

УДК 34.096

**ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
В КОНТЕКСТЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ****Я. А. КУРТО***(Представлено: канд. юрид. наук, доц. П. В. СОЛОВЬЕВ)*

В данной статье рассматривается вопрос защиты персональных данных при применении искусственного интеллекта. Анализируются нормы национальных и международно-правовых актов касательно исследуемого вопроса. Проводится сравнение полученных выводов и современного состояния правового регулирования искусственного интеллекта в контексте защиты персональных данных в Республике Беларусь.

Актуальность исследований в сфере защиты персональных данных возрастает прямо пропорционально развивающимся технологиям. Вопрос защиты персональной информации рассматривается исследователями в разных областях в том числе с целью выработки единого подхода к правовому регулированию. Однако не все отрасли права развиты в должной степени для того, чтобы обеспечить полную защиту прав субъекта персональных данных.

Так, развитие технологий искусственного интеллекта (далее – ИИ) представляет новый вызов в области защиты персональных данных. Несмотря на значимость поставленного вопроса и продолжающиеся дискуссии в правовой науке, среди научного сообщества не существует единого мнения об отнесении вопроса правового регулирования искусственного интеллекта к определенной отрасли права. Данный предмет обсуждения рассматривается с разных точек зрения в гражданском, информационном, конституционном и иных отраслях права [1]. Рассмотрим ключевые вопросы влияния искусственного интеллекта на сферу защиты персональных данных.

В академической сфере существует множество определений ИИ в зависимости от отрасли науки, в которой исследуется данная технология. А. Карцхия определяет искусственный интеллект как интеллектуального робота, который действует автономно посредством датчиков обмена данными с окружающей средой, обладает способностью к самообучению, имеет независимую поддержку и адаптирует свое поведение и действия к окружающей среде [2]. Названные характеристики играют значимую роль для определения особенностей правового регулирования технологии в рамках информационного права.

Понятие ИИ закреплено в законодательстве Республики Беларусь. Им признается комплекс технологических решений, позволяющий имитировать когнитивные функции человека и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека, и включающий в себя информационно-коммуникационную инфраструктуру, программное обеспечение, процессы и сервисы по обработке данных и поиску решений [3].

Как было отмечено ранее, одним из признаков ИИ является обмен данными. Для этого алгоритмы ИИ должны пройти этап обучения на основе добавленной информации, в процессе которого они выявляют закономерности между полученными сведениями. Процесс добавления информации для обучения ИИ называется аннотированием данных. На данном этапе разработчики ИИ предоставляют машинным алгоритмам информацию, необходимую для их обучения и дальнейшего составления прогнозов, принятия решений и т.д. [4]. После этого ИИ приступает к этапу использования данных в соответствующих целях. Следовательно, на названных стадиях помимо обработки информации, которая не относится к идентифицированному физическому лицу, происходит обработка персональных данных.

К сожалению, способы, с помощью которых ИИ получает данные, не всегда являются правомерными. Требования к защите персональных данных при применении технологии ИИ регулируются национальными и международными правовыми актами. Законодательство Республики Беларусь не содержит требований к защите персональных данных при использовании искусственного интеллекта. Регулирование данного вопроса позволит достичь цели Концепции правовой политики Республики Беларусь, которая устанавливает, что в сферах законодательства предстоит урегулировать вопрос применения искусственного интеллекта [5].

Рассмотрим основополагающие международно-правовые акты, а также национальные законы некоторых стран, которые регулируют вопрос защиты персональных данных при применении технологий ИИ.

Ведущим нормативным правовым актом, утверждающим требования к обеспечению защиты персональных данных на территории Европейского союза, является «Общий регламент по защите персональных данных (GDPR)» (далее – Регламент), действующий на территории Европейского союза с 2018 года [6]. В нем установлены нормы, которые нашли отражение в Законе Республики Беларусь №99-З «О защите персональных данных» (далее – Закон №99-З) [7]. В данном акте определены как общие критерии по отношению к защите персональных данных, так и требования к разработчикам ИИ при обработке системой персональных данных, которые являются операторами.

