Алексеева Кристина Александровна
магистрант
Научный руководитель
Фастова Марина Андреевна
канд. юрид. наук, доцент
ФГБОУ ВО «Российский государственный социальный университет»
г. Москва

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ СИСТЕМАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ВЫЗОВЫ И ПЕРСПЕКТИВЫ

Аннотация: *в статье рассматриваются актуальные проблемы правового регулирования обработки персональных данных с использованием систем искусственного интеллекта (далее – ИИ) в условиях цифровизации публичного и частного секторов. Анализируются ключевые риски для прав субъектов персональных данных: непрозрачность алгоритмических решений, расширение масштабов профилирования, смещение целей обработки, рост вероятности дискриминации, сложности реализации прав на доступ, исправление и удаление данных, а также вопросы распределения ответственности между оператором, разработчиком и поставщиком ИИ-решений. Особое внимание уделяется соотношению общих норм законодательства о персональных данных и специальных требований к высокорисковым ИИ-системам, формирующихся в зарубежных правопорядках, прежде всего в Европейском союзе. Обосновывается необходимость комплексного подхода, сочетающего риск-ориентированное регулирование, усиление требований к качеству данных и управлению жизненным циклом моделей, документирование и аудит, механизмы объяснимости и оценку воздействия на права и свободы человека. Предлагаются направления совершенствования российского регулирования: уточнение правил о профилировании и автоматизированном принятии решений, закрепление требований к прозрачности и*

прослеживаемости алгоритмов, развитие практики DPIA-подобных оценок, а также внедрение стандартов и сертификации в сфере ИИ при сохранении технологической нейтральности законодательства.

Ключевые слова: *персональные данные, искусственный интеллект, профилирование, дискриминация, прозрачность алгоритмов, ответственность, оценка воздействия.*

Общие основы правового режима персональных данных при использовании ИИ.

Трансформация цифровой экономики обусловила переход от традиционных способов обработки персональных данных к интенсивному использованию интеллектуальных технологий, способных осуществлять прогнозирование, классификацию, ранжирование и принятие решений в отношении физических лиц [6, с. 54]. Системы искусственного интеллекта, включая машинное обучение и иные методы анализа больших массивов данных, выступают не только инструментом повышения эффективности управления и оказания услуг, но и источником новых правовых рисков, связанных с изменением природы обработки: возрастают масштабы и скорость обработки, усложняются технологические цепочки, усиливается зависимость результата от качества обучающих данных и архитектуры модели [3, с. 310]. В таких условиях традиционные конструкции законодательства о персональных данных испытывают нагрузку, поскольку многие гарантии прав субъектов строились с расчетом на преимущественно «понятные» и проверяемые процедуры обработки, тогда как ИИ-решения зачастую характеризуются ограниченной объяснимостью, вероятностным характером вывода и распределенностью ответственности между участниками жизненного цикла системы.

В России базовые требования к обработке персональных данных закреплены в Федеральном законе от 27.07.2006 №152-ФЗ «О персональных данных» [2], который устанавливает принципы законности, справедливости, соразмерности целей, минимизации данных, ограничения хранения и обеспечения

безопасности. Указанные принципы формально технологически нейтральны и применимы к обработке с использованием ИИ. Однако при внедрении ИИ проявляются специфические проблемы правоприменения: во-первых, усложняется идентификация цели и правового основания обработки в условиях вторичного использования данных для обучения моделей и последующего дообучения; во-вторых, возникает риск «смещения цели» и фактического расширения состава обрабатываемых сведений за счет производных данных и выводов, формируемых алгоритмами; в-третьих, повышается вероятность несоответствия принципу точности, поскольку данные и модели подвержены дрейфу, а ошибки обучения могут приводить к систематическим искажениям.

Ключевые вызовы: профилирование, непрозрачность, дискриминация, безопасность и ответственность.

Существенным вызовом является профилирование и автоматизированное принятие решений [11, с. 10]. Хотя российское законодательство содержит ограничения на принятие решений, порождающих юридические последствия, исключительно на основе автоматизированной обработки (при наличии условий и исключений), практические сценарии ИИ часто строятся как «человек в контуре» формально, но по существу решение определяется рекомендацией системы. При таком дизайне возрастает риск обхода гарантий: лицо получает отказ в услуге или неблагоприятный рейтинг, но оператор заявляет, что решение принял сотрудник, не предоставляя эффективных механизмов проверки влияния алгоритма. Следовательно, перспективным направлением является нормативное и методическое уточнение критериев «существенного влияния» автоматизированной обработки на итоговое решение, а также введение обязанностей по фиксации роли системы ИИ в процессе принятия решений (журналы событий, протоколы, карточки модели), что позволит обеспечить доказуемость соблюдения требований закона и реальность права на оспаривание.

