Научная статья
УДК 004.032.26

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ПРАВОВЫЕ АСПЕКТЫ ОБЕЗЛИЧИВАНИЯ И ДЕПЕРСОНАЛИЗАЦИИ ДАННЫХ В КОНТЕКСТЕ РАЗВИТИЯ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ

Инна Вадимовна Щепеткина[1], Александр Сергеевич Шайдуров[2]
[1, 2] Уральский государственный лесотехнический университет, Екатеринбург, Россия
[1] inna4050@mail.ru
[2] shaydurov-01@mail.ru

Аннотация. В статье исследуются правовые проблемы, связанные с обезличиванием и деперсонализацией данных в контексте развития технологий ИИ, в частности машинного обучения. Предлагаются пути совершенствования правового регулирования в данной сфере.

Ключевые слова: искусственный интеллект, машинное обучение, персональные данные, обезличивание данных, деперсонализация данных, правовое регулирование, защита данных

Для цитирования: Щепеткина И. В., Шайдуров А. С. Искусственный интеллект и персональные данные: правовые аспекты обезличивания и деперсонализации данных в контексте развития технологий машинного обучения // Эффективный ответ на современные вызовы с учетом взаимодействия человека и природы, человека и технологий = Effective reaction to modern challenges of the interaction between human and nature, human and technologies : материалы XVI Международной научно-технической конференции. Екатеринбург : УГЛТУ, 2025. С. 613–618.

Original article

ARTIFICIAL INTELLIGENCE AND PERSONAL DATA: LEGAL ASPECTS OF DATA ANONYMIZATION AND DEPERSONALIZATION IN THE CONTEXT OF MACHINE LEARNING DEVELOPMENT

Inna V. Schepetkina[1], Alexander S. Shaidurov[2]
[1, 2] Ural State Forest Engineering University, Ekaterinburg, Russia
[1] inna4050@mail.ru
[2] shaydurov-01@mail.ru

Abstract. This paper examines legal issues related to data anonymization and depersonalization in the context of AI technologies development, particularly machine learning. It proposes ways to improve legal regulation in this area.

Keywords: artificial intelligence, machine learning, personal data, data anonymization, data depersonalization, legal regulation, data protection

For citation: Schepetkina I. V., Shaidurov A. S. (2025) Iskusstvennyj intellekt i personal'nye dannye: pravovye aspekty obezlichivaniya i depersonalizacii dannyx v kontekste razvitiya texnologij mashinnogo obucheniya [Artificial intelligence and personal data : legal aspects of data anonymization and depersonalization in the context of machine learning development]. Effektivnyi otvet na sovremennye vyzovy s uchetom vzaimodeistviya cheloveka i prirody, cheloveka i tekhnologii [Effective reaction to modern challenges of the interaction between human and nature, human and technologies] : proceedings of the XVI International Scientific and Technical Conference. Ekaterinburg : USFEU, 2025. P. 613–618. (In Russ).

Развитие технологий искусственного интеллекта, в частности машинного обучения, предполагает обработку больших данных, включая персональные, что создает риски нарушения прав граждан. Государственная политика РФ направлена на поиск баланса между стимулированием инноваций и защитой прав субъектов персональных данных [1].

Особую актуальность приобретают инструменты обезличивания и деперсонализации данных. В условиях стремительного развития технологий, связанных с обработкой больших данных и искусственным интеллектом, наибольшее значение приобретает правовое регулирование оборота информации, позволяющей идентифицировать личность. Базовым документом, определяющим понятие и правовой режим персональных данных в России, является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных).

Согласно ст. 3 данного закона, персональными данными признается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных) [2].

Применительно к контексту искусственного интеллекта, определение персональных данных приобретает специфические черты. С одной стороны, алгоритмы машинного обучения способны выявлять неочевидные корреляции и зависимости в больших наборах данных, что может приводить к идентификации личности даже на основе информации, которая традиционно не считалась персональной. С другой стороны, развитие технологий дифференцированной обработки данных, таких как федеративное обучение, позволяет создавать и обучать модели искусственного интеллекта без необходимости централизованного хранения и обработки персональных данных [3].

