Group-IB. // Хабр: [Электронный ресурс]. URL: https://habr.com/ru/news/712488/ (дата обращения: 6.07.25).
[361] См.: Объем слитых персональных данных в РФ вырос на 60 процентов. // INFOWATCH: [Электронный ресурс]. URL: https://www.infowatch.ru/company/presscenter/news/obyem-slitykh-personalnykh-dannykh-v-rf-vyros-na-shestdesyat-protsentov (дата обращения: 6.07.25).
[362] См.: Арялина М. Объем утекших в сеть данных россиян вырос на 70% за год. // Ведомости: [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/articles/2025/01/24/1088050-obem-utekshih-v-set-dannih-rossiyan-viros (дата обращения: 6.07.25).

В условиях набирающей скорость и масштабы цифровизации социальных отношений и того, что некоторые современные технологии стали оказывать на сферу защиты персональных данных значительное влияние, возникла необходимость привлекать к контролю над этой сферой и общество. Например, в Нидерландах пошли именно по этому пути, государственный регулятор решил «привлечь добровольных помощников из независимых специалистов, которых достаточно среди населения»[363] к работе по проверке информационных систем использующих нейросети. Как было доказано ранее, применение ИИ-систем, а также использование технологии bigdata для обработки и хранения больших объёмов информации, в том числе и информации о физических лицах, стали теми факторами, которые начали оказывать влияние не только на права физических лиц, но и затрагивать общество в целом. В последнее время множество операторов персональных данных стали полагаться в своей деятельности на нейросети для решения задач, связанных с анализом имеющейся у них информации о физических лицах. Ключевой проблемой, связанной с использованием этих технологий, является, то, что их задействование непрозрачно для субъекта персональных данных, а также контроль со стороны государства в этой области ещё находится на стадии становления. Учитывая масштабное воздействие нейросетей и технологии bigdata на личность и социум, применение инструментов общественного контроля в системе защиты персональных данных позволит обеспечить надлежащее соблюдение права граждан на защиту персональных данных.

Поскольку ИИ-системы используются во многих случаях именно для аналитики больших массивов информации, эти две технологии следует рассматривать в комплексе; и, учитывая то, что регулирование общественных отношений, связанных с системами искусственного интеллекта требует принятия отдельных нормативных актов[364], которые учитывают особенности этих отношений, то общественный контроль в сфере применения технологии

[363] См.: Батурин Ю. М. Аудит алгоритмов. // Вестник Московского университета. Серия 26. Государственный аудит. — 2024.— №4 — С.152.
[364] См.: Метёлкин П. Правовое регулирование искусственного интеллекта. // Журнал "Системы безопасности" : [Электронный ресурс]. URL: https://www.secuteck.ru/articles/pravovoe-regulirovanie-iskusstvennogo-intellekta (дата обращения: 6.07.25).

нейросетей при обработке ими персональных данных должен опираться на эти особенности. Анализ функционирования ИИ-алгоритмов показывает, что их выходные данные могут содержать ранее не зафиксированную информацию о физическом лице, полученную в результате обработки нейросетями. Такая информация не всегда нейтральна: она может содержать личные данные особого типа или касаться частной жизни, которая защищена законом. В результате появляются потенциальные угрозы нарушения прав человека. Кроме этого, сбор и хранение больших массивов данных также требуют контроля, по причине того, что эта информация может использоваться как для обучения ИИ-систем, которые применяет оператор персональных данных, так и представлять коммерческий интерес для иных разработчиков нейросетевых моделей. Эта проблема поднимается в юридической литературе: «Удобство использования онлайн-сервисов стоит в одном ряду с нарушением прав субъектов персональных данных. Становится в значительной степени сложнее сохранить приватность в Интернете»[365]. Предлагается распространить общественный контроль на деятельность организаций, использующих технологии ИИ-систем и bigdata. Это позволит выявлять случаи нарушения прав человека и законодательства в сфере обработки персональных данных при применении нейросетей и технологии bigdata, и готовить обращения по таким фактам в соответствующие государственные органы. Именно своевременное выявление нарушений и возможность оперативно осуществлять проверку жалоб на ущемление прав является тем фактором, который и определяет необходимость в разработке правовых подходов к общественному контролю в рассматриваемой области.

Ниже предлагается модель общественного контроля за использованием нейросетей и технологии bigdata при обработке персональных данных. Следует начать с формулирования принципов общественного контроля в рассматриваемой области:

[365] См.: Кто что знает обо мне: обработка персональных данных онлайн-платформами. // портал Гарант.ру : [Электронный ресурс]. URL: https://www.garant.ru/news/1446555/ (дата обращения: 6.07.25).

1. Осуществление общественного контроля в области применения нейросетей (ИИ-систем) на основе принципов приоритета прав человека, добровольности, равноправия, объективности и законности;
2. Самостоятельность в осуществлении деятельности Общественных наблюдательных комиссий по общественному контролю от органов государственной власти, органов местного самоуправления, государственных и муниципальных организаций, иных органов и организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия. Недопустимость вмешательства политических партий, международных и иностранных организаций (объединений) в сферу деятельности общественных наблюдательных комиссий;
3. Публичный и открытый характер осуществления общественного контроля, а также обсуждения его итогов;
4. Недопустимость оказания неправомерного воздействия со стороны субъектов общественного контроля на деятельность проверяемых организации;

Субъектами, осуществляющими контроль в области применения технологий bigdata и ИИ-систем, могут являться общественные наблюдательные комиссии и члены таких комиссий. Важным аспектом деятельности таких комиссий является информационное обеспечение их работы, поскольку возможность граждан сообщить в комиссию о возможном нарушении в рассматриваемой области, позволяет адресно реагировать на эти обращения и силами наблюдательных комиссий и отдельных членов, проводить верификацию поступивших заявлений, и, в случае подтверждения, передавать материалы проверок в соответствующие государственные органы.

Основной целью работы таких общественных наблюдательных комиссий является обеспечение конституционных прав человека в области обработки персональных данных при помощи нейросетей и при применении технологии bigdata.

Среди задач, которые должен решать общественный контроль, можно выделить следующие: осуществление общественного контроля над обеспечением

прав человека при обработке персональных данных ИИ-системами и\или с использованием технологии bigdata на территории субъекта Российской Федерации, в котором образована общественная наблюдательная комиссия; подготовка решений в форме заключений, предложений и обращений (далее — решения) по результатам проведения общественного контроля; создание условий для коммуникации организаций общественного контроля с операторами обработки персональных данных и органами публичной власти, уполномоченными обеспечивать законные права и свободы в сфере защиты персональных данных.

Состав общественных наблюдательных комиссий (по субъектам Российской Федерации), может устанавливаться Советом Общественной Палаты Российской Федерации для каждого конкретного субъекта Российской Федерации.

Важным аспектом работы общественных наблюдательных комиссий является этическая составляющая. В связи с этим в своей работе члены таких комиссий должны руководствоваться Кодексом этики, который бы утверждался Общественной палатой Российской Федерации по представлению совета Общественной палаты.

Также, следует обратить внимание на то, каким должен быть регламент работы общественных наблюдательных комиссий. Данный документ, в соответствии с которым и осуществляет свою деятельность наблюдательная комиссия, должен утверждаться на первом её заседании. Утверждение осуществляется большинством голосов её членов. Регламент должен устанавливать, определять: проведение заседаний общественной наблюдательной комиссии, их правомочность и периодичность, принятие и оформление решений общественной наблюдательной комиссии, подготовку и рассмотрение вопросов на заседании общественной наблюдательной комиссии, и осуществление иных форм деятельности общественной наблюдательной комиссии.

Организационное и ресурсное обеспечение общественных наблюдательных комиссий является важной стороной их функционирования. Финансирование расходов, обусловленных реализацией полномочий членов комиссий, должно осуществляться за счёт средств Общественной палаты Российской Федерации,

которая также обязана обеспечивать материально-техническую и информационную поддержку. Помимо этого, целесообразно закрепить на нормативном уровне возможность оказания государственными органами комплексной поддержки общественным наблюдательным комиссиям, включая информационную, консультационную и иные формы содействия. Соответственно, следует учесть и закрепить нормативно, иные законные способы поддержки общественных наблюдательных комиссий.

Следует обратить внимание на регламентацию процедуры наделения статусом члена общественной наблюдательной комиссии физического лица. Этим статусом может быть наделено лицо, имеющее гражданство Российской Федерации, и не имеющее гражданства (подданства) иностранного государства, либо лицо, имеющее вид на жительство или иной документ, подтверждающий право на постоянное проживание гражданина Российской Федерации на территории иностранного государства, достигшее возраста 25 лет, и имеющее опыт в области защиты прав граждан. Деятельность членов общественной наблюдательной комиссии осуществляется на общественных началах. Институт членства в общественной комиссии предусматривает ограничение в три последовательных срока. В соответствии с действующими нормами, к участию в деятельности общественных наблюдательных комиссий не допускаются лица, состоящие на государственной или муниципальной службе, а также осуществляющие адвокатскую деятельность.

Для обеспечения эффективности общественного контроля необходимо при регламентации деятельности Комиссий (контексте использования ИИ-систем и bigdata при обработке персональных данных) выделить и обосновать наиболее значимые формы их практической реализации:

— проведение инспекционных мероприятий на местах в отношении объектов инфраструктуры операторов персональных данных, использующих ИИ-системы и технологии bigdata для обработки персональных данных;

— осуществление рассмотрения поступающих от граждан предложений, заявлений и жалоб, указывающих на нарушения законодательства в области

обработки персональных данных с применением ИИ-систем и bigdata, наряду с организацией и проведением публичных слушаний и общественных обсуждений по вопросам собственной деятельности;

— после завершения мероприятий общественного контроля формируются решения, а документация с итогами направляется в установленном порядке в Общественную палату РФ, Уполномоченному по правам человека, операторам персональных данных и регулирующим органам;

— взаимодействие по вопросам, относящимся к деятельности Комиссии с органами государственной власти Российской Федерации, государственными органами, не являющимися органами государственной власти, органами местного самоуправления и их должностными лицами, Уполномоченным по правам человека в Российской Федерации, Уполномоченным при Президенте Российской Федерации по правам ребенка, Уполномоченным при Президенте Российской Федерации по защите прав предпринимателей, Уполномоченным по правам человека в субъектах Российской Федерации, Уполномоченными по правам ребенка в субъектах Российской Федерации, Уполномоченными по защите прав предпринимателей в субъектах Российской Федерации, Общественной палатой Российской Федерации, Общественными палатами субъектов Российской Федерации, организациями, средствами массовой информации, общественными наблюдательными комиссиями, образованными в других субъектах Российской Федерации и иными субъектами, должно быть разрешено проводить ей по своему усмотрению;

— в рамках достижения своих целей общественные наблюдательные комиссии могут участвовать в иных видах деятельности при условии их соответствия законодательству Российской Федерации.

Представляется целесообразным отдельно рассмотреть права членов общественных наблюдательных комиссий, задействованных в осуществлении общественного контроля. Минимально допустимый состав проверяющей группы целесообразно определить в три человека. Их члены должны иметь право:

— проводить ознакомление с технической, технологической и иной документацией, относящейся к информационным системам, которые обрабатывают персональные данные с применением нейросетей и используют технологию bigdata;

— лица, входящие в состав общественной наблюдательной комиссии должны иметь право запрашивать у администрации организации, где проводится проверка, в установленном законодательством Российской Федерации порядке, документы и сведения, необходимые для проведения общественного контроля и подготовки заключений, предложений и т.д.

— члены общественных наблюдательных комиссий при посещении организации, обрабатывающей персональные данные с применением нейросетей и bigdata, должны иметь право привлекать сторонних экспертов по необходимым направлениям для оценки деятельности оператора персональных данных на соответствие законодательству Российской Федерации в сфере обработки персональных данных и соблюдению прав человека.

— индивиды, включённые в состав общественной наблюдательной комиссии при осуществлении своих полномочий должны быть обязаны соблюдать положения нормативных правовых актов, которые регулируют работу посещаемой организации, соблюдать правила внутреннего распорядка и подчиняться законным требованиям руководства посещаемой организации, кроме этого, деятельность общественной наблюдательной комиссии не должна нарушать и/или чинить препятствия повседневной деятельности инспектируемой организации.

— члены общественной наблюдательной комиссии должны иметь право вести кино-, фото-, видео- и аудиозапись работы комиссии в проверяемой организации.

— член общественной наблюдательной комиссии не должен быть вправе осуществлять общественный контроль в организации, где работает его близкий родственник.

— член общественной комиссии не должен быть вправе получать материальное вознаграждение за свою деятельность по осуществлению общественного контроля.

Ключевым функциональным элементом механизма общественного контроля является система информационного обеспечения общественных наблюдательных комиссий — это в значительной степени работа с данными и информацией, начиная с поиска и получения информации, и заканчивая её анализом и доведением до заинтересованных лиц. Одним из ключевых вопросов, связанных с обеспечением информационной деятельности по общественному контролю, является своевременное получение наблюдательными комиссиями данных о нарушении прав граждан. В современном мире развитие информационно-коммуникационных технологий позволило в значительной степени повысить эффективность коммуникации между людьми за счёт электронных средств обмена информацией (электронная почта, формы обратной связи на сайте), однако в последние годы, с распространением смартфонов, особую роль стали играть тематические мобильные приложения. Применение цифровых технологий позволяет повысить эффективность методов, способов и приёмов проведения общественного контроля. Эти процессы характеризуются не только повышением скорости информационного обмена между субъектом и объектом контроля, но и автоматизацией некоторых этапов получения информации субъектом об объекте контроля. Применение данных технологий на каждом этапе общественного контроля может определяться его формами и методами. Например, для получения информации от граждан можно использовать не только специализированный веб-портал, но и приложение для мобильных устройств. Такой подход позволит собирать информацию о недобросовестных операторах персональных данных, которые нарушают права граждан при обработке их с помощью ИИ-систем и технологии bigdata. Цифровой сервис по сбору и обработке этих данных позволит адресно, т.е., имея сведения о возможных нарушениях со стороны организации, выбирать объект для проведения проверки, что в значительной степени повысит эффективность работы общественных наблюдательных комиссий.