Одним из условий законности обработки персональных данных является соблюдение требований к их обработке. Принципы обработки персональных данных установлены 5 статьей Регламента а именно принципы законности, справедливости и прозрачности; ограничения целью; минимизации данных; точности; ограничения хранения; целостности и конфиденциальности [6].

Статья 22 Регламента является специальной нормой по отношению к защите персональных данных при использовании ИИ. Так, субъект данных имеет право не подвергаться решению, которое основано исключительно на автоматизированной обработке, в том числе профилировании, вызывающему для него юридические последствия или похожим образом существенно влияющему на него. Примером такого решения является применение банками ИИ для оценки платёжеспособности клиента [6].

Однако соблюдение названных принципов операторами еще не подтверждает законность обработки персональных данных. Наличие правового основания их обработки, предусмотренного статьей 6 Регламента, является необходимым для этого условием. К примеру, в случае обработки данных ИИ для показа персонализированной рекламы в Интернет-пространстве компании должны иметь соответствующее правовое основание.

Одним из самых громких нарушений требований Регламента разработчиками ИИ является кейс с участием ChatGPT, одного из самых популярных сервисов ИИ, который позволяет пользователям использовать компьютерное мышление для достижения своих целей. Согласно итальянскому ведомству по защите данных, компания OpenAI, разработчик ChatGPT, противоправно собирала персональные данные пользователей, что привело к их утечке и нарушению требований Регламента по отношению к обработке персональных данных [8].

Иным правовым актом, регулирующим правоотношения в сфере защиты персональных данных в плоскости ИИ и действующим на территории Европейского союза, является «AI Act», который был принят 13 марта 2024 года. Важнейшим нововведением акта является разделение систем ИИ на 4 уровня риска: неприемлемого, высокого, ограниченного и минимального уровня риска. Для каждого класса вводятся различные правила и требования, которые влияют в том числе и на возможность обработки персональных данных отдельными видами ИИ [9].

Несмотря на то, что названные международные и национальные акты обязательного характера ставят своей целью защиту персональных данных, на данный момент полное правовое регулирование вопроса не представляется возможным. М.С. Абламейко утверждает, что применение систем ИИ практически невозможно ограничить территориально, а принятие законодательных актов может стать сдерживающим фактором технологического процесса. Вследствие этого на международном уровне разрабатываются и применяются документы так называемого «мягкого права», которые носят рекомендательный характер [1]. Одним из таких документов рекомендательного характера являются Рекомендации Совета в отношении ИИ (Recommendation of the Council on Artificial Intelligence), принятые Организацией экономического сотрудничества и развития (OECD) в 2019 году. Данный акт призван помочь разработчикам ИИ сделать так, чтобы их системы не нарушали права пользователей в сфере защиты данных и частной жизни [10].

В Соединенных Штатах Америки вопрос регулирования защиты персональных данных при использовании ИИ не регламентирован на федеральном уровне. Ведется активная законодательная деятельность по разработке и внедрению правовых норм касательно ИИ и его влияния на частную жизнь человека. 28 сентября 2024 года был принят Законопроект №1008 который вносит поправки в Закон о защите прав потребителей Калифорнии (the California Consumer Privacy Act, CCPA), признавая, что персональная информация может быть использована системами ИИ для принятия решений [11].

Стремление Китайской Народной Республики стать глобальным лидером в индустрии ИИ подтверждается высоким уровнем регулирования вопроса защиты персональных данных в контексте использования ИИ. Так, Закон о защите персональной информации (Personal Information Protection Law, PIPL) является рамочным законом и применяется как к автоматизированной обработке персональных данных, так и неавтоматизированной. PIPL дает определение автоматическому принятию решений, которое обозначается как использование компьютерных программ для автоматического анализа или оценки поведения, пристрастия, интересов или увлечений физических лиц или финансового, медицинского или кредитного статуса физических лиц. Согласно закону, при использовании персональных данных в процессе автоматического принятия решений должна быть обеспечена прозрачность, справедливость и соблюдение правопорядка в автоматизированных результатах [12]. Закон о кибербезопасности (the Cybersecurity Law of the People's Republic of China, CSL), Закон о безопасности данных (the Data Security Law, DSL), Меры по генеративному ИИ (the Generative AI Measures) более детально регулируют вопрос ИИ в сфере защиты персональной информации.