Непрозрачность алгоритмических моделей формирует системный конфликт между интересами инноваций и правом на информированность [7, с. 56]. В классических моделях обработки субъект персональных данных может получить

сведения о составе данных, целях, сроках и способах обработки. В ИИ-контуре требуется более сложный уровень прозрачности: необходимо раскрывать не только формальные сведения об операторе и цели, но и сведения о логике обработки, категориях используемых данных, источниках обучающих выборок, критериях ранжирования, а также о факторах, существенно повлиявших на результат в конкретном случае [12, с. 105]. При этом следует учитывать баланс с охраной коммерческой тайны и безопасностью, поскольку чрезмерное раскрытие может облегчить злоупотребления (например, «обход» скоринговых моделей). В качестве компромисса представляется обоснованным развитие подходов к объяснимости в формате «понятных причин» решения и «проверяемых процедур» разработки и тестирования модели, а также закрепление права на получение значимой информации о применении ИИ и об основаниях неблагоприятного решения без раскрытия исходного кода.

Отдельное измерение проблемы связано с качеством данных и недискриминацией. ИИ-системы способны воспроизводить и усиливать предвзятость, содержащуюся в исторических данных, что приводит к различиям в доступе к услугам, кредитам, трудоустройству и социальным гарантиям. В российском праве запрет дискриминации закреплен на конституционном уровне и в отраслевом законодательстве, однако механизмы выявления алгоритмической дискриминации остаются недостаточно разработанными [8, с. 72]. Для повышения эффективности защиты прав требуется институционализация процедур оценки рисков дискриминации: тестирование моделей на репрезентативных выборках, мониторинг показателей справедливости, анализ прокси-признаков, которые косвенно кодируют чувствительные характеристики. В правовом плане это может выражаться в обязанности операторов проводить оценку воздействия на права и свободы при использовании ИИ в высокорисковых сферах (кредитование, труд, образование, здравоохранение, публичные услуги), а также в расширении компетенций надзорного органа по проверке алгоритмических систем на предмет соблюдения принципов недискриминации и соразмерности.

Вопрос распределения ответственности при обработке персональных данных системами ИИ осложняется множественностью участников: оператор данных, заказчик решения, разработчик модели, поставщик облачной инфраструктуры, провайдер данных, а также организации, выполняющие разметку и подготовку наборов данных. Российская модель ответственности преимущественно ориентирована на оператора как на лицо, определяющее цели и состав обработки, однако в ИИ-цепочке фактическая возможность влиять на параметры обработки может быть распределена. Перспективным является развитие договорных и деликтных конструкций, обеспечивающих регресс и распределение рисков, а также закрепление минимальных требований к документации и управлению жизненным циклом модели, позволяющих установить причинно-следственную связь между дефектом данных/модели и нарушением прав субъектов. При этом важно избегать размывания ответственности: для субъектов персональных данных должен сохраняться понятный адресат требований – оператор, а внутреннее распределение рисков должно решаться между участниками рынка на основе контрактов, стандартов и страховых механизмов [5, с. 63].

Особую значимость имеет обеспечение безопасности персональных данных в условиях ИИ. Помимо традиционных угроз несанкционированного доступа и утечек, возникают специфические угрозы: извлечение данных из модели, восстановление элементов обучающей выборки, атаки с отравлением данных, подмена входных данных для манипулирования результатом. Следовательно, меры защиты должны учитывать не только информационную безопасность инфраструктуры, но и безопасность модели как объекта, включая контроль доступа к весам модели, аудит тренировочных данных, мониторинг аномалий, а также применение методов приватности (дифференциальная приватность, федеративное обучение, минимизация логирования). С правовой точки зрения это требует уточнения перечней организационных и технических мер с учетом специфики ИИ, развития подзаконного регулирования и стандартов, а также внедрения обязательного документирования принятых мер и результатов тестирования.

Перспективы развития регулирования: риск-ориентированный подход, комплаенс и стандартизация.

Сравнительно-правовой анализ показывает, что в Европейском союзе складывается двухконтурная модель: общий режим защиты данных дополняется специальным регулированием ИИ на основе риск-ориентированного подхода. Такой подход представляется методологически значимым, поскольку позволяет не «переписывать» персональные данные под ИИ, а вводить дополнительный слой требований для высокорисковых ИИ-систем: управление рисками, качество данных, техническая документация, ведение логов, прозрачность, человеческий надзор, устойчивость и кибербезопасность [9, с. 245]. Для российского правопорядка перспективным является заимствование логики риск-ориентированности при сохранении национальных особенностей: целесообразно разграничивать ИИ-применения по степени влияния на права и свободы и устанавливать более строгие требования к тем, которые используются в сферах повышенной социальной значимости.

Представляется, что перспективы развития правового регулирования обработки персональных данных ИИ-системами в России должны включать: во-первых, нормативное уточнение режима профилирования и автоматизированных решений, включая обязанность информировать о применении ИИ и обеспечивать эффективный механизм оспаривания и пересмотра решения человеком [4, с. 49]; во-вторых, внедрение обязательств по оценке воздействия на права субъектов при высоких рисках, с минимальными требованиями к содержанию такой оценки (цели, правовое основание, карта данных, риски дискриминации, меры снижения рисков, результаты тестирования модели); в-третьих, развитие стандартов прозрачности и прослеживаемости, включая требования к документации модели, описанию обучающих данных, метрик качества и процедур мониторинга дрейфа; в-четвертых, укрепление договорной дисциплины в цепочках поставки ИИ, включая требования к процессорам и поставщикам по обеспечению безопасности и предоставлению информации для аудита; в-пятых, развитие механизмов независимой оценки соответствия (сертификация, аудит) для ИИ-решений в

чувствительных сферах, при этом такие механизмы должны быть соразмерны и не создавать необоснованных барьеров инновациям.