Институт общественного контроля является важным и эффективным средством контроля общества над той или иной сферой хозяйственной деятельности, не только государственных органов, но и частных компаний. В условиях требований цифровой эры и проникновения новых технологий во все сферы общественной жизни, влияние применения ИИ-систем и bigdata на права и свободы личности не вызывает сомнений. В современном демократическом обществе система правовой защиты персональных данных должна включать не только работу государственных органов, но и привлечение гражданского общества к контролю применения новых технологий. Именно к ним относятся технологии bigdata и нейросетей, используемые для обработки персональных данных; общественный контроль в рассматриваемой области позволит повысить качество защиты прав и свобод человека. Кроме этого, такой подход будет способствовать вовлечению общества в процесс управления государством, и в процесс формирования предложений и рекомендаций по внесению изменений в законодательство в сфере правовой защиты персональных данных при применении современных технологий. Результаты анализа позволяют сделать вывод о целесообразности включения институтов общественного контроля в архитектуру правового регулирования обработки персональных данных в Российской Федерации.

Требуется выработка правовых подходов к вопросу применения общественного контроля в сфере обработки персональных данных при помощи нейросетей и\или технологии bigdata, для чего может быть использована описанная выше модель.

ЗАКЛЮЧЕНИЕ

В основе института защиты персональных данных лежит право на неприкосновенность частной жизни, сильное влияние на которую оказало стремительное развитие и распространение информационных технологий. Возникла необходимость в выработке новых правовых подходов к защите информации о частной жизни человека. Потребовалось ввести в оборот категорию, на которую бы опиралось правовое регулирование работы с данными, относящимися к конкретному человеку. В результате сформировалось правовое понятие: «персональные данные».

Принятие Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» стало результатом выделения неприкосновенности частной жизни как самостоятельной ценности в отечественной юридической науке и появления соответствующих прав человека. Важной особенностью этого нормативно-правового акта стала его ориентация на ручную или слабо автоматизированную обработку персональных данных. Существующие проблемы в сфере защиты персональных данных сохраняют актуальность, несмотря на законодательное регулирование данного вопроса. Эволюция института персональных данных обусловила регламентацию социальных взаимодействий в сфере обработки персональных данных и стандартизацию методов идентификации личности. В информационных системах стали скапливаться значительные объёмы информации о населении. Это привело к тому, что информация о человеке, которая ранее не позволяла его идентифицировать, эволюционировала в комплекс данных, обладающий достаточным информационным потенциалом для идентификации индивида. Предложенное в диссертации решение проблемы заключается в актуализации нормативного определения персональных данных с учётом современных технологических и правовых аспектов их обработки, а так же формирования и становления информационного общества.

В Российской Федерации назрела необходимость коррекции используемой модели правового регулирования отношений, касающихся персональных данных, которая изначально была ориентирована на обработку информации о физических

лицах, документированной преимущественно на бумажных, а не электронных носителях, в ручном или слабо автоматизированном режиме. Развитие информационных технологий привело к увеличению объёмов персональных данных, которые обрабатываются в автоматизированном режиме. Доступ к информации о человеке стал практически мгновенным и значительно упростился. Законодательство, регулирующее обработку персональных данных, постоянно устаревает, из-за чего требуется или его постоянное совершенствование, или кардинальный пересмотр. Решение этой проблемы является условием для выстраивания современной системы правовой защиты персональных данных, которая будет соответствовать целям и задачам информационно-правового регулирования обработки информации о физических лицах в Российской Федерации. Важным событием станет введение в Российской Федерации в эксплуатацию «Единого регистра сведений о населении»; централизация автоматизации обработки сведений о населении не только положительно скажется на сокращении времени предоставления государственных услуг, но и позволит повысить эффективность и качество информационного обеспечения принимаемых управленческих решений.

Для выработки новых подходов к правовому регулированию персональных данных был проанализирован зарубежный опыт. Развитие юридической науки и законодательства об охране персональных данных привели к формированию двух основных моделей регламентации обработки информации о физических лицах: централизованной и децентрализованной. Централизованная модель характерна для стран Европы и Китайской Народной Республики, а также для постсоветских государств. Децентрализованная модель регулирования прижилась в США. Оба этих подхода к защите персональных данных имеют свою специфику и преимущества. Исследование опыта США и ЕС в сфере правовой защиты персональных данных демонстрирует наличие эффективных механизмов регулирования, которые могут быть экстраполированы на национальные системы регламентации обработки персональных данных. Фундаментом регулирования обработки информации о человеке в США и ЕС является приоритет прав личности,

а также система мер, направленная на принуждение оператора персональных данных не только к соблюдению требований законодательства, но и на развитие механизма получения компенсаций пострадавшими от утечек информации. Правовые подходы, применяемые в Китайской Народной Республике, заслуживают отдельного упоминания. В КНР была выстроена эффективная система защиты персональных данных граждан, которая учитывает современные особенности цифровой обработки такой информации. Важным отличием правовой модели регулирования обработки информации о физических лицах в КНР от США и ЕС является то, что её ключевой принцип — обеспечение безопасности государства, права личности имеют меньший приоритет. Это сказалось на том, что регуляторы имеют достаточно широкие полномочия. Среди интересных для отечественной правовой науки конструкций, в опыте КНР можно выделить категорирование информационных систем обработки персональных данных на классы в зависимости от значимости хранимой информации, а также независимый аудит операторов персональных данных с предоставлением результатов регулятору. Заимствование и адаптация проверенных правовых решений, успешно применяемых в зарубежных юрисдикциях, способны расширить инструментарий отечественной юридической науки в сфере регулирования обработки персональных данных и помочь устранить существующие пробелы в национальном законодательстве

С развитием и становлением информационного общества персональные данные стали приобретать черты социально-экономической характеристики человека. В сочетании с распространением технологий автоматизации анализа данных, информация о физических лицах начала превращаться в значимый ресурс, что повлекло за собой значительный рост числа атак на информационную инфраструктуру операторов персональных данных со стороны различных злоумышленников, желающих получить доступ к сведениям о физических лицах. Число утечек персональных данных постоянно увеличивается. Требования к информационной безопасности систем обработки персональных стали усложняться. Рост числа утечек информации о физических лицах связан с

недостаточностью внимания, уделяемого информационной безопасности систем, которые обрабатывают такие сведения. По этой причине основным принципом совершенствования регламентации обработки персональных данных должно стать выявление недобросовестных операторов, халатно относящихся к требованиям законодательства о защите персональных данных. Эта мера будет стимулировать операторов уделять больше внимания соблюдению требования к обработке информации о физических лицах. Наблюдаемая тенденция к ежегодному росту числа утечек персональных данных в сочетании с недостаточным уровнем соблюдения операторами законодательных требований по защите автоматизированных информационных систем актуализирует научную и практическую задачу разработки механизмов информирования субъектов о надёжности операторов персональных данных. В диссертации предлагается осуществлять временную потребительскую маркировку операторов персональных данных, которая будет информировать об имевшейся недавно утечке на этапе до получения от субъекта согласия на обработку информации о нём. Данная мера положительно скажется на прозрачности репутации операторов персональных данных и позволит физическим лицам оценивать добросовестность организации и иметь представление о возможных рисках, связанных с безопасностью личной информации. Проблема информированности физического лица о передаче его персональных данных третьим лицам, также является в достаточной степени важной. Она сказывается на прозрачности обработки личной информации, это не позволяет субъекту ограничить передачу сведений о себе нежелательным для него организациям и лицам.

Влияние цифровизации на социальные отношения имеет сложный и многоуровневый характер, затрагивая государственный суверенитет, стабильность и национальную безопасность государства, государственное управление, а не только интересы личности. В информационном обществе данные превратились в ресурс и стали иметь критически важное значение для целей социального и экономического развития. Особую ценность приобрели персональные данные, они стали иметь стратегическое значение для государства из-за их значимости для

государственного управления, а также по причине превращения в социально-экономическую характеристику физического лица, с опорой на которую, можно не только осуществлять прогнозирование, но и составлять детализированное досье на человека. Это расширяет возможности не только разведывательных структур иностранных государств, но и различных экстремистских и террористических организаций, использующих сведения о человеке для его вербовки или принуждения к совершению действий, несущих угрозу национальной безопасности.

Развитие современных аналитических технологий привело к повышению эффективности преобразования информации в полезные данные. Превращение персональных данных в ресурс с высоким уровнем спроса как для легальной, так и для нелегальной обработки, а также влияние их защищённости на национальную безопасность, требует от юридической науки поиска новых подходов к обеспечению информационной безопасности не только личности, но и общества и государства в условиях стремительного роста объёмов обработки информации о населении в электронной форме.

Несовершенство механизмов идентификации личности в сети Интернет может приводить не только к нанесению вреда или ущерба личности, но и оказывать воздействие на стабильность общества. Эта проблема также негативно сказывается на доверии к цифровым сервисам, в том числе и предоставляемым государством. Институт общественного контроля мог бы стать важным и эффективным средством отслеживания злоупотреблений, сдерживающим фактором не только для государственных органов, но и для частных компаний, а также для защиты права на частную жизнь. Кроме того, такой подход способствует вовлечению гражданского общества в процесс управления государством.

В информационном обществе одним из ключевых элементов общественных отношений является дистанционная идентификация личности, которая отвечает требованиям: безопасности, достоверности и массовости; эта задача требует выработки новых подходов, в том числе и правовых. В качестве временной меры переходного периода, до решения необходимых правовых и технических задач,

связанных с внедрением «цифрового паспорта гражданина», можно разрешить идентификацию личности через демонстрацию изображений документов через специальное мобильное приложение. Внедрение «цифрового паспорта гражданина» должно стать одной из ключевых задач для государства в процессе построения информационного общества. Требуется консолидация усилий государства и общества для выработки эффективных и непротиворечивых механизмов регламентации отношений, связанных с обработкой персональных данных, с учётом не только интересов государства, но и личности. Для решений этой задачи в диссертации предлагается организовать экспертно-консультативный орган, с опорой на который бы осуществлялась трансформация отечественного права в соответствии с реалиями информационного общества. Такая площадка позволила бы более согласовано и системно, на достаточном экспертном уровне, не только обсуждать современные проблемы информационного права, но и давать рекомендации по законодательным инициативам, связанным с регулированием отношений, касающихся обработки персональных данных. В диссертационном исследовании выдвигается тезис о необходимости актуализации документов стратегического планирования, обусловленной трансформацией современных реалий. Особое внимание уделяется обоснованию важности персональных данных для национальной безопасности и необходимости их комплексной защиты от несанкционированного доступа как элемента обеспечения безопасности государства. Выстраивание государством эффективной системы правовой защиты персональных данных является одним из ключевых условий поддержания требуемого уровня его информационной безопасности.

Внедрение технологий автоматизации идентификации личности позволило осуществлять её множеством новых способов. Одним из них стала биометрия, в достаточной степени достоверная и безопасная, и поэтому используемая для совершения юридически значимых действий. Однако имеющееся в законодательстве определение биометрических данных не в полной мере учитывает специфику такой информации. В работе предложено правовое определение понятия «биометрические персональные данные», которое учитывает

специфику и особенности этой информации о человеке. Но важной задачей остается выработка правовых подходов к защите процедур идентификации физических лиц посредством биометрии, с учётом новых угроз и вызовов, в том числе связанных и с фальсификацией биометрических данных при помощи информационных технологий.

Нельзя не упомянуть использование технологии искусственного интеллекта в сфере персональных данных. Достигнуты два основных результата использования искусственного интеллекта для обработки информации о физических лицах — высокая эффективность анализа данных и генерация новой информации. Способность нейросетей осуществлять генерацию биометрической информации, которая используется для идентификации личности, как другими людьми, так и автоматизированными системами, оказала ощутимое воздействие на отношения, связанные с обработкой и защитой персональных данных и идентификацией личности. Наибольшему воздействию изменений подверглась сфера аналитики, где внедрение ИИ-систем привело к качественному скачку в методах обработки и интерпретации данных. При этом в отечественная правовая наука только работает над концепцией правового режима для информации с персональными данными, генерируемой нейросетями.

Применение нейросетей в сфере работы с персональными данными в целом позитивно и позволяет решить множество задач. Однако злоумышленники уже начали использовать нейросети для достижения противозаконных, в том числе преступных целей. Генеративные алгоритмы нейросетей породили проблему, и поставили перед юристами и государством задачу по выработке новых процедур и алгоритмов идентификации личности по биометрическим данным, которые были бы устойчивы к неправомерному применению технологий.

Важным фактором, влияющим на отношения в сфере обработки персональных данных, является отсутствие в законодательстве процедуры фиксации согласия или несогласия субъекта персональных данных на обработку информации о нём искусственным интеллектом.

Разработка нормативного регулирования применения нейросетей в сфере безопасности осложняется тем, что необходимо соблюсти баланс между защитой прав субъектов персональных данных и эффективностью применения ИИ-аналитики для прогнозирования правонарушений. Особенно это актуально в сфере безопасности, где применение нейросетей может предотвратить совершение, как мошенничеств, так и террористических атак.

Одним из инструментов решения проблем с использованием нейросетей в сфере персональных данных должна стать выстроенная система независимого аудита за разработкой и применением ИИ-алгоритмов, что позволит не только осуществлять контроль уже действующих и применяемых систем искусственного интеллекта, но и тех, которые находятся на стадии проектирования и разработки. Такой аудит даст возможность предотвращать появление ИИ-решений, логика работы которых оказывает негативное влияние на защищённость прав человека, в том числе и связанных с персональными данными.

В диссертации предложено:

а) разработать правовую концепцию регулирования отношений, связанных с применением нейросетей при выполнении операций по обработке персональных данных;

б) определить основополагающие принципы эксплуатации ИИ-систем в процессе обработки персональных данных;

в) разработать концептуальные критерии и исследовательские методики анализа влияния на права человека примененния нейросетей;

г) сформировать концептуальную модель требований к обработке персональных данных нейросетями, что обеспечит существенное повышение уровня защищённости идентификационной информации граждан в контексте распространения нейросетей и позволит устранить дефекты регулирования, пусть на данный момент и экспериментального, в сфере применения этой технологии для обработки персональных данных.

И в заключение стоит упомянуть еще об одной актуальной проблеме.

Персональные данные и большие данные, на первый взгляд далекие друг от друга сущности, тесно связаны. Анализ больших массивов информации дает новые знания, которые могут содержать персональные данные конкретных физических лиц. Перед государством и правоведами встает задача совершенствования правового регулирования отношений по обработке больших данных в увязке с защитой персональных данных. Если анализом больших данных занимается нейросеть, влияние на сферу защиты персональных данных усиливается. Даже обезличенные массивы информации, проанализированные по определённым алгоритмам, могут предоставить новую информацию об индивидууме. Бесконтрольное использование этой технологии может стать причиной нарушения конституционных прав граждан, связанных с тайной частной жизни.