В контексте стремительного развития технологий машинного обучения, требующих для своего функционирования больших объемов данных,

все более актуальными становятся вопросы обезличивания и деперсонализации. Эти механизмы позволяют использовать информацию о гражданах для научных, коммерческих и иных целей без нарушения их прав, гарантированных Законом о персональных данных.

Обезличивание данных – это процесс преобразования персональных данных таким образом, чтобы сведения, содержащиеся в результате такого преобразования, не позволяли определить принадлежность данных конкретному субъекту персональных данных.

К числу наиболее распространенных технологий обезличивания относятся: маскирование данных (замена отдельных элементов персональных данных фиктивными значениями, например замена реальных ФИО на вымышленные); генерация синтетических данных (создание наборов данных, которые по своей структуре и статистическим характеристикам напоминают реальные данные, но не содержат информации о конкретных лицах); агрегирование данных (объединение данных о нескольких субъектах таким образом, чтобы информация о каждом отдельном лице теряла свою индивидуальность); удаление идентификаторов (исключение из набора данных элементов, которые прямо указывают на личность, например номер паспорта, СНИЛС).

Деперсонализация данных – более радикальный метод обработки, в результате которого полностью утрачивается возможность установить принадлежность данных конкретному субъекту. Ключевым отличием деперсонализации от обезличивания является необратимость проведенных преобразований.

Законодательство РФ предъявляет жесткие требования к процедурам обезличивания и деперсонализации данных. Так, согласно ст. 7 Закона о персональных данных, обезличивание допустимо только при условии невозможности ассоциировать полученные сведения с конкретным субъектом персональных данных. Более того, операторы обязаны принять все необходимые меры для предотвращения реидентификации субъектов данных в результате несанкционированного доступа к обезличенным данным.

Несмотря на прогресс в области технологий обезличивания и деперсонализации, ряд правовых проблем в этой сфере остается нерешенным. В частности, отсутствует четкое определение понятия «невозможность ассоциировать данные с конкретным субъектом» и критериев ее оценки. Кроме того, существующие методы обезличивания не всегда гарантируют полную защиту от реидентификации, особенно с учетом развития технологий анализа больших данных [4].

Вопрос о том, являются ли обезличенные данные персональными данными и распространяется ли на них действие Закона о персональных данных, является дискуссионным. В России отсутствует единая правоприменительная практика по данному вопросу.

Все это свидетельствует о необходимости дальнейшего совершенствования правового регулирования в сфере обезличивания и деперсонализации данных с учетом специфики развития технологий машинного обучения и искусственного интеллекта.

Динамичное развитие технологий искусственного интеллекта, в особенности в области машинного обучения, ставит перед правовой системой Российской Федерации ряд вызовов, связанных с поиском баланса между стимулированием инноваций и защитой фундаментальных прав граждан на неприкосновенность частной жизни и персональных данных.

Среди основных проблем правового регулирования обезличивания и деперсонализации данных в контексте искусственного интеллекта можно выделить:

– отсутствие четких критериев невозможности реидентификации (законодательство не дает исчерпывающего ответа на вопрос о том, какие именно меры обезличивания следует считать достаточными для исключения возможности установить принадлежность данных конкретному лицу, что создает неопределенность для операторов персональных данных и потенциальные риски для прав субъектов данных);

– необходимость учета специфики технологий машинного обучения (традиционные методы обезличивания могут оказаться неэффективными в условиях использования алгоритмов машинного обучения, способных выявлять скрытые корреляции и зависимости в больших наборах данных, что требует разработки новых, более совершенных методов и алгоритмов обезличивания);

– проблема трансграничной передачи обезличенных данных (в условиях глобализации информационного пространства обезличенные данные могут свободно перемещаться между различными юрисдикциями, что создает дополнительные сложности для обеспечения их конфиденциальности) [5].