Указ Президента Российской Федерации от 10 октября 2019 г. N 490 «О развитии искусственного интеллекта в Российской Федерации» признает необходимость обеспечения защиты персональных данных и иной информации ограниченного доступа, объектов интеллектуальных прав при создании и обучении моделей искусственного интеллекта как новый вызов для государства [13]. Федеральный закон «О персональных

данных» является ключевым актом в сфере защиты персональных данных в Российской Федерации [14]. Данный закон не дает определения автоматизированному принятию решений, как PIPL, однако утверждает понятие автоматизированной обработки данных и утверждает требования к ней.

В результате анализа названных правовых актов следует подчеркнуть, что различные страны регулируют вопрос защиты персональных данных при использовании технологии ИИ и принимают различные правовые акты в зависимости от степени развития правовой системы, приоритетов государственного развития и наличия соответствующих угроз.

Республика Беларусь имеет более низкий уровень регламентации ИИ в контексте защиты персональных данных, чем в Китае и России. Данный факт можно объяснить стремительным развитием технологий и невозможностью моментального реагирования на современные вызовы. Закон №99-З регулирует отношения в сфере защиты персональных данных в целом, без конкретизации требований к системам ИИ. Правовой статус ИИ на сегодняшний день не определен, а также отсутствует регламентация получения согласия субъекта для обработки его персональных данных системой ИИ. Определение требований к системам ИИ в Законе №99-З может стать новым этапом в сфере защиты персональных данных в Республике Беларусь.

Предлагается принять во внимание опыта иностранных государств по установлению требований к ИИ при обработке персональных данных. Внедрение в статью 1 Закона №99-З понятия автоматизированной обработки персональных данных, аналогично статье 3 Федерального закона «О персональных данных», сделает пункт 1 статьи 2 названного Закона более прозрачным для субъектов.

Законом № 99-З установлены принципы обработки персональных данных и обязательство к получению согласия субъекта персональных данных для их обработки соответственно принципам Регламента. Представляется возможным отнесение обработки персональных данных ИИ без согласия субъекта при соблюдении условия обработки в научных или иных целях, а также при их обезличивании, то есть анонимизации [15]. Угрозой в отношении обезличенных персональных данных являются возможности некоторых систем ИИ к деанонимизации персональных данных. В таком случае разработчики соответствующих ИИ должны понести ответственность за нарушение требований законодательства. Предлагается установление требования к обработке персональных данных с использованием ИИ только при условии соблюдения общих требований Закона № 99-З, в том числе получения письменного согласия субъекта персональных данных, либо обязательного обезличивания персональных данных.

Определение уровней риска в отношении персональных данных в зависимости от присвоенного уровня риска ИИ, подобно установленным в «AI Act», позволит расширить возможности защиты персональной информации. Данный подход сделает возможным определение степеней ответственности операторов, нарушивших требования законодательства о защите персональных данных.

В условиях стремительного развития технологий ИИ законодательное регулирование вопроса защиты персональных данных не является исчерпывающим. Закон №99-З не содержит специальных требований к обработке персональных данных системами ИИ. В ходе анализа иностранных и международно-правовых актов автор пришел к выводу о необходимости совершенствования сферы защиты персональных данных в Республике Беларусь. Принятие специальных правовых норм в Законе №99-З приведет к комплексному регулированию защиты персональных данных и недопущению нарушений закона в связи с пробелами законодательства. Развитие правового регулирования в данной области позволит достичь целей в сфере искусственного интеллекта, предусмотренных Концепцией правовой политики Республики Беларусь.