БИБЛИОГРАФИЯ

I. Нормативные источники и документы

Нормативные правовые акты Российской Федерации, РСФСР, СССР

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) // Российская газета. 1993 г. 25 декабря. (с учётом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30 декабря 2008 года № 6-ФКЗ, от 30 декабря 2008 года № 7-ФКЗ, от 5 февраля 2014 года № 2-ФКЗ, от 21 марта 2014 года № 6-ФКЗ и от 21 июля 2014 года № 11-ФКЗ, а также с учетом изменений, одобренных в ходе общероссийского голосовании 1 июля 2020 года)

2. Уголовно-исполнительный кодекс Российской Федерации от 08.01.1997 № 1-ФЗ. // Собрание законодательства РФ, 13.01.1997, № 2

3. Федеральный закон от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» // Собрание законодательства РФ, 20.02.1995, № 8, ст. 609.

4. Федеральный закон от 04.04.2005 № 32-ФЗ «Об Общественной палате Российской Федерации» // Собрание законодательства РФ, 11.04.2005, № 15, ст. 1277.

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. — 2006. — № 31 (ч. I). — ст. 3451.

6. Федеральный закон от 21.07.2014 № 212-ФЗ «Об основах общественного контроля в Российской Федерации» // Собрание законодательства РФ, 28.07.2014, № 30 (Часть I), ст. 4213.

7. Федеральный закон от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» // Собрание законодательства РФ, 04.01.2021, № 1 (часть I).

8. Федеральный закон от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности»» // Собрание законодательства РФ, 18.07.2022, № 29 (часть III), ст. 5233.

9. Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства РФ, 02.01.2023, № 1 (часть I).

10. Федеральный закон от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // Собрание законодательства РФ, 02.12.2024, № 49 (часть IV), ст. 7411.

11. Федеральный закон от 30.11.2024 № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // Собрание законодательства РФ, 02.12.2024, № 49 (часть IV), ст. 7412.

12. Федеральный закон от 28.02.2025 № 23-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и отдельные

законодательные акты Российской Федерации» // Собрание законодательства РФ, 03.03.2025, № 9, ст. 852.

13. Федеральный закон от 24.06.2025 № 156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ, 30.06.2025, № 26 (часть I), ст. 3486.

14. Указ Президента РФ от 25.06.1996 № 989 "О Политическом консультативном совете". // Собрание законодательства РФ, 01.07.1996, № 27, ст. 3232.

15. Указ Президента РФ от 17.12.1997 № 1300 "Об утверждении Концепции национальной безопасности Российской Федерации" // "Российские вести", № 239, 25.12.1997.

16. Указ Президента РФ от 08.08.2000 № 1461 "О Политическом консультативном совете. // Собрание законодательства РФ, 14.08.2000, № 33, ст. 3351.

17. Указ Президента РФ от 12.05.2009 № 537 "О Стратегии национальной безопасности Российской Федерации до 2020 года" // Собрание законодательства РФ, 18.05.2009, № 20, ст. 2444.

18. Указ Президента РФ от 19.12.2012 № 1666 "О Стратегии государственной национальной политики Российской Федерации на период до 2025 года" // Собрание законодательства РФ, 24.12.2012, № 52, ст. 7477.

19. Указ Президента РФ от 31.12.2015 № 683 "О Стратегии национальной безопасности Российской Федерации" // Собрание законодательства РФ, 04.01.2016, № 1 (часть II), ст. 212.

20. Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" // "Собрание законодательства РФ", 12.12.2016, № 50, ст. 7074.

21. Указ Президента РФ от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы". // "Собрание законодательства РФ", 15.05.2017, № 20, ст. 2901

22. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

23. Указ Президента РФ от 10.10.2019 № 490 "О развитии искусственного интеллекта в Российской Федерации" (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года") // Собрание законодательства РФ, 14.10.2019, № 41, ст. 5700.

24. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ, 05.07.2021, № 27 (часть II), ст. 5351.

25. Указ Президента РФ от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации"// Собрание законодательства РФ, 05.07.2021, № 27 (часть II), ст. 5351.

26. Указ Президента РФ от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации"// Собрание законодательства РФ, 05.07.2021, № 27 (часть II), ст. 5351.

27. Указ Президента РФ от 15.02.2024 № 124"О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490 "О развитии искусственного интеллекта в Российской Федерации" и в Национальную стратегию, утвержденную этим Указом" // "Собрание законодательства РФ", 19.02.2024, № 8, ст. 1102

28. Указ Президента РФ от 07.05.2024 № 309 "О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года". // Собрание законодательства РФ, 13.05.2024, № 20, ст. 2584.

29. Распоряжение Президента РФ от 16.02.1994 № 78-рп "Об Общественной палате при Президенте Российской Федерации". // "Собрание актов Президента и Правительства РФ", 21.02.1994, № 8, ст. 592.

30. Распоряжение Правительства РФ от 09.06.2005 № 748-р. «Об одобрении Концепции создания системы персонального учета населения Российской Федерации» Собрание законодательства РФ, 13.06.2005, № 24, ст. 2414.

31. Приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 "Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну" (Зарегистрирован 10.08.2021 № 64589) // Официальное опубликование правовых актов : [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202108100027

32. Приказ Роскомнадзора от 27.10.2022 № 178 "Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных" // Официальное опубликование правовых актов : [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202211290004

33. Приказ Роскомнадзора от 28.10.2022 № 179 «Об утверждении требований к подтверждению уничтожения персональных данных» // Министерство Юстиции Российской Федерации: [Электронный ресурс]. URL: https://minjust.consultant.ru/special/documents/document/33515

34. Текст Конституции СССР 1924 г. // История Советской Конституции в документах. — М., 1957.

35. Свод законов Российской империи. Том двенадцатый. Часть I. Уставы путей сообщения, почтовый, телеграфический, строительный, и пожарный — 1857–1868 — Тип. Второго Отделения Собственной Е.И.В.Канцелярии — 664 с.

36. Постановление Съезда Народных Депутатов Российской Советской Федеративной Социалистической Республики «Об упразднении органов народного контроля в РСФСР» // Ведомости СНД РСФСР и ВС РСФСР, 1990, № 3, ст. 28.

37. Постановление ВС РСФСР от 22 ноября 1991 г. N 1920-1 "О Декларации прав и свобод человека и гражданина" // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации от 26 декабря 1991 г., № 52, ст. 1865.

38. Послание Президента Российской Федерации Федеральному Собранию «О национальной безопасности» от 13 июля 1996 г. // Российская газета, № 17, 14.07.1996.

39. Положеніе о рабочемъ контроле. // СУ РСФСР, 1917, № 3, ст. 35.

40. Об образовании Общественной палаты Конституционного совещания. // Собрание актов Президента и Правительства РФ, 27.09.1993, № 39, ст. 3674.

41. О народном контроле в СССР // Ведомости ВС СССР, 1979, № 49, ст. 840.

42. Конституция СССР 1977 года // Сборник нормативных актов по советскому государственному праву. М.: Юрид. лит., 1984. С. 179–194.

43. Конституция РСФСР 1925 // История советской Конституции (в документах) 1917–1956. М:. Юрид. лит.,1957.

44. Конституция (Основной Закон) Союза Советских Социалистических Республик (принята ВС СССР .07.10.1977) // Ведомости ВС СССР, 1977, № 41, ст. 617.

45. Конституция (Основной Закон) Российской Социалистической Федеративной Советской Республики. Принята V Всероссийским съездом Советов 10 июля 1918 года // СУ РСФСР. 1918.

46. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // Российская газета, № 187, 28.09.2000.

Проекты законов Российской Федерации

1. Федеральный закон от 24.06.2025 № 156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ, 30.06.2025, № 26 (часть I), ст. 3486.

2. Проект 04/13/02-20/00099581 «О внесении изменений в Федеральный закон Об информации, информационных технологиях и о защите информации». // Портал правовой информации : [Электронный ресурс].. URL: https://regulation.gov.ru/p/99581 (дата обращения: 22.06.25).

3. О предъявлении документов с использованием информационных технологий // Федеральный портал проектов нормативных правовых актов. URL: https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=137532# (дата обращения: 3.12.23).

Международные нормативные акты

1. Всеобщая декларация прав человека от 10 декабря 1948 г. // Международное публичное право. Сборник документов / Бекяшев К. А., Бекяшев Д. К. — М.: Проспект, 2009. — С. 221–224.

2. Конвенция о защите физических лиц при автоматизированной обработке персональных данных // Собрание законодательства РФ, 03.02.2014, № 5, ст. 419.

3. Международный пакт о гражданских и политических правах (Нью-Йорк, 19 декабря 1966 г.) // Бюллетень Верховного Суда РФ. 1994. № 12. С. 5.

4. О защите физических лиц при автоматизированной обработке персональных данных. // Официальный интернет-портал правовой информации: [Электронный ресурс]. URL: http://www.pravo.gov.ru (дата обращения: 13.10.23).

5. Хартия Европейского Союза об основных правах: Комментарий / под ред. д.ю.н., проф. С. Ю. Кашкина. — М.: Юриспруденция, 2001.

6. Европейская конвенция по правам человека. // European Court of Human Rights: [Электронный ресурс]. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_rus (дата обращения: 07.20.23).

Нормативные правовые акты зарубежных государств

1. Закон КНР «О защите прав потребителей». // Chinalaw.center 中国法律俄文网: [Электронный ресурс]. URL: https://chinalaw.center/civil_law/china_consumer_rights_protection_law_revised_2013_russian/ (дата обращения: 17.11.23).

2. Конституция Греческой Республики "Το Σύνταγμα της Ελλάδας" от 11.06.1975 г. с изм. и допол. в ред. от 2008 г. // WIPO : [Электронный ресурс]..URL: https://www.wipo.int/wipolex/en/legislation/details/9463 (дата обращения: 29.09.23), (пер.: Яндекс-переводчик).

3. Конституция Итальянской Республики "Costituzione della Repubblica Italiana" от 1.01.1948 г. с изм. и допол. в ред. от 26.09.2023 // Senato della Repubblica : [Электронный ресурс]. URL: https://www.senato.it/sites/default/files/media-documents/Costituzione_RUSSO.pdf(дата обращения: 29.09.23).

4. Конституция Республики Казахстан (принята на республиканском референдуме 30 августа 1995 года) (с изменениями и дополнениями по состоянию на 19.09.2022 г.) // Параграф : [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=1005029(дата обращения: 19.11.23).

5. Федеральная Конституция Швейцарской конфедерации "Federal Constitution of the Swiss Confederation" от 18.04.1999 г. с изм. и допол. в ред. от 13.02.2022 г. // Swiss Right: [Электронный ресурс]. URL: https://www.swissrights.ch/gesetze/uebersicht.php?buch=BV&jahr=2024&lg=EN (дата обращения: 30.09.23)

6. Закон КНР «О защите прав потребителей». // Chinalaw.center 中国法律俄文网 : [Электронный ресурс] .URL: https://chinalaw.center/civil_law/china_consumer_rights_protection_law_revised_2013_russian/ (дата обращения: 17.11.23).

7. Конституция Греческой Республики "Το Σύνταγμα της Ελλάδας" от 11.06.1975 г. с изм. и допол. в ред. от 2008 г. // WIPO : [Электронный ресурс]..URL: https://www.wipo.int/wipolex/en/legislation/details/9463 (дата обращения: 29.09.23), (пер.: Яндекс-переводчик).

8. Конституция Итальянской Республики "Costituzione della Repubblica Italiana" от 1.01.1948 г. с изм. и допол. в ред. от 26.09.2023 // Senato della Repubblica : [Электронный ресурс]. URL: https://www.senato.it/sites/default/files/media-documents/Costituzione_RUSSO.pdf(дата обращения: 29.09.23).

9. Конституция Республики Казахстан (принята на республиканском референдуме 30 августа 1995 года) (с изменениями и дополнениями по состоянию на 19.09.2022 г.) // Параграф : [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=1005029(дата обращения: 19.11.23).

10. Федеральная Конституция Швейцарской конфедерации "Federal Constitution of the Swiss Confederation" от 18.04.1999 г. с изм. и допол. в ред. от 13.02.2022 г. // Swiss Right: [Электронный ресурс]. URL: https://www.swissrights.ch/gesetze/uebersicht.php?buch=BV&jahr=2024&lg=EN (дата обращения: 30.09.23)

11. Конституция Японии "日本国憲法" от 3 ноября 1946 г // Prime Minister of Japan and His Cabinet : [Электронный ресурс]. URL: https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html(дата обращения: 30.09.23), (пер.: Яндекс-переводчик).

12. Конституция Японии "日本国憲法" от 3 ноября 1946 г // Prime Minister of Japan and His Cabinet : [Электронный ресурс]. URL: https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html(дата обращения: 30.09.23).

13. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 01.07.2024 г.) // Эділет : [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/Z1300000094/links (дата обращения: 22.11.23).

14. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 01.07.2024 г.) // Эділет : [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/Z1300000094/links (дата обращения: 22.11.23).

15. Общий регламент защиты персональных данных (GDPR) Европейского союза // GDPR TEXT : [Электронный ресурс]. URL: https://gdpr-text.com/ru/read/article-14/ (дата обращения: 1.12.23).

II. Судебная практика

1. Постановление Конституционного Суда РФ от 16.06.2015 № 15-П "По делу о проверке конституционности положений статьи 139 Семейного кодекса Российской Федерации и статьи 47 Федерального закона "Об актах гражданского состояния" в связи с жалобой граждан Г.Ф. Грубич и Т.Г. Гущиной"// "Вестник Конституционного Суда РФ", № 5, 2015.

2. Апелляционное определение Московского городского суда от 30.01.2020 по делу №33а-707/2020, 2а-577/2019

3. Кассационное определение Второго кассационного суда общей юрисдикции от 31.07.2020 г. №88а-17020/2020;

4. Постановление Второго кассационного суда общей юрисдикции от 07.07.2020 г. по делу №16-3770/20.

5. Постановление Девятого арбитражного апелляционного суда от 06.02.2018 г. по делу № А40–18827/17;

6. Постановление Мирового судьи судебного участка № 374 Таганского района г. Москвы от 13.02.202 г.; Решение Таганского районного суда г. Москвы от 16.03.2020 г.