Перспективы развития правового регулирования в этой сфере связаны:

– с уточнением понятийного аппарата и критериев обезличивания и деперсонализации данных (необходимо законодательно закрепить единые подходы к определению понятий «обезличивание», «деперсонализация», «невозможность реидентификации», а также разработать четкие критерии оценки эффективности применяемых методов обезличивания);

– со стимулированием научных исследований и разработок в области технологий обезличивания и деперсонализации (важную роль в этом процессе должно играть государство, создавая благоприятные условия для развития инноваций в данной сфере);

– с разработкой механизмов международного сотрудничества в целях гармонизации правовых норм и обеспечения адекватного уровня защиты персональных данных при их трансграничной передаче [6].

Анализ правовых аспектов обезличивания и деперсонализации данных в контексте развития искусственного интеллекта в Российской Федерации

показал необходимость дальнейшего совершенствования законодательства. Ключевые проблемы: отсутствие четких критериев невозможности реидентификации, необходимость учета специфики машинного обучения, сложности трансграничного регулирования. Своевременное и эффективное регулирование в этой сфере – важное условие развития инноваций и защиты прав граждан.

Список источников

1. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы : утв. Указом Президента РФ от 09.05.2017 № 203 // Экспертный центр электронного государства. URL: https://d-russia.ru/wp-content/uploads/2017/05/inf_obschestvo.pdf (дата обращения: 23.09.2024).

2. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) // КонсультантПлюс. URL : http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 10.02.2024).

3. Еременко Т. А. Обезличивание персональных данных как механизм защиты конституционных прав человека // Вестник СГЮА. 2023. № 1 (150). С. 104–109. URL: https://cyberleninka.ru/article/n/obezlichivanie-personalnyh-dannyh-kak-mehanizm-zaschity-konstitutsionnyh-prav-cheloveka (дата обращения: 02.10.2024).

4. Вичугова А. Как машинное обучение защищает большие данные: ML в Cybersecurity // Школы Больших Данных. URL: https:// big-dataschool.ru/blog/machine-learning-in-cybersecurity.html (дата обращения: 23.09.2024).

5. Петрищева Е. Д. Правовое регулирование защиты персональных данных в сети Интернет // Молодой ученый. 2023. № 43 (490). С. 185–186. URL: https://moluch.ru/archive/490/107082/ (дата обращения: 02.10.2024).

6. Обезличивание данных: сохранение баланса между правами граждан и развитием инноваций // ГАРАНТ.РУ. URL: https://www.garant.ru/news/1464529/ (дата обращения: 23.09.2024).

References

1. Strategy for the Development of the Information Society in the Russian Federation for 2017–2030: approved by Decree of the President of the Russian Federation No. 203 of 05.09.2017 // Expert Center of Electronic Government. URL: https://d-russia.ru/wp-content/uploads/2017/05/inf_obschestvo.pdf (accessed: 23.09.2024).

2. Federal Law № 152-FZ of July 27, 2006 (as amended on July 14, 2022) «On Personal Data» // ConsultantPlus. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (accessed: 10.02.2024).

3. Eremenko T. A. Depersonalization of personal data as a mechanism for protecting constitutional human rights. Vestnik SGYuA, 2023. № 1 (150). P. 104–109. URL: https://cyberleninka.ru/article/n/obezlichivanie-personalnyh-dannyh-kak-mehanizm-zaschity-konstitutsionnyh-prav-cheloveka (accessed: 02.10.2024).

4. Vichugova A. How machine learning protects big data: ML in Cybersecurity // Big Data Schools. URL: https://bigdataschool.ru/blog/machine-learning-in-cybersecurity.html (accessed: 23.09.2024).

5. Petrishcheva E. D. Legal regulation of personal data protection on the Internet. Young Scientist. 2023. № 43 (490). P. 185–186. URL: https://moluch.ru/archive/490/107082/ (accessed: 02.10.2024).

6. Data anonymization: maintaining a balance between citizens' rights and innovation development // GARANT.RU. URL: https://www.garant.ru/ news/ 1464529/ (accessed: 23.09.2024).