Таким образом, обработка персональных данных системами искусственного интеллекта требует комплексной модернизации правового инструментария: общие принципы защиты данных сохраняют применимость [10, с. 150], но должны быть дополнены процедурами управляемости ИИ-рисков, обеспечивающими реальность прав субъектов и доказуемость добросовестного поведения оператора. Вектор развития регулирования целесообразно строить на сочетании технологической нейтральности, риск-ориентированного подхода и усиления процедурной прозрачности, что позволит обеспечить баланс между стимулированием внедрения ИИ и гарантией конституционно значимых прав личности [1].

Список литературы

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с учётом поправок, внесённых Законами РФ о поправках к Конституции РФ от 30.12.2008 №6-ФКЗ, от 30.12.2008 №7-ФКЗ, от 05.02.2014 №2-ФКЗ, от 01.07.2020 №11-ФКЗ) // Собрание законодательства Российской Федерации. – 2020. – №31. – Ст. 4398.

2. О персональных данных: Федеральный закон от 27.07.2006 №152-ФЗ // Собрание законодательства Российской Федерации. – 2006. – №31 (ч. I). – Ст. 3451.

3. Альпидовская М.Л. Цифровой постимпериализм: время определяемого будущего: коллективная монография / М.Л. Альпидовская, С.М. Аракелян, К.В. Воденко; отв. ред. М. Л. Альпидовская, О. В. Карамова. – М.: Прометей, 2022. – 408 с. – ISBN 978-5-00172-351-6 // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/290462 (дата обращения: 10.07.2026).

4. Бембеева Б.С. Право на защиту персональных данных и различные категории персональных данных / Б.С. Бембеева // Право в сфере Интернета: сборник статей / отв. ред. М.А. Рожкова. – М.: Статут, 2018. – С. 48–61. – EDN VNLNWS.

5. Бондаренко Н.Л. Правовая и организационная природа процессов цифровизации и регуляторная функция государства в данной сфере / Н.Л. Бондаренко,

Ю.Г. Конаневич // Ex Jure. – 2021. – №1. – С. 56–67. – EDN OZFAFE. DOI 10.17072/2619-0648-2021-1-56-67

6. Бондаренко Н.Л. Социальное предпринимательство: проблемы идентификации и институционализации / Н.Л. Бондаренко, Ю.Г. Конаневич, М.С. Бондаренко // Юстиция Беларуси. – 2022. – №6. – С. 54–62. – EDN NPKRTA.

7. Бессмертный И.А. Интеллектуальные системы: учебник и практикум для вузов / И.А. Бессмертный, А.Б. Нугуманова, А.В. Платонов. – 2-е изд. – М.: Юрайт, 2026. – 211 с. – ISBN 978-5-534-22201-2.

8. Правовое обеспечение профессиональной деятельности для специальности «Информационные системы и программирование»: учебник / А.И. Землин, Д.Ю. Левшиц, Е.С. Митячкина, М.В. Мамонова. – М.: КноРус, 2024. – 128 с. – EDN DLIPYY.

9. Липунов В.И. Искусственный интеллект и тренды цифровизации: техногенный прорыв как вызов праву / В.И. Липунов // Искусственный интеллект и тренды цифровизации: техногенный прорыв как вызов праву: материалы Третьего Международного транспортно-правового форума (Москва, 10–11 февраля 2021 г.). – М.: Российский университет транспорта, 2021. – С. 241–249. – EDN PBDDMP.

10. Липчанская М.А. Реализация конституционных социальных прав и свобод с использованием искусственного интеллекта: монография / М.А. Липчанская. – М.: Проспект, 2022. – 208 с. – ISBN 978-5-392-36451-0 // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/280754 (дата обращения: 10.07.2026). DOI 10.31085/9785392364510-2022-208. EDN KNVRCX

11. Нугуманова А.Б. Автоматизированная обработка текстовых массивов: учебник и практикум для вузов / А.Б. Нугуманова. – 2-е изд. – М.: Юрайт, 2026. – 70 с. – ISBN 978-5-534-22198-5 // Образовательная платформа Юрайт: сайт. – URL: https://urait.ru/bcode/600891/p.1 (дата обращения: 10.07.2026).

12. Раханов К.Я. Обеспечение конфиденциальности информации в сети Интернет: учебное пособие / К.Я. Раханов, Н.А. Раханова. – Новополоцк: ПГУ им.

Евфросинии Полоцкой, 2021. – 192 с. – ISBN 978-985-531-723-5. – URL: https://e.lanbook.com/book/366821 (дата обращения: 21.10.2025).