7. Постановление Суда по интеллектуальным правам от 24.07.2018 г. по делу № А40–18827/2017;

8. Решение Арбитражного суда г. Москвы от 12.10.2017 г. по делу № А40-18827/17–110–180;

9. Решение Арбитражного суда г. Москвы от 22.03.2021 г. по делу № А40–18827/17–110–180; Постановление Девятого арбитражного апелляционного суда от 08.07.2021 г. по делу № А40–18827/17.

10. Постановление ВС РСФСР от 22 ноября 1991 г. N 1920-1 "О Декларации прав и свобод человека и гражданина" // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации от 26 декабря 1991 г., № 52, ст. 1865.

III. Научная литература: диссертации, монографии, словари, учебно-методическая литература

Монографии, учебники, научные статьи

1. Аберхаев Э. Р. Право на неприкосновенность частной жизни: юридическая характеристика и проблемы реализации // Russian Journal of Economics and Law, №. 1 (5), 2008, С. 90–94.

2. Авакьян С. А. Конституционное право России. Учебный курс: учеб. пособие: в 2 т. — 5*е изд., перераб. и доп. — М.:Норма : ИНФРА*М, 2014. —с.675.

3. Актуальные проблемы информационного права: учебник / подред. И. Л. Бачило, М.А Лапиной. 2-е изд. перераб. М.: Юрайт, 2019.

4. Алексашин М. Н. Защита персональных данных как условие обеспечения безопасности личности // Право и безопасность. 2014. № 1. С. 68–73.

5. Амелин Р. В. Использование государственных информационных систем как форм (источников) права: перспективы и проблемы // Вестник Московского университета. Серия 21: Управление (государство и общество). — 2021. — № 4. — С. 3–15.

6. Антонова В. В. Проблемы и решения правового регулирования защиты персональных данных // Учет и контроль. — 2022. — № 3. — С. 15–17.

7. Афанасьев С. Д. Биометрическая идентификация и права человека: демаркационная линия / С. Д. Афанасьев, И. А. Терещенко, Д. А. Яцкевич // Закон. – 2022. – № 3. – С. 33-46.

8. Баглай М. В. Конституционное право Российской Федерации: учеб. для вузов. — 13-е изм. и доп. — М. Норма, 2018. —с. 228.

9. Батурин Ю. М. Аудит алгоритмов. // Вестник Московского университета. Серия 26. Государственный аудит. — 2024.— №4 — С. 146-154

10. Батурин Ю. М. От интернета до виртуальной Земли и метавселенной:(краткая история информационных технологий на критическом рубеже). М.: ИИЕТ РАН; Саратов: Амирит, 2022.

11. Бахтеев Д. В. Преодоление нелегальной трансграничной передачи персональных данных / Д. В. Бахтеев, А. М. Сосновикова, Е. В. Казенас // Journal of Digital Technologies and Law. – 2024. – Т. 2, № 4. – С. 943-972.

12. Бачило И. Л. Правовое обустройство информационной действительности: проблемы и перспективы / И. Л. Бачило, П. У Кузнецова // Российский юридический журнал. – 2008. – № 5(62). – С. 15-25.

13. Бачило И.Л. Информационное право: учебник для вузов. 5-е изд.,перераб. и доп. М.: Юрайт, 2022.

14. Бердникова Е. В. Общественный контроль в конституционно-правовом взаимодействии публичной власти и институтов гражданского общества в Российской Федерации: специальность 12.00.02 "Конституционное право; конституционный судебный процесс; муниципальное право": диссертация на соискание ученой степени доктора юридических наук, 2022. — 482 с.

15. Бобунова С. А. Персональные данные и цифровизация. // Молодой ученый. — 2022. — № 36 (431). — С. 75–79.

16. Большие данные и их применение в образовании / М. В. Алиева, З. Б. Батчаева, З. М. Муцурова, М. З. Исаева // Журнал прикладных исследований. — 2023. — № 6. — С. 140–146.

17. Бочарникова А. Д. Модернизация государственного управления в условиях цифровизации общества // 25 лет конституционного развития России и проблемы государственного управления: материалы межвузовской научно-практической конференции, Краснодар, 12 декабря 2018 года. — Краснодар: Кубанский государственный университет. — 2018. — С. 246–249.

18. Бражник Т. А. Правовые вопросы обеспечения информационной безопасности личности // Информационное право. – 2018. – № 4. – С. 17-21.

19. Бундин М. В. К вопросу о содержании персональных данных // Информационное право. – 2019. – № 4. – С. 25-30.

20. Бундин М. В. Персональные данные как информация ограниченного доступа // Информационное право. – 2009. – № 1. – С. 10-14.

21. Будник Р. А. Особенности публично-правовой защиты персональных (в том числе биометрических) данных на постсоветском пространстве: модель Республики Казахстан / Р. А. Будник, Д. Ю. Сапронов, Э. А. Иваева // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2024. – Т. 10, № 4. – С. 159-164.

22. Ван Г. Механизм административно-п равового регулирования защиты персональных данных в Китае: состояние, недостатки и путь решения // Вестник Московского университета. Серия 11: Право. – 2024. – № 4. – С. 204-232.

23. Велиева Д. С. Право на неприкосновенность частной жизни и проблемы его обеспечения в условиях развития цифровых технологий // Права человека: история, теория, практика: сборник научных статей. — Курск: Университетская книга, 2022. — С. 16–22.

24. Войниканис Е. А., Машукова Е. О., Степанов-Егиянц В. Г. Неприкосновенность частной жизни, персональные данные и ответственность за незаконные сбор и распространение сведений о частной жизни и персональных данных: проблемы совершенствования законодательства // Законодательство. 2014. № 12. С. 74–80.

25. Войниканис Е.А. Большие (персональные) данные: проблема баланса интересов // Журнал Суда по интеллектуальным правам, № 4 (34), 2021 г., с. 19-27.

26. Волчинская Е. К. Законодательство о защите персональных данных: проблемы и решения / Е. К. Волчинская, В. В. Дятленко // Информационное право. – 2006. – № 1. – С. 11-16.

27. Волчинская Е. К. Место персональных данных в системе информации ограниченного доступа / Е. К. Волчинская // Право. Журнал Высшей школы экономики. – 2014. – № 4. – С. 193-207

28. Гагарин А. С. Одиночество как экзистенциал средневековой философии // Научный ежегодник Института философии и права Уральского отделения Российской академии наук. — 2012. — № 12. — С. 148–165.

29. Гаджиев Г. К. Защита персональных данных и приватности в эпоху цифровизации: вызовы и решения // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9, № 10(48). – С. 38-41

30. Городов О.А. Информационное право: учебник для бакалавров.2-е изд. М.: Проспект, 2019.

31. Горячева Е. В. Проблемы защиты персональных данных в банковской сфере // Юридическая наука и практика. – 2023. – Т. 19, № 3. – С. 23-29.

32. Гриб В. В. Общественный контроль: учебник; Московский государственный университет имени М.В. Ломоносова Высшая школа государственного аудита (факультет) Центр общественного контроля. — Москва: Издательская группа "Юрист", 2017. — 656 с. — ISBN 978-5-94103-417-8.

33. Гриб В. В. Роль и место общественных палат в системе общественного контроля в Российской Федерации // Конституционное и муниципальное право. — 2015. — № 5. — С. 33.

34. Гринев С. А. Формирование стратегических приоритетов промышленного развития РФ как инновационный фактор преодоления кризисных периодов / Гринев С. А, Квинт В. Л. // Экономика промышленности. – 2023. – Т. 16, № 3. С. 275-283.

35. Гринько С. Д. Противодействие посягательствам на информационную безопасность // Право и государство: теория и практика). — 2020. — № 3 (183). — С. 246–249.

36. Данилова В. А., Левкин Д. М. Правовые аспекты регулирования "deepfake" технологии в россии // Право и государство: теория и практика. 2022. №7 (211), стр. 88–91.

37. Денисенко В. В., Евтеева К. С., Савченко И. И., Скрыпников А. А. Использование искусственного интеллекта для обработки персональных данных // Международный журнал гуманитарных и естественных наук. 2020. №7–1. с. 110–114.

38. Денисова А. Б., Сенюшина В. Г. Влияние информационной реальности на существование человека // Современные проблемы науки и образования. — 2012. — № 6 с. 347.

39. Дикаев С. У. Право безопасности и доктрина информационной безопасности России // Криминология: вчера, сегодня, завтра. – 2017. – № 1(44). – С. 37-39.

40. Добробаба М. Б. Дипфейки как угроза правам человека // Lex Russica (Русский закон). – 2022. – Т. 75, № 11(192). – С. 112-119.

41. Дремлюга Р. И. "Использование искусственного интеллекта в преступных целях: уголовно-правовая характеристика" // Азиатско-Тихоокеанский регион: экономика, политика, право, том l. 23, №. 3, 2021, С. 153–165.

42. Дроздов В. Ю. Использование искусственного интеллекта для предупреждения преступности. // Закон и право. — 2021. — № 9. — С. 114–117.

43. Елин В. М. Защита персональных данных в медицинской отрасли США // Информационное право. – 2020. – № 1. – С. 15-19.

44. Заславская. Н. М. Пределы цифровизации государственного экологического управления // Правовое государство: теория и практика. – 2024. – № 4(78). – С. 44-54.

45. Зубарев С. М. Понятие и сущность общественного контроля за деятельностью государственных органов // Административное право и процесс. — 2011. — № 5. — С. 7–13., Зубарев С. М. Новые технологии общественного контроля: реальность или иллюзия? // Вестник Пермского университета. Юридические науки. 2019. № 1.

46. Зубарев С. М. Правовые риски цифровизации государственного управления // Актуальные проблемы российского права. — 2020. №6 (115). — С 23–32.

47. Ильюшина И. С. Историческая ретроспектива развития правового регулирования и защиты персональных данных в дореволюционной период // Информационное право. – 2023. – № 4(78). – С. 38-41.

48. Информационное право: учебник / под ред. С. Е. Чаннова. М.: Норма; ИНФРА-М, 2024.Информационное право: учебник для вузов / Н. Н. Ковалева [и др.] ; под ред. Н. Н. Ковалевой. М.: Юрайт, 2024.

49. Информационное право: учебник для вузов / под ред. д-ра юрид.наук, проф. М. А. Федотова. 2-е изд., перераб. и доп. М.: Юрайт, 2023.

50. Информационные технологии в юридической деятельности (правовая информатика в цифровую эпоху): учебное пособие: в 2 ч. /под ред. д-ра юрид. наук, проф В. А. Вайпана. М.: Юстицинформ, 2024, 2025.

51. Ишеков. К. А. Гражданско-правовое регулирование института персональных данных умерших в современной России / К. А. Ишеков, Д. С. Холопцев // Вестник Российской правовой академии. – 2022. – № 1. – С. 76-81.

52. Ищенко А. Н. Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности России в информационной сфере / А. Н. Ищенко, А. Н. Прокопенко, А. А. Страхов // Проблемы правоохранительной деятельности. – 2017. – № 2. – С. 55-62.

53. Кабышев В. Т. Народовластие в системе конституционного строя России: конституционно-политическое измерение // С Конституцией по жизни: Избранные научные труды. — М.: Формула права, 2013. — 320 с., Кабышев В. Т. Человек и власть: конституционные принципы взаимоотношений // С Конституцией по жизни: Избранные научные труды. — М.: Формула права, 2013. — 320 с.

54. Камалова Г. Г. Биометрические персональные данные: определение и сущность // Информационное право. – 2016. – № 3. – С. 8-12.

55. Касюк А. Я. Информационное противоборство: генезис и первые шаги // Вестник Московского государственного лингвистического университета. Общественные науки. 2019. №3 (836), С. 157-172.

56. Кирильчик Е. В. Проблемы обеспечения защиты биометрических персональных данных в условиях цифровой экономики / Е. В. Кирильчик, Е. В. Белованс // ГлаголЪ правосудия. — 2022. — № 3(29). — С. 16–21.

57. Климашин А. Г. Утрата государственной монополии на персональные данные как риск национальной безопасности // Журнал Белорусского государственного университета. Социология. – 2019. – № 3. – С. 107-112.

58. Клименко С. А. Обеспечение защищённости персональных данных как основа национальной безопасности России в условиях цифровизации // Право и государство: теория и практика. – 2024. – № 6(234). – С. 216-221.

59. Кнышоид М. З. Особенности правовой защиты персональных данных в рамках межведомственного электронного документооборота // Образование и право. — 2023. — № 2. — С. 151–158

60. Ковалева Н. Н. Проблемы обеспечения конфиденциальности персональных данных при использовании систем искусственного интеллекта / Н. Н. Ковалева, Н. А. Жирнова // Журнал российского права. – 2024. – Т. 28, № 7. – С. 109-121.

61. Колюшин Е. И. Правовые проблемы электронизации (цифровизации) выборов // Вестник Университета имени О. Е. Кутафина . —2019. —№. 9 (61). — С. 103-113.

62. Комкова Г. Н. Проблемы обеспечения равенства и справедливости на современном этапе конституционного развития России // Вестник Саратовской государственной юридической академии. — 2018. — № 2 (121), Комкова, Г. Н., Бердникова, Е. В. Содержание объекта и предмета общественного контроля в Российской Федерации: теоретико-правовые вопросы // Российское право: образование, практика, наука. — 2019. — № 4 (112).

63. Комментарий к Конституции Российской Федерации / Под ред. проф. В. Д. Зорькина — 3-е изд., пересмотр. — Москва: Норма: НИЦ ИНФРА-М, 2013. — 1040 с. ISBN 978-5-91768-441-3.

64. Комментарий к Конституции Российской Федерации / Под ред. проф. В. Д. Зорькина — 3-е изд., пересмотр. — Москва: Норма: НИЦ ИНФРА-М, 2013. — 1040 с. ISBN 978-5-91768-441-3.

65. Конвенция о защите прав человека и основных свобод. Заключена в г. Риме 4 ноября 1950 г. (с изм. от 13.05.2004, вместе с протоколами № 1, № 4 и № 7 // Собрание законодательства РФ. 2001. № 2. ст. 163.

66. Копылов В. А. Информационное право: учебник. — 2-е, перераб. и доп изд. — Москва: Юристъ, 2005. — 510 с.

67. Корецкий А. С. Управление процессами трансформации предприятия в условиях цифровой экономики // Вестник Московского университета. Серия 21: Управление (государство и общество). — 2021. — № 1. — С. 48-63.