ЛИТЕРАТУРА

1. Абламейко, М.С. Этические и правовые аспекты применения технологий искусственного интеллекта с учетом международного опыта / М.С. Абламейко // *Право.by*. – 2023. – № 5(85). – С. 70.
2. Карцхия, А. Искусственный интеллект: "ларец Пандоры" или новая надежда? / А. Карцхия // *Интеллектуальная собственность. Авторское право и смежные права*. – 2017. – № 4. – С. 23–30.
3. О мерах по реализации Указа Президента Республики Беларусь от 7 апреля 2022 г. №136: Постановление Совета Министров Респ. Беларусь, 21 апр. 2023 г., № 280 // *Эталон – Беларусь* [Электронный ресурс]. – Режим доступа: <https://etalonline.by/document/?regnum=c22300280>. – Дата доступа: 01.10.2024.
4. Jensen, B. Exploring the Complex Ethical Challenges of Data Annotation / B. Jensen // *Stanford University Human-Centered Artificial Intelligence* [Electronic resource]. – 10.07.2024. – Mode of access: <https://hai.stanford.edu/news/exploring-complex-ethical-challenges-data-annotation>. – Date of access: 05.10.2024.
5. О Концепции правовой политики Республики Беларусь: Указ Президента Респ. Беларусь, 28 июня 2023 г., № 196 // *Эталон – Беларусь* [Электронный ресурс]. – Режим доступа: https://etalonline.by/document/?regnum=p32300196&q_id=1034267. – Дата доступа: 01.10.2024.
6. General Data Protection Regulation // *EUR-Lex* [Electronic resource]. – Режим доступа: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. – Date of access: 06.10.2024.
7. О защите персональных данных: Закон Респ. Беларусь от 7 мая 2021 г. № 99-З / *Эталон – Беларусь* [Электронный ресурс]. – Режим доступа: <https://etalonline.by/document/?regnum=H12100099>. – Дата доступа: 30.09.2024.

8. The Curious Case of ChatGPT: Banned in Italy, Admired Globally, and Raising Eyebrows Everywhere // Allganize [Electronic resource] – 10.07.2024. – Mode of access: <https://www.allganize.ai/en/blog/the-curious-case-of-chatgpt-banned-in-italy-admired-globally-and-raising-eyebrows-everywhere>. – Date of access: 30.09.2024.
9. Artificial Intelligence Act (AI Act) [Electronic resource] // Mode of access: <https://ai-act-law.eu/> – Date of access: 06.10.2024.
10. Recommendation of the Council on Artificial Intelligence // OECD Legal Instruments [Electronic resource]. – Mode of access: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> – Date of access: 05.10.2024.
11. AB-1008 California Consumer Privacy Act of 2018: personal information // California Legislative Information [Electronic resource]. – Mode of access: https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB1008. – Date of access: 06.10.2024.
12. Закон КНР о защите персональных данных PIPL. Подробный разбор в 2023 // TDSC [Электронный ресурс]. – Режим доступа: <https://thedimsum.com/ru/china-information-protection-law/>. – Дата доступа: 06.10.2024.
13. Указ Президента РФ от 10 октября 2019 г. №490 "О развитии искусственного интеллекта в Российской Федерации" (с изменениями и дополнениями) // КонсультантПлюс. Россия [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_335184/. – Дата доступа: 07.10.2024.
14. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ // КонсультантПлюс. Россия [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61801/. – Дата доступа: 07.10.2024.
15. А.А. Гаев, В.И. Диско, С.В. Задиран, Е.М. Липлянин, А.А. Парфенчик, И.А. Пырко, Н.А. Саванович, Е.В. Синюк, Н.А. Швед, Д.А. Шевчук Постатейный комментарий к Закону Республики Беларусь «О защите персональных данных» – Режим доступа: <https://cpd.by/pravovaya-osnova/metodologicheskiye-dokumenty-rekomendatsii/postatejnyj-kommentarij-k-zakonu-respubliki-belarus-o-zashhite-personalnyh-dannyh/>. – Дата доступа: 09.10.2024.