68. Корецкий, А. С. Управление процессами трансформации предприятия в условиях цифровой экономики / А. С. Корецкий // Вестник Московского университета. Серия 21: Управление (государство и общество). — 2021. — № 1. — С. 48–63.

69. Кривогин М. С. Особенности правового регулирования биометрических персональных данных / М. С. Кривогин // Право. Журнал Высшей школы экономики. – 2017. – № 2. – С. 80-89.

70. Кротов, А. В. Соотношение права на частную жизнь с правом на жизнь, свободу и личную неприкосновенность // Адвокат. — 2011. — № 1. — С. 32–39.

71. Кудина М. В., Ишеков К. А., Ленков И. Н. Теории и практики государственного управления в современных условиях (итоги работы секции ежегодной научной конференции "Ломоносовские чтения" в 2021 Г.) // Вестник Московского университета. Серия 21: Управление (государство и общество). — 2021. — № 2. См: — С. 67–102.

72. Кузнецов П. У. Информационное право: учебник. М.: Юстиция, 2019.Ловцов Д. А. Информационное право: учебное пособие. М.: РГУП, 2019.Лопатин В.Н. Информационное право: учебник. 3-е изд. М.: Проспект, 2021.

73. Кучерявый М. М. Основные факторы влияния политики информационной безопасности на национальную безопасность современной России // Евразийская интеграция: экономика, право, политика. – 2013. – № 14. – С. 164-168.

74. Локк Д. Избранные философские произведения. Т. 2. М.: Соцэкгиз, 1960. — 532 с.

75. Лясковская Е. А., Григорьева К. М., Халилова Г. Р.. Цифровизация государственного и муниципального управления в субъектах российской федерации. // Вестник Южно-Уральского государственного университета. Серия «Экономика и менеджмент». — 2023. — Том 17 № 4. — С.29–42.

76. Малеина М. Н. Право на тайну и неприкосновенность персональных данных // Журнал российского права. – 2010. – № 11(167). – С. 18-28.

77. Малюк А. А., Морозов А. В. Формирование цифровой экономики и проблемы совершенствования нормативно-правового регулирования в области обеспечения информационной безопасности. // Безопасность информационных технологий. — 2019. — Т. 26, № 4. — С. 21–36. — DOI 10.26583/bit.2019.4.02. — EDN TWVZMS.

78. Марченко М. Н. Теория государства и права учебник / М.Н. Марченко; Московский государственный университет имени М.В. Ломоносова. — 2-е изд., перераб. и доп. — Москва : Проспект, Изд-во Московского университета, 2018. — 636 с.

79. Марченко, М. Н. Проблемы теории государства и права : учебник / М. Н. Марченко ; Московский государственный университет им. М. В. Ломоносова, юридический факультет. — 2-е изд., перераб. и доп. — Москва : ООО «Юридическое издательство Норма», 2019. — 784 с.

80. Медведев В. В. Роль цифрового стратегического планирования в государственном регулировании экономики. // Университет им. В.И. Вернадского. № 2(92). 2024 г.С. 88-105

81. Минбалеев А. В. Проблемы цифрового права: учебное пособие. Саратов: Амирит, 2022.

82. Минбалеев А. В., Сторожакова Е. Э. Проблемы правовой охраны персональных данных в процессе использования нейронных сетей // Вестник Университета имени О. Е. Кутафина. 2023. №2 (102), стр. 71–79.

83. Минзов А. С. О новой доктрине информационной безопасности России (размышления о совершенствовании системы профессионального образования в сфере информационной безопасности) / А. С. Минзов, А. Ю. Невский, О. Ю. Баронов // ИТНОУ: Информационные технологии в науке, образовании и управлении. – 2017. – № 3(3). – С. 80-85.

84. Михайлова И. А. Персональные данные и их правовая охрана: некоторые проблемы теории и практики // Законы России : опыт, анализ, практика : правовой журнал. 2017. № 10. С. 11–19.

85. Молчанов Н. А. Новые аспекты правового регулирования государственного стратегического планирования в Российской Федерации / Н. А. Молчанов, В. П. Егоров, Е. К. Матевосова // Актуальные проблемы российского права. – 2015. – № 2(51). – С. 28-34.

86. Морозов А. В. Информационное право и информационная безопасность. Часть 1 : учебник для магистров и аспирантов / А. В. Морозов, Л. В. Филатова, Т. А. Полякова. — Москва, Саратов : Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. — 604 с.

87. Морозов А. В., Филатова Л. В., Полякова Т.А. Информационное правои информационная безопасность: учебник для магистров и аспирантов: в 2 ч. М.: ВГУЮ (РПА Минюста России), 2016.

88. Морозова Л. А. Роль правовых приоритетов в формировании стратегии законотворчества в России // Юридическая техника, №. 9, 2015, С. 485-487.

89. Мунтян А. В. Мы вступилив эпоху цифрового огораживанияи национализации (персональных) данных // Закон. – 2022. – № 3. – С. 8-15.

90. Нерсесянц В. С. Научные биографии. Сократ / АН СССР. — Москва : Наука, 1977. — 150 с.

91. Нерсесянц В.С. Общая теория права и государства: учеб. для юрид. вузов и факультетов / В.С. Нерсесянц. – М.: НОРМА, 2001. – 552 с.

92. Никитина Е. Е. Информационная безопасность как элемент конституционного статуса личности // Журнал российского права. – 2024. – Т. 28, № 1. – С. 81-94.

93. Николаева К. С. Цифровизация государственного управления как условие снижения транзакционных издержек в сфере публичного управления // Современный город: власть, управление, экономика. — 2021. — Т. 1. — С. 40–47.

94. Новгородцев П. И. Об общественном идеале. — М.: Издательство «Пресса», 1991. — 640 с.

95. Овчинникова М. А. Применение big data в лабораторной медицине / М. А. Овчинникова, Ю. И. Жиленкова, Н. Ю. Черныш // Российский журнал персонализированной медицины. — 2023. — Т. 3, № 4. — С. 77–87.

96. Организационное и правовое обеспечение информационной безопасности: учебник и практикум / отв. ред. Т.А. Полякова, А.А. Стрельцов. М.: Юрайт, 2023.

97. Панина О. В., Красюкова Н. Л., Дорофеев А. Н., [и др.]. Выявление направлений совершенствования государственного управления за счет цифровизации государственного управления // Цифровизация государственного управления. — М.: "Издательство Прометей". — 2023. — С. 210–294.

98. Пешин Н. Л. Муниципальная власть: продолжение государства или институт самоорганизации общества / Вестник Воронежского государственного университета. Серия: Право. – 2019. – № 2(37). – С. 38-50

99. Пиголкин А. С. Теория государства и права : учебник для вузов / А. С. Пиголкин, А. Н. Головистикова, Ю. А. Дмитриев ; под редакцией А. С. Пиголкина, Ю. А. Дмитриева. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 516 с.

100. Платон. Сочинения в четырех томах. т. 3. ч. 1 / Под общ. ред. А. Ф. Лосева и В. Ф. Асмуса; Пер.: с древнегреч. — С -Пб: Изд-во С.-Петерб., 2007. — 752 с.

101. Полубинская С. В. Big Data в здравоохранении: информационная безопасность и правовая охрана персональных данных / С. В. Полубинская, М. И. Галюкова // Государство и право. – 2023. – № 6. – С. 149-160

102. Полякова Т. А, Бойченко И. С. Особенности взаимодействия и правового обеспечения информационной безопасности в единой биометрической

системе в Российской Федерации // Правовая политика и правовая жизнь. — 2023. — № 3. — С. 26-34. — DOI 10.24412/1608-8794-2023-3-26-34. — EDN BQZMXN.

103. Полякова Т. А. Влияние цифровой экономики на развитие транспортной отрасли и проблемы обеспечения информационной безопасности: правовой аспект // Транспортное право и безопасность. 2019. № 1 (29). С. 82–86.

104. Полякова Т. А. Роль стратегического планирования в совершенствовании системы государственного управления в Российской Федерации / Т. А. Полякова, Д. А. Афиногенов // Вестник Академии права и управления. – 2016. – № 4(45). – С. 11-18.

105. Полякова Т. А., Бойченко И. С. "Информационная безопасность через призму национального проекта «цифровая экономика»: правовые проблемы и векторы решений" // Право и государство: теория и практика. — №. 2 (170). — 2019. — С. 97–100.

106. Полякова Т. А., Минбалеев А. В., Бойченко И. С. Концептуальные подходы к правовому регулированию информационной безопасности в условиях цифровизации и трансформации права // Вестник УрФО. Безопасность в информационной сфере. 2019. № 3 (33). С. 64–68

107. Полякова Т. А., Минбалеев А. В., Бойченко И. С. Концептуальные подходы к правовому регулированию информационной безопасности в условиях цифровизации и трансформации права // Вестник УрФО. Безопасность в информационной сфере. 2019. № 3 (33). С. 64–68.

108. Попова Т. В. Цифровые технологии и риски неприкосновенности частной жизни // Информационное право. – 2020. – № 4. – С. 30-32.

109. Постникова Е. В. Некоторые аспекты правового регулирования защиты персональных данных в рамках внутреннего рынка Европейского союза / Е. В. Постникова // Право. Журнал Высшей школы экономики. – 2018.

110. Проблемы гармонизации экономических отношений и права в цифровой экономике: монография / отв. ред. В. А. Вайпан, М. А. Егорова. М. : Юстицинформ, 2020.

111. Проблемы общей теории права и государства : учебник / Н. В. Варламова, В. В. Лазарев, В. В. Лапаева, Е. А. Лукашева, Г. В. Мальцев и др. ; под общ. ред. В. С. Нерсесянца ; Ин-т государства и права РАН. — 2-е изд., перераб. — Москва : Норма : ИНФРА-М, 2010. — 815 с.

112. Проблемы общей теории права и государства: Учебник для вузов / Под общ. ред. академика Российской академии наук, д-ра юридических наук, проф. В. С. Нерсесянца. : Норма, 2002. — 832 с..

113. Проблемы создания цифровой экосистемы: правовые и экономические аспекты: монография / под общ. ред. В. А. Вайпана, М. А. Егоровой. М.: Юстицинформ, 2021.

114. Равин С. М. Три конституции Советского государства (1918–1924–1936 гг.) // С. Равин. — Л. : Изд-во Леноблисполкома и Ленсовета, 1937. — 79, [1] с.

115. Рассолов И. М. Биометрия в контексте персональных данных и генетической информации: правовые проблемы / И. М. Рассолов, С. Г. Чубукова, И. В. Микурова // Lex Russica (Русский закон). – 2019. – № 1(146). – С. 108-118.

116. Рассолов И. М. Информационное право: учебник и практикум для вузов. 6-е изд., перераб. и доп. М.: Юрайт, 2025.

117. Рассолов М. М. Теория государства и права : учебник для вузов / М. М. Рассолов. — Москва : Издательство Юрайт, 2010. — 635 с.

118. Рогозин В. Ю., Вепрев С. Б., Остроушко А. В. Информационное право: учебное пособие для студентов вузов. М.: Юнити-Дана, 2017.

119. Савельев А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М.: Статут, 2017. 164 с.

120. Савельев А. И. Новое законодательство КНР в области персональных данных: приватность"с китайской спецификой" / А. И. Савельев, М. А. Иманалиева // Закон. – 2022. – № 3. – С. 75-96.

121. 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.

122. Сапронов Д. Ю. Особенности правового регулирования персональных данных в Китайской Народной Республике. // Вестник Московского университета. Серия 26: Государственный аудит. — 2022. — № 4. — С. 149–157.

123. Сапронов Д. Ю. Правовая эволюция общеевропейского регулирования защиты персональных данных // Труды по интеллектуальной собственности. — 2019. — Т. 34, № 3–4. — С. 83–88.

124. Сапронов Д. Ю. Историческая ретроспектива правового регулирования персональных данных в некоторых странах // Труды по интеллектуальной собственности. — 2022. — Т. 42, № 3. — С. 26–32.

125. Сапронов Д. Ю. Влияние всеобщей цифровизации на правотворчество в сфере персональных данных // Сборник научных статей. В 2-х томах. — Стратегия развития экономики Беларуси: вызовы, инструменты реализации и перспективы. — Право и экономика Минск: 2022. — С. 340–344.

126. Сапронов Д. Ю. Об основных направлениях совершенствования правового регулирования обработки персональных данных (информационно-правовой аспект) // Вестник Московского университета. Серия 26: Государственный аудит. – 2025. – № 3. – С. 136-151.

127. Сапронов Д. Ю. Идентификация физических лиц в цифровую эпоху: информационно-правовые проблемы / Д. Ю. Сапронов // Третьи Бачиловские чтения. Цифровая трансформация: вызовы праву и векторы научных исследований : материалы Международной научно-практической конференции, Москва, 07 февраля 2020 года. – Москва: Общество с ограниченной ответственностью "Проспект", 2020. – С. 302-308.

128. Сапронов Д.Ю. К вопросу об эволюции правового института защиты персональных данных // Вестник Российской правовой академии. — 2025. — № 6. – С.83-95. EDN: AKJZNF.

129. Северин В. А. Методика правового обеспечения безопасности персональных данных в организациях // Вестник Московского университета. Серия 11: Право. – 2021. – № 3. – С. 49-61.

130. Северин В. А. Правовые аспекты обеспечения информационной безопасности цифровой экономики // Пробелы в российском законодательстве. – 2023. – Т. 16, № 8. – С. 46-51.

131. Селютина, Е. Н. Проблемы теории государства и права : учебное пособие для бакалавриата и магистратуры / Е. Н. Селютина, В. А. Холодов. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 168 с.

132. Сергеева Н. Ю. Защита персональных данных граждан Российской Федерации в сети Интернет: отдельные проблемы правового регулирования, Л. Т. Шарудинова // Гражданин и право. — 2021. — № 9. — С. 89–92.

133. Солдатова В. И. Защита персональных данных в условиях применения цифровых технологий / В. И. Солдатова // Lex Russica (Русский закон). – 2020. – Т. 73, № 2(159). – С. 33-43

134. Стародубова О. Е. Современные информационные технологии и информационная безопасность / О. Е. Стародубова, Н. А. Назаров // Информационное право. – 2023. – № 3(77). – С. 44-45.

135. Степкина Ю.С., Яворский М.А. Анализ динамических методов идентификации личности // Актуальные проблемы правоведения. 2022. № 3 (75). С. 28-31.

136. Стрельцов А. А. Новая доктрина информационной безопасности Российской Федерации: информационно-правовые основы обеспечения безопасности информационных угроз // Труды по интеллектуальной собственности. – 2017. – Т. 28, № 1. – С. 116-123.

137. Строкова П. С. Персональные данные в понятийном аппарате цифровой экономики // Информационное право. – 2022. – № 4(74). – С. 34-37. – DOI 10.55291/1999-480X-2022-4-34-37.

138. Ступин Р. С. Искусственный интеллект в системе статистического анализа. // Цифровой регион: опыт, компетенции, проекты: Сборник трудов IV Международной научно-практической конференции, приуроченной к Году науки и технологий в России, Брянск, 25 ноября 2021 года. — Брянск: Федеральное государственное бюджетное образовательное учреждение высшего образования

"Брянский государственный инженерно-технологический университет", 2021. — С. 575–590.

139. Субетто А. И. Закон о биометрии в России — это потенциальное оружие «запада» в войне против // Теоретическая экономика. — 2023. — № 3(99). — С. 128–130.

140. Сунь-цзы. Искусство войны / Пер. с кит. Н. И. Конрада. – М.: Издательство АСТ, 2019. – 256 с.

141. Суриков И.Е. Институт остракизма в Афинах: проблемы и перспективы изучения. С .126-143.

142. Сырых В. М. Теория государства и права : учебник для вузов по специальности «Юриспруденция» : допущено Министерством образования РФ / В. М. Сырых. — 5-е изд., стер. — Москва : Юстицинформ, 2006. — 703 с.

143. Талапина Э. В. Алгоритмы и искусственный интеллект сквозь призму прав человека // Журнал российского права. – 2020. – № 10. – С. 25-39.

144. Талапина Э. В. Большие данные и права человека: на пути к правовому регулированию // Государство и право. 2023. № 7. С. 129–138.

145. Талапина Э. В. Право и цифровизация: новые вызовы и перспективы / Э. В. Талапина // Журнал российского права. – 2018. – № 2(254). – С. 5-17.

146. Талапина Э. В. Правовая защита персональных данных во Франции / Э. В. Талапина // Право. Журнал Высшей школы экономики. – 2012. – № 4. – С. 152-162.

147. Тедеев А. А. К вопросу о трансформации системы права в условиях развития информационно-коммуникационных технологий: постановка проблемы // Информационное пространство: обеспечение информационной безопасности и право. Сб. науч. трудов / под ред. Т. А. Поляковой, В. Б. Наумова, А. В. Минбалеева. М.: ИГП РАН, 2018. С.3.

148. Тедеев А. А. К вопросу о трансформации системы права в условиях развития информационно-коммуникационных технологий: постановка проблемы // Информационное пространство: обеспечение информационной безопасности и

право. Сб. науч. трудов / под ред. Т. А. Поляковой, В. Б. Наумова, А. В. Минбалеева. М.: ИГП РАН, 2018.

149. Теория государства и права : учебник / [С. С. Алексеев, С. И. Архипов, Е. А. Белканови др.] ; отв. ред. В. Д. Перевалов. — 5-е издание, переработанное и дополненное. — Москва : НОРМА [и др.], 2023. — 552 с.

150. Теория государства и права : учебник / Российский университет дружбы народов, Юридический институт; под ред. д.ю.н., проф. А.А. Клишаса. – М.: Статут, 2019. – 512 с

151. Теория государства и права: учебник для студентов высших учебных заведений, обучающихся по направлению и специальности "Юриспруденция" / Н. И. Матузов, А. В. Малько ; Саратовский филиал ин-та государства и права Российской акад. наук. - Изд. 2-е, перераб. и доп. – М : Юристъ, 2007. – 540 с.

152. Терещенко Л. К. Большие данные в публичной и частной сферах // Информационное право. – 2023. – № 3(77). – С. 4-9.

153. Терещенко Л. К. Влияние цифровой экономики на правовые режимы информации / Л. К. Терещенко, М. В. Якушев // Информационное право. – 2021. – № 2. – С. 4-10.

154. Терещенко Л. К. Государственный контроль в сфере защиты персональных данных / Л. К. Терещенко // Право. Журнал Высшей школы экономики. – 2018. – № 4. – С. 142-161.

155. Трегубов В. Н. Использование информации сотовых операторов в городских транспортных исследованиях // Транспортные системы и технологии. – 2020. – Т. 6, № 2. – С. 20-33.

156. Трофимцева С. Ю. К вопросу об обеспечении защиты персональных данных в России // Сборники конференций НИЦ «Социосфера». 2014. № 63. С. 120-125.

157. Туликов А. В. Обеспечение информационной безопасности как гарантия прав человека // Право. Журнал Высшей школы экономики. – 2015. – № 2. – С. 50-60.

158. Туликов А. В. Обеспечение информационной безопасности как гарантия прав человека // Право. Журнал Высшей школы экономики. – 2015. – № 2. – С. 50-60.

159. Хабриева Т.Я., Черногор Н.Н. Будущее права. Наследие академика В. С. Степина и юридическая наука. М.: Российская академия наук; Институт законодательства и сравнительного правоведения при Правительстве РФ; ИНФРА-М, 2023.

160. Химченко А. И. О создании единого государственного информационного ресурса о населении // Информационное право. – 2020. – № 3. – С. 28-31.

161. Химченко А. И. Правовые режимы персональных данных и их влияние на формирование доверия к цифровой среде // Информационное право. – 2023. – № 4(78). – С. 33-37.

162. Цацулин А. Н., Куприн А. А., Данилова Т. В., Сошников А. В. Потенциал модернизации государственного управления в эпоху цифровизации экономики // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 3: Экономические, гуманитарные и общественные науки. — 2019. — № 1. — С. 9–13.

163. Цифровое право: учебник / А. Дюфло, Л. В. Андреева. В. В. Блажеев [и др.); под общ. ред. В. В. Блажеева. М.А. Егоровой. М.: Проспект, 2020.

164. Чаннов С. Е. Большие данные в государственном управлении: возможности и угрозы // Журнал российского права. – 2018. – № 10(262). – С. 111-122.

165. Чаннов С. Е. Правовые проблемы обработки персональных данных в государственных информационных системах // Информационное право. – 2018. – № 2. – С. 10-13.

166. Чеботарева А. А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе // Юридический мир. — 2016. — № 8. — С. 63–66. - Библиогр.: с. 66 (6 назв.). — ISSN 1811-1475.

167. Человек и системы искусственного интеллекта / под ред. акад. РАН В. А. Лекторского. СПб.: Юридический центр. 2022.

168. Черкасов А. И. Цифровизация местного управления и ее особенности в европейских странах // Сравнительное конституционное обозрение. 2024. № 1 (158). С. 90–109.

169. Чубукова С. Г. Стратегии развития информационного общества и направления развития законодательства// Правовая информатика: теория и опыт. – М.: Научный центр правовой информации при Министерстве юстиции Российской Федерации, 2018, С. 247-252.

170. Чудиновских О. С. К вопросу о создании регистра населения и использовании административных данных для нужд государственной статистики. Вопросы статистики, Т. 28, № 1, стр. 5–17.

171. Шахрай С. М. Цифровая конституция. основные права и свободы личности в тотально информационном обществе // Вестник Российской академии наук. — 2018. — Т. 88, № 12. — С. 1075–1082.

172. Шелудченко И. А. Защита персональных данных в Российской Федерации сквозь призму делегированного правотворчества // Вестник Московского университета. Серия 11: Право. – 2025. – № 1. – С. 77-99.

173. Шинкарецкая Г. Г. Геном человека как объект защиты персональных данных // Информационное право. – 2019. – № 2. – С. 30-34.

174. Amankwah-Amoah J. COVID-19 and digitalization: The great acceleration // Journal of Business Research. — Vol. 2021 — № 136 — P. 602–611.

175. Barrutia J. M. Effect of the COVID-19 pandemic on public managers' attitudes toward digital transformation // Technology in Society —2021 — Vol. 67 — P. 101776.

176. Khan E. M. Comprehensive national security:contemporary discourse // Margalla Papers-2022 (Issue-I) p.1-17.

177. Lee T. Tracing surveillance and auto-regulation in Singapore: «smart» responses to COVID-19 / T. Lee, H. Lee // Media International Australia. — 2020. — Vol. 177 (1). — P. 47–60.

178. Page B. Who deliberates? // Mass media in modern democracy. — Chicago, 1996. — P.5.

179. Posner D. T. on Privacy // International Journal of Applied Philosophy. Vol. 27, № 2(2013), p. 147–160

180. Richards N. M. and Solove D. J., Privacy's Other Path: Recovering the Law of Confidentiality.// Georgetown Law Journal, Vol. 96, p. 123.

181. Rössler, B. The Value of Privacy // Cambridge; Polity Press.

182. Szabo M . D. Kisérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival. // Információs Társadalom 2005-2. p. 46

183. Warren S. D., Brandeis L. D. The Right to Privacy // Harvard Law Review. 1890. Vol.IV. № 5. p.193–220, (пер.: Яндекс-переводчик).

184. Westin A. F.: Social and political dimensions of privacy // Journal of Social Issues Vol 59, No. 2. (2003) p. 431-434.

IV. Иные научно-практические материалы

1. «Сбер» оценил долю утекших данных взрослых россиян в 90% // РБК: [Электронный ресурс]. URL: https://www.rbc.ru/finances/06/11/2024/672b2da59a79470df56c61e7(дата обращения: 20.07.23).

2. 199 лет общественному контролю за тюрьмами: история, проблемы, перспективы. // Блог Андрея Бабушкина: [Электронный ресурс]. URL: https://an-babushkin.livejournal.com/830553.html(дата обращения: 6.07.25).

3. Аналитический отчет 2023 "Система государственного стимулирования использования сервисов искусственного интеллекта в здравоохранении на основе анализа российского и зарубежного опыта", НЦРИИ. // Искусственный интеллект Российской Федерации : [Электронный ресурс]. URL: https://ai.gov.ru/knowledgebase/investitsionnaya-aktivnost/2023_analiticheskiy_otchet_sistema_gosudarstvennogo_stimulirovaniya_ispolyzovaniya_servisov_iskusstvennogo_intellekta_v_zdravoohranenii_na_osnove_analiza_rossiyskogo_i_zarubeghnogo_opyta_ncrii/ (дата обращения: 29.12.23).

4. 72% утечек персональных данных происходят по вине сотрудников // Справочник секретаря : [Электронный ресурс]. URL: https://www.sekretariat.ru/news/214623-72-utechek-personalnyh-dannyh-proishodyat-po-vine-sotrudnikov (дата обращения: 19.12.23).

5. 81% россиян обеспокоены вопросами утечки персональных данных. // CNEWS : [Электронный ресурс]. URL: https://safe.cnews.ru/news/line/2023-10-23_81_rossiyan_obespokoeny_voprosami (дата обращения: 20.07.23).

6. Самые громкие утечки персональных данных за 2022 год в России // vc.ru : [Электронный ресурс]. URL: https://vc.ru/u/1241455-delis-arhiv/494035-samye-gromkie-utechki-personalnyh-dannyh-za-2022-god-v-rossii (дата обращения: 19.10.23).

7. Арялина М. Объем утекших в сеть данных россиян вырос на 70% за год. // Ведомости: [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/articles/2025/01/24/1088050-obem-utekshih-v-set-dannih-rossiyan-viros (дата обращения: 6.07.25).

8. Ашманов: телефонные мошенники похищают у россиян до 1 млрд рублей в день. // ТАСС: [Электронный ресурс]. URL: https://tass.ru/ekonomika/23376231 (дата обращения: 20.07.23).

9. Бардина П. На что повлияет регистр населения России // Ведомости : [Электронный ресурс]. URL: https://www.vedomosti.ru/opinion/articles/2020/06/19/833059-registr-naseleniya-rossii (дата обращения: 18.12.23).

10. Бобрышев Е. Экс-командующий сухопутными войсками РФ и его жена стали жертвами мошенников. // РИАМО: [Электронный ресурс]. URL https://riamo.ru/news/proisshestviya/eks-komandujuschij-suhoputnymi-vojskami-rf-i-ego-zhena-stali-zhertvami-moshennikov/ (дата обращения: 03.07.24).

11. Больше 70% россиян заявили о незащищенности от утечек данных. // РБК : [Электронный ресурс]. URL: https://www.rbc.ru/society/07/09/2021/613722689a79477f426fd451 (дата обращения: 20.07.23).

12. Бундин М. В. Персональные данные в системе информации ограниченного доступа, Специальность: 12.00.13 — информационное право, диссертация на соискание ученой степени кандидата юридических наук, 2017 год, URL: https://izak.ru/upload/iblock/a61/a61916d1bf3c94d110fd287137213345.pdf (дата обращения: 7.10.23).

13. В 2023 году число случаев подделки доверенностей и судебных приказов выросло на 12% // Smart Engines : [Электронный ресурс].URL: https://smartengines.ru/news/report-2023/ (дата обращения: 4.12.23).

14. В МВД заявили о готовности к введению в России электронных паспортов // ИЗВЕСТИЯ : [Электронный ресурс].URL: https://iz.ru/1228574/2021-09-29/v-mvd-zaiavili-o-gotovnosti-k-vvedeniiu-v-rossii-elektronnykh-pasportov (дата обращения: 3.12.23).

15. В Москве создан единый центр биометрических испытаний. // Interfax: [Электронный ресурс]. URL: https://www.interfax.ru/moscow/1012254 (дата обращения: 16.10.23)

16. В Правительстве одобрили компенсации пострадавшим от утечек // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : [Электронный ресурс]. URL: https://digital.gov.ru/ru/events/47423/(дата обращения: 23.12.23).

17. В России могут ввести оборотные штрафы за утечку персональных данных . // КоммерсантЪ : [Электронный ресурс]. URL: https://www.kommersant.ru/doc/5227921 (дата обращения: 19.10.23).

18. В России разработали нейросеть, выявляющую террористов среди мигрантов. // РИА Новости : [Электронный ресурс]. URL: https://ria.ru/20240413/neyroset-1939738693.html (дата обращения: 12.07.24).

19. В РФ за 10 дней совершили более 40 поджогов и взрывов из-за мошенников. // ТАСС : [Электронный ресурс]. URL: https://tass.ru/proisshestviya/22773923 (дата обращения: 20.07.23).

20. В Сбербанке крупнейшая утечка в истории российского банковского сектора. // Cnews : [Электронный ресурс]. URL:

https://www.cnews.ru/news/top/2019-10-03_sberbank_dopustil_krupnejshuyu (дата обращения: 19.10.23).

21. Валагин.А. NI: Заказы в пиццериях у Пентагона позволяют предсказывать войны. // Российская газета : [Электронный ресурс]. URL: https://rg.ru/2025/06/23/ni-zakazy-v-picceriiah-u-pentagona-pozvoliaiut-predskazyvat-vojny.html

22. Вступительное слово на расширенном заседании Правительства с участием глав субъектов Российской Федерации. // Президент России: [Электронный ресурс]. URL: http://www.kremlin.ru/events/president/transcripts/22592 (дата обращения: 6.07.25).

23. Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации. // Совет Безопасности Российской Федерации : [Электронный ресурс]. URL: http://www.scrf.gov.ru/security/information/document155/ (дата обращения: 20.07.23).

24. Глоссарий понятий и терминов, используемых в исследовании проблем декартелизации экономики, включая ее цифровой сегмент. // ИПРАН РАН: [Электронный ресурс]. URL: https://www.issras.ru/competition/glcon_a.php (дата обращения: 25.11.23).

25. Госдума приняла закон о едином регистре сведений о населении России. // ТАСС. URL: https://tass.ru/obschestvo/8527939 (дата обращения: 5.10.23).

26. ГОСТ Р ИСО/МЭК 20546-2021 // Федеральное агентство по техническому регулированию и метрологии : [Электронный ресурс]. URL: https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=4&month=4&year=-1&search=&id=240981 (дата обращения: 16.05.25).

27. Государство создаёт Единый регистр сведений о населении // Аргументы недели: [Электронный ресурс]. URL: https://yandex.ru/turbo/argumenti.ru/s/society/2023/09/858360 (дата обращения: 11.12.23).

28. Гражданский кодекс Китая 中国民法典 // Наблюдатель за правосудием Китая: [Электронный ресурс]. URL: https://ru.chinajusticeobserver.com/t/china-civil-code(дата обращения: 17.11.23).

29. Деловые объединения РФ предлагают доработать законопроект об оборотных штрафах за утечку ПДн, отсрочить его вступление // Деловая Россия : [Электронный ресурс]. URL: https://deloros.ru/press-centr/publikacii/delovye-obedineniya-rf-predlagayut-dorabotat-zakonoproekt-ob-oborotnykh-shtrafakh-za-utechku-pdn-ots/ (дата обращения: 23.12.23).

30. Единая биометрическая система. // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : [Электронный ресурс]. URL: https://digital.gov.ru/ru/activity/directions/802/?utm_referrer=https%3a%2f%2fwww.google.com%2f (дата обращения: 11.10.23)

31. Единый регистр сведений о населении РФ не будет содержать биометрических данных. // ТАСС : [Электронный ресурс]. URL: https://tass.ru/obschestvo/8657699(дата обращения: 11.10.23).

32. Есть ли шанс у цифровой идентификации в России. // EY Russia : [Электронный ресурс]. URL: https://www.ey.com/Publication/vwLUAssets/ey-digital-id-survey-rus/$FILE/ey-digital-id-survey-rus.pdf (дата обращения: 28.11.23).

33. Жертвы GDPR: кто уже прекратил работу из-за нового регулирования персональных данных // Habr : [Электронный ресурс].URL: https://habr.com/en/company/it-grad/blog/418501/ (дата обращения: 5.11.23).

34. Закон о едином регистре населения окончательно принят Госдумой // РОСБАЛТ : [Электронный ресурс]. URL: https://www.rosbalt.ru/russia/2020/05/21/1844581.html (дата обращения: 19.12.23).

35. Законопроект № 571124-7 // Система обеспечения законодательной деятельности : [Электронный ресурс]. URL: https://sozd.duma.gov.ru/bill/571124-7 (дата обращения: 22.06.25).

36. Законопроект № 571124-7 Статья 1, п.2. стр. 3 // Система обеспечения законодательной деятельности: [Электронный ресурс]. URL: https://sozd.duma.gov.ru/bill/571124-7 (дата обращения: 19.06.25).

37. Злоупотребление должностными полномочиями — самые громкие приговоры 2023 года // Адвокат Саркисов : [Электронный ресурс]. URL: https://www.advokat-sarkisov.ru/blog/zloupotreblenie-dolzhnostnymi-polnomochiyami-samye-gromkie-prigovory-2023-goda.html (дата обращения: 5.06.25).

38. Зорькин: Задача государства — признавать и защищать цифровые права граждан // Российская газета : [Электронный ресурс]. URL: https://rg.ru/2018/05/29/zorkin-zadacha-gosudarstva-priznavat-i-zashchishchat-cifrovye-prava-grazhdan.html (дата обращения: 1.10.23).

39. Иванова В. По статье «диверсия» // Гудок : [Электронный ресурс]. URL https://gudok.ru/zdr/173/?ID=1637772 (дата обращения: 28.12.23).

40. Искусственный интеллект становится искусным поставщиком услуг. // Ведомости.Капитал : [Электронный ресурс]. URL: https://www.vedomosti.ru/kapital/trends/articles/2024/07/24/1051936-iskusstvennii-intellekt-stanovitsya-iskusnim-postavschikom-uslug (дата обращения: 29.12.23).

41. Использование больших данных в финансовом секторе и риски финансовой стабильности. // ЦБ РФ. URL: https://cbr.ru/Content/Document/File/131359/Consultation_Paper_10122021.pdf (дата обращения: 18.06.25).

42. Использование персональных данных в маркетинге: законы и этика // РБК Тренды : [Электронный ресурс] URL: https://trends.rbc.ru/trends/industry/615fdf6f9a794719ca4d1ddc (дата обращения: 1.10.23).

43. Как запретить брокерам данных продажу своей личной информацию // Лаборатория Касперского : [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-stop-data-brokers-from-selling-your-personal-information (дата обращения: 29.12.23).

44. Как изменится закон о персональных данных с 1 сентября 2022 года// Контур : [Электронный ресурс]. URL: https://kontur.ru/articles/1000 (дата обращения: 21.12.23).

45. Как найти аккаунты и личные данные человека в сети Деанон по открытым источникам // Вастрик Блог : [Электронный ресурс]URL: https://vas3k.blog/blog/389/ (дата обращения: 7.10.23).

46. Как трансформировались «сквозные технологии». // КоммерсантЪ : [Электронный ресурс]. URL: https://www.kommersant.ru/doc/5925906 (дата обращения: 27.06.25).

47. Как ужесточились требования к работе с персональными данными в 2021 году // Контур : [Электронный ресурс]. URL: https://kontur.ru/articles/4816 (дата обращения: 21.12.23).

48. Капранов О. В. России прошла целая серия утечек персональных данных // Российская газета : [Электронный ресурс]. URL: https://rg.ru/2022/10/03/so-vzlomom-napereves.html (дата обращения: 19.12.23).

49. Китайскому eCommerce прогнозируют опережающий рост. // ShopifyBlog : [Электронный ресурс]. URL: https://e-pepper.ru/news/kitayskomu-ecommerce-prognoziruyut-operezhayushchiy-rost.html (дата обращения: 13.11.23)

50. Количество слитых персональных данных в 2024 году выросло на треть. // сайт компании Infowatch : [Электронный ресурс]. URL: https://www.infowatch.ru/company/presscenter/news/kolichestvo-slitykh-personalnykh-dannykh-v-dve-tysyachi-dvadtsat-chetvertom-godu-vyroslo-na-tret(дата обращения: 20.07.23).

51. Коллегия Минсвязи России рассмотрела проект Концепции создания автоматизированной системы «Государственный регистр населения (АС ГРН)» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : [Электронный ресурс]. URL: https://digital.gov.ru/ru/events/1513/ (дата обращения: 11.12.23).

52. Кто что знает обо мне: обработка персональных данных онлайн-платформами. // портал Гарант.ру : [Электронный ресурс]. URL: https://www.garant.ru/news/1446555/ (дата обращения: 6.07.25).

53. Кузнецов М. Эффект зловещей долины: как распознать дипфейк и не дать себя обмануть. // FORBES : [Электронный ресурс]. URL: https://www.forbes.ru/finansy/439601-effekt-zlovesej-doliny-kak-raspoznat-dipfejk-i-ne-dat-seba-obmanut (дата обращения: 03.03.24).

54. Латухина К. Владимир Путин: Внедрить цифровые технологии во все сферы жизни. // Российская газета : [Электронный ресурс]. URL: https://rg.ru/2017/06/04/reg-szfo/vladimir-putin-vnedrit-cifrovye-tehnologii-vo-vse-sfery-zhizni.html (дата обращения: 4.10.23).

55. Метёлкин П. Правовое регулирование искусственного интеллекта. // Журнал "Системы безопасности" : [Электронный ресурс]. URL: https://www.secuteck.ru/articles/pravovoe-regulirovanie-iskusstvennogo-intellekta (дата обращения: 6.07.25).

56. Минцифры заморозило проект электронного паспорта на неопределенный срок // ТАСС : [Электронный ресурс]. URL: https://tass.ru/obschestvo/14885335 (дата обращения: 1.12.23).

57. Минцифры заявило о ежемесячном расчете показателя информбезопасности чиновников // ТАСС : [Электронный ресурс]. URL: https://tass.ru/ekonomika/18566019 (дата обращения: 26.11.23).

58. Минцифры предложило разрешить использовать приложение «Госуслуг» вместо паспорта // Ведомости : [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/news/2023/04/13/970836-mintsifri-predlozhilo-razreshit (дата обращения: 3.12.23).

59. Минцифры согласилось не вводить штрафы для бизнеса за первый факт утечки персональных данных // RB.RU : [Электронный ресурс]. — URL: https://rb.ru/news/leak-law/ (дата обращения: 19.10.23).

60. Морозова А. МВД сообщило о массовых звонках с предложением поджечь военкомат. // Ведомости : [Электронный ресурс]. URL:

https://www.vedomosti.ru/politics/articles/2023/08/08/989026-mvd-o-massovih-zvonkah-s-predlozheniem-podzhech-voenkomat (дата обращения: 20.07.23).

61. Мошенники обманывают людей с помощью дипфейков. // Центральный Банк России : [Электронный ресурс]. URL: https://cbr.ru/information_security/pmp/15082024/ (дата обращения: 03.03.24).

62. Мошенники убедили россиянку отдать им 750 тысяч рублей и поджечь гостиницу. // Газета.ру : [Электронный ресурс]. URL https://www.gazeta.ru/social/news/2023/11/02/21630997.shtml (дата обращения: 28.12.23)

63. Национальный проект «Экономика данных и цифровая трансформация государства». Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : [Электронный ресурс]. URL: https://digital.gov.ru/target/naczionalnyj-proekt-ekonomika-dannyh-i-czifrovaya-transformacziya-gosudarstva (дата обращения: 03.10.25)

64. Нейросеть в городе: как исскуственный интеллект помогает москвичам. // Ведомости : [Электронный ресурс]. Город. URL: https://www.vedomosti.ru/gorod/ourcity/articles/neiroset-v-gorode-kak-iskusstvennii-intellekt-pomogaet-moskvicham (дата обращения: 29.12.23).

65. Нормативное обеспечение стратегического планирования // Минэкономразвития РФ : [Электронный ресурс]. URL: https://www.economy.gov.ru/material/directions/strateg_planirovanie/normativnoe_obespechenie_strategicheskogo_planirovaniya/ (дата обращения: 27.12.23).

66. Нормативное регулирование цифровой среды. // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : [Электронный ресурс]. URL: https://digital.gov.ru/ru/activity/directions/862/ (дата обращения: 6.12.23).

67. Нормативное регулирование цифровой среды. // Министерство экономического развития Российской Федерации : [Электронный ресурс]. URL: https://www.economy.gov.ru/material/directions/gosudarstvennoe_upravlenie/normativnoe_regulirovanie_cifrovoy_sredy/ (дата обращения: 5.10.23).

68. Обзор технологий создания Deepfake и методов его выявления. // ФГУП «ГРЧЦ : [Электронный ресурс]. URL: https://rdc.grfc.ru/2020/06/research-deepfake/ (дата обращения: 03.03.24).

69. Общественный контроль в тюрьмах: реальность и перспективы. // Общественная палата Российской Федерации: [Электронный ресурс]. URL: https://www.oprf.ru/news/obshchestvennyy-kontrol-v-tyurmakh-realnost-i-perspektivy (дата обращения: 6.07.25).

70. Общественный контроль за работой органов и учреждений уголовно-исполнительной системы со стороны гражданского общества. // Прокуратура Владимирской области: [Электронный ресурс]. URL: https://epp.genproc.gov.ru/ru/web/proc_33/activity/legal-education/explain?item=23019822 (дата обращения: 6.07.25).

71. Общие положения гражданского права КНР. // Законодательство Китая : [Электронный ресурс]. URL: https://chinalawinfo.ru/civil_law/general_principles_civil_law(дата обращения: 15.11.23).

72. Объем слитых персональных данных в РФ вырос на 60 процентов. // INFOWATCH: [Электронный ресурс].URL: https://www.infowatch.ru/company/presscenter/news/obyem-slitykh-personalnykh-dannykh-v-rf-vyros-na-shestdesyat-protsentov (дата обращения: 6.07.25).

73. Объём утечек персональных данных россиян в 2022 году вырос в 40 раз по отношению к 2021 году, демонстрирует отчёт компании Group-IB. // Хабр: [Электронный ресурс]. URL:https://habr.com/ru/news/712488/ (дата обращения: 6.07.25).

74. Определение больших данных. // Сайт корпорации Amazon : [Электронный ресурс]. URL: https://aws.amazon.com/ru/big-data/what-is-big-data/ (дата обращения: 20.06.25).

75. Опубликован паспорт национальной программы «Цифровая экономика Российской Федерации». // Официальный сайт Правительства Российской

Федерации : [Электронный ресурс]. URL: http://government.ru/info/35568/ (дата обращения: 4.10.23).

76. Основной закон для Федеративной Республики Германия (Grundgesetz für die Bundesrepublik Deutschland) от 23.05.1949 23.05.1949 г. — с изм. и допол. в ред. от 19.12.2022. // Федеральный центр политического просвещения : [Электронный ресурс]. URL: http://www.recht-harmonisch.de/GG-russisch.pdf (дата обращения: 21.09.23).

77. Послание Федеральному Собранию Российской Федерации. 26 мая 2004 года // Президент России : [Электронный ресурс]. URL: http://archive.kremlin.ru/text/appears/2004/05/71501.shtml (дата обращения: 6.07.25).

78. Правительственная комиссия по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности. // Правительство России : [Электронный ресурс]. URL: http://government.ru/department/492/about/ (дата обращения: 6.12.23).

79. Правительство отклонило законопроект Минкомсвязи о больших данных». // Сайт газеты Ведомости : [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/articles/2020/03/27/826513-pravitelstvo-otklonilo-zakonoproekt (дата обращения: 27.06.25).

80. Право на неприкосновенность частной жизни в цифровой век. Доклад Верховного комиссара Организации Объединенных Наций по правам человека (A/HRC/39/29) // Сайт ООН : [Электронный ресурс]. URL:https://documents.un.org/doc/undoc/gen/g18/239/60/pdf/g1823960.pdf? (дата обращения: 29.12.23).

81. Применение электронной подписи // ФНС России : [Электронный ресурс]. URL: https://www.nalog.gov.ru/rn77/related_activities/el_doc/use_electronic_sign/. (дата обращения: 9.08.2023).

82. Принят закон об электронных досье на жителей России. // HABR URL: https://habr.com/ru/news/503256/ (дата обращения: 18.12.23).

83. Прозорова М. Гражданский кодекс Китая и защита персональных данных // Worldbussineslaw : [Электронный ресурс].URL: https://worldbiz.ru/analytics/Grazhdanskii-kodeks-Kitaia-i-zaschita-personalnykh-dannykh (дата обращения: 17.11.23).

84. Профайлинг представляет собой совокупность психологических методов оценки и прогнозирования поведения человека на основе анализа его наиболее информативных частных признаков, характеристик внешности, вербального и невербального поведения (Вереникина Н. А. Профайлинг как средство раскрытия и расследования преступлений // Актуальные проблемы российского права. – 2017. – № 9(82). – С. 203-209).

85. Путин: Россия ускорит внедрение цифровых технологий // Вести.RU : [Электронный ресурс]. URL: https://www.vestifinance.ru/articles/86338 (дата обращения: 17.11.23).

86. Разбираемся в приказе ФСТЭК России № 77 // ГК ЦИБИТ : [Электронный ресурс]. URL: https://www.cibit.ru/stati-ekspertov/razbirayemsya-v-prikaze-fstek-rossii77/ (дата обращения: 27.10.23).

87. Развитие методов анализа социальных явлений с использованием больших данных соцсетей. // ВШССН МГУ : [Электронный ресурс]. URL: https://nosh.msu.ru/math/tpost/zxkjfmab31-razvitie-metodov-analiza-sotsialnih-yavl(дата обращения: 12.07.24).

88. Раздьяконов Е. С. Поиск персональных данных в неструктурированных текстах с использованием нейронных сетей. // Инженерный вестник Дона, №7 (2023) : [Электронный ресурс]. URL: http://ivdon.ru/uploads/article/pdf/IVD_86__6y23_razdyakonov.pdf_47d75621b4.pdf (дата обращения: 29.12.23).

89. Раскрытие искусственного интеллекта: 10 шагов для защиты прав человека // Council of Europe : [Электронный ресурс]. URL: https://rm.coe.int/-10-/16809a42e4 (дата обращения: 12.07.24).

90. Распознавание отпечатков пальцев. // Национальная библиотека им. Н. Э. Баумана : [Электронный ресурс]. Электронный ресурс URL: https://ru.bmstu.wiki/Распознавание_отпечатков_пальцев (дата обращения: 1.12.23).

91. Расследование: как обезличенные данные становятся персональными и продаются на сторону. // ХАБР : [Электронный ресурс]. URL: https://habr.com/ru/post/518458/ (дата обращения: 18.06.25).

92. Регулирование данных в Российской Федерации: текущее состояние, проблемы, перспективы // НИУ ВШЭ: [Электронный ресурс]. URL: https://www.hse.ru/mirror/pubs/share/480910412.pdf.

93. Решение профильного комитета (Комитет Государственной Думы по информационной политике, информационным технологиям и связи). // Система обеспечения законодательной деятельности : [Электронный ресурс].. URL: https://sozd.duma.gov.ru/download/C9C4EF85-CACE-4956-8C21-FFDF8EFCE15D (дата обращения: 22.06.25).

94. Роскомнадзор сообщил о росте утечек данных в четыре раза в I полугодии// ТАСС : [Электронный ресурс]. URL: https://tass.ru/obschestvo/18333157 (дата обращения: 28.12.23).

95. Руководство по применению статьи 8 Европейской конвенции по правам человека. // European Court of Human Rights : [Электронный ресурс]. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_rus (дата обращения: 07.20.23).

96. Сапожников А. Россия опустилась на 137-е место в рейтинге восприятия коррупции. // КоммерсантЪ : [Электронный ресурс]. URL: https://www.kommersant.ru/doc/5797806 (дата обращения: 5.07.25).

97. Слагаемые успеха: технологии умного города. // CNEWS : [Электронный ресурс]. URL: http://smartcity.cnews.ru/articles/2018-08-09_slagaemye_uspeha_tehnologii_umnogo_goroda (дата обращения: 16.05.25).

98. Соловьёва О. Россияне не доверяют государству свои лица и голоса. // Независимая газета : [Электронный ресурс] URL:

https://www.ng.ru/economics/2023-07-05/1_8765_biometrics.html (дата обращения: 20.07.23).

99. Список изменений в Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) «О персональных данных». // Закон РФ : [Электронный ресурс]. URL: https://www.zakonrf.info/izmeneniya-v-zakonodatelstve/izmenenie-zakon-o-personalnyh-dannyh/(дата обращения: 20.07.23).

100. Степанова Ю. Абонентов загрузили на сервер // КоммерсантЪ : [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4986542(дата обращения: 19.10.23).

101. Страшное лицо больших данных. // Сайт Лаборатории Касперского : [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/scary-big-data/8676/ (дата обращения: 27.06.25).

102. Токарев А. Телефон вместо почты: как развивается авторизация через мобильный ID // РБК : [Электронный ресурс].Тренды URL: https://trends.rbc.ru/trends/industry/cmrm/62cea5f69a79478c4a42cd63 (дата обращения: 7.10.23).

103. Тотальная слежка: как устроен рынок торговли пользовательскими данными: [Электронный ресурс] // РБК. URL: https://www.rbc.ru/magazine/2018/04/5aafdfc99a7947654297214d (дата обращения: 1.10.23)

104. Утечка данных с сервера ОФД «Дримкас» оказалась масштабнее, чем предполагалось ранее // SecurityLab.ru : [Электронный ресурс]. URL: https://www.securitylab.ru/news/501312.php(дата обращения: 19.10.23).

105. Утечки возьмут в оборот. // КоммерсантЪ : [Электронный ресурс]. URL: https://www.kommersant.ru/doc/5379590 (дата обращения: 19.10.23).

106. Утечки информации ограниченного доступа в мире и России, первое полугодие 2023 г. // INFOWATCH : [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-mire-i-rossii-za-pervoe-polugodie-2023-goda.pdf (дата обращения: 18.12.23).

107. Утечки информации ограниченного доступа в России за 2022 год // InfoWatch: [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-god (дата обращения: 21.11.2023).

108. Фроленко В. На Урале зафиксировали случаи принуждения жертв мошенников к поджогам военкоматов. // ТАСС. URL: https://tass.ru/proisshestviya/17567183 (дата обращения: 1.12.23).

109. Фролова М. Рост на 700%: мошенники стали чаще использовать дипфейки в сфере финансов. // Известия : [Электронный ресурс]. URL: https://iz.ru/1679621/mariia-frolova/rost-na-700-moshenniki-stali-chashche-ispolzovat-dipfeiki-v-sfere-finansov (дата обращения: 03.03.24).

110. Хакеры взломали сайт МосгорБТИ // Forbes : [Электронный ресурс]. URL: https://www.forbes.ru/tekhnologii/494123-hakery-vzlomali-sajt-mosgorbti (дата обращения: 28.12.23).

111. Хакеры провели инвентаризацию // КОММЕРСАНТ : [Электронный ресурс]. URL: https://www.kommersant.ru/doc/6147895?ysclid=llgwmtxzp9332474382 (дата обращения: 28.12.23).

112. Цифровой профиль гражданина — что известно на сегодняшний день. // Экспертный центр электронного государства: [Электронный ресурс]. URL:https://d-russia.ru/tsifrovoj-profil-grazhdanina-chto-izvestno-na-segodnyashnij-den.html (дата обращения: 5.10.23).

113. Чернышева. Е. Россияне сдали мошенникам рекордные ₽14 млрд.// РБК: [Электронный ресурс]. URL: https://www.rbc.ru/newspaper/2023/02/15/63eb5da89a794701b759621f (дата обращения: 28.12.23).

114. Что изменится в работе с персональными данными с 1 марта 2023 года // Контур: [Электронный ресурс]. URL: https://kontur.ru/articles/1478 (дата обращения: 21.12.23).

115. Что такое Big Data — большие данные. // Сайт корпорации Oracle : [Электронный ресурс]. URL: https://www.oracle.com/ru/big-data/what-is-big-data/ (дата обращения: 12.06.25).

116. Что такое Big data. // Rusbase : [Электронный ресурс] URL: https://rb.ru/howto/chto-takoe-big-data/ (дата обращения: 16.06.25).

117. Что такое big data: зачем нужны большие данные, как их собирают и обрабатывают. // Журнал Mail.ru : [Электронный ресурс]. “Cloud Solutions об IT-бизнесе, технологиях и цифровой трансформации”. URL: https://mcs.mail.ru/blog/big-data-vse-govoryat-no-malo-kto-shchupal (дата обращения: 16.06.25).

118. Что такое единый регистр сведений о населении и зачем он необходим // Государственная Дума Федерального Собрания Российской Федерации: [Электронный ресурс]. URL: http://duma.gov.ru/news/53118/ (дата обращения: 15.12.23).

119. Что такое поведенческая биометрия и кто применяет её на российском рынке. // Рамблер.Новости : [Электронный ресурс]. URL: https://news.rambler.ru/other/41803543-chto-takoe-povedencheskaya-biometriya-i-kto-primenyaet-ee-na-rossiyskom-rynke/ (дата обращения: 9.10.23).

120. Что такое цифровой след? // АО «Лаборатория Касперского» : [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/definitions/what-is-a-digital-footprint (дата обращения: 25.11.23).

121. Эксперты рассказали о рисках централизованной системы хранения данных. // Рамблер-финансы : [Электронный ресурс].. URL: https://finance.rambler.ru/other/43154312-eksperty-rasskazali-o-riskah-tsentralizovannoy-sistemy-hraneniya-dannyh/ (дата обращения: 18.12.23).

122. Электронный паспорт гражданина РФ. // Комсомольская правда : [Электронный ресурс]. URL: https://www.kp.ru/putevoditel/zakony/ehlektronnyj-pasport-grazhdanina-rf/ (дата обращения: 5.10.23).

123. AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data. // The Economic Times : [Электронный ресурс]. URL

¨https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms?from=mdr (дата обращения: 29.12.23).

124. AI Enables Data Brokers to Create “Detailed Dossiers” // AI in Business : [Электронный ресурс]. URL: https://aiinbusiness.substack.com/p/ai-enables-data-brokers-to-create (дата обращения: 29.12.23).

125. Artificial intelligence risks to privacy demand urgent action – Bachelet // ООН, Офис Верховного комиссара по правам человека : [Электронный ресурс]. URL: https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet?LangID=E&NewsID=27469 (дата обращения: 03.07.24).

126. Bernhardt G. Global Ecommerce Sales Growth Report for 2020–2025. // Shopify Blog : [Электронный ресурс]. URL: https://www.shopify.com/blog/global-ecommerce-sales(дата обращения: 13.11.23)

127. Big Data: что это такое простыми словами — характеристики технологии больших данных и методы их обработки. // Cleverence: [Электронный ресурс]. URL: https://www.cleverence.ru/articles/auto-busines/big-data-chto-eto-takoe-prostymi-slovami-kharakteristiki-tekhnologii-bolshikh-dannykh-i-metody-ikh-o/ (дата обращения: 25.06.25)

128. Brokeš F. Russia’s Sovereign Internet // Central European Financial Observer. 2018 : [Электронный ресурс] URL: https://financialobserver.eu/cse-and-cis/russias-sovereign-internet/ (дата обращения: 26.11.23)

129. China passes new cybersecurity law. // Covingon & Burling LLC : [Электронный ресурс]. URL: https://www.cov.com/-/media/files/corporate/publications/2016/11/china_passes_new_cybersecurity_law.pdf (дата обращения: 9.11.23).

130. ChinaCybersecurityLaw // D-russia.ru. URL:https://d-russia.ru/wp-content/uploads/2017/04/China-Cybersecurity-Law.pdf (дата обращения: 17.11.23).

131. Deadline Passes on T-Mobile's $350 Million Settlement Days After Another Data Breach. // CNET : [Электронный ресурс]. URL:

https://www.cnet.com/personal-finance/deadline-passes-on-t-mobiles-350-million-settlement-days-after-another-data-breach/ (дата обращения: 21.12.23).

132. EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). // EDPИ : [Электронный ресурс]. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en (дата обращения: 12.07.24).

133. Moser-Plautz B. COVID-19 and digitalization: The great acceleration. // Sciencedirect : [Электронный ресурс]. URL: https://www.sciencedirect.com/science/article/pii/S0148296321005725 (дата обращения: 9.08.2023).

134. The computer matching and privacy protection act // IRS : [Электронный ресурс]. URL: https://www.irs.gov/irm/part11/irm_11-003-039 (дата обращения: 5.11.23).

135. Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021) // DigiChina. URL: https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ (дата обращения: 17.11.23).

136. Watchdog Poland. // Citizens Network Watchdog Poland : [Электронный ресурс].URL: https://siecobywatelska.pl/?lang=en (дата обращения: 6.07.25).

137. What is Synthetic Identity Fraud? // Credit and Fraud Risk Solutions & Analitics — ID Analytics: [Электронный ресурс]. URL: https://www.idanalytics.com/solutions-services/fraud-risk-management/synthetic-identity-fraud/ (дата обращения: 1.12.23).