



ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ, ЗАПРЕТ АВТОМАТИЗИРОВАННЫХ РЕШЕНИЙ И РЕГУЛИРОВАНИЕ СИНТЕТИЧЕСКОГО КОНТЕНТА: ГРАЖДАНСКО-ПРАВОВЫЕ АСПЕКТЫ

Султонова Дурдона Шарофиддин кизи

Ташкентский государственный юридический университет

Аннотация

Статья посвящена анализу гражданско-правовых аспектов регулирования технологий искусственного интеллекта в контексте защиты персональных данных, ограничения автоматизированного принятия решений и правового статуса синтетического контента. Автор проводит сравнительно-правовой анализ подходов Европейского союза, Великобритании, Китая, Республики Казахстан и Республики Узбекистан к определению и защите персональных данных, отмечая различия в признании этого права основополагающим или ограниченной технической гарантией. Рассматривается институт запрета полностью автоматизированных юридически значимых решений. Автор приходит к выводу об отсутствии в законодательстве Узбекистана специального регулирования, учитывающего специфику искусственного интеллекта, и необходимости выработки норм о правовом статусе контента, его маркировке и распределении ответственности с учётом передового зарубежного опыта.

Ключевые слова: искусственный интеллект; персональные данные; защита данных; автоматизированное принятие решений; GDPR; синтетический контент; дипфейк; авторское право; цифровые права; правовое



регулирование; гражданско-правовая ответственность; Республика Узбекистан.

Технологии искусственного интеллекта развиваются стремительно и приносят немало пользы, однако вместе с очевидными преимуществами эти технологии несут в себе серьёзные угрозы, прежде всего в сфере защиты личных данных. В отличие от традиционных компьютерных программ, системы искусственного интеллекта способны анализировать огромные массивы информации о человеке, делать выводы о его поведении, привычках и личных качествах, а затем принимать на этой основе решения, которые напрямую затрагивают его права и интересы. При этом действующие законы во многих странах, включая Узбекистан, пока не успевают за такими темпами развития технологий и не обеспечивают достаточной правовой защиты. Именно это несоответствие между возможностями искусственного интеллекта и уровнем правового регулирования делает проблему защиты персональных данных одной из наиболее актуальных задач современности.

Широкое распространение систем искусственного интеллекта, предполагающих массовый сбор и обработку персональных данных, порождает существенные угрозы личным правам и интересам граждан. Данные угрозы обусловлены прежде всего колоссальными объёмами информации, которые аккумулируют, обрабатывают и хранят современные системы искусственного интеллекта. В частности, недостаточная защищённость таких систем создаёт реальную опасность утечки данных и несанкционированного доступа к ним, что в свою очередь открывает возможности для хищения персональных сведений, совершения мошеннических действий и иных правонарушений. Помимо этого, передовые методы машинного обучения нередко позволяют осуществлять повторную идентификацию лиц путём сопоставления формально обезличенных данных с



иными общедоступными сведениями, что фактически обесценивает традиционные инструменты анонимизации и ставит под сомнение их эффективность в современных условиях.

Наконец, особую озабоченность вызывает способность систем искусственного интеллекта выявлять на основе внешне нейтральных сведений делать заключения о состоянии здоровья человека, его политических взглядах или иных личных характеристиках, создавая тем самым почву для дискриминации и манипулятивного воздействия на личность.

Изложенное свидетельствует о том, что перед научным сообществом и законодателем стоит непростая задача поиска оптимального баланса между использованием потенциала искусственного интеллекта в интересах общественного прогресса и обеспечением надлежащей защиты личных прав и законных интересов граждан, включая охрану их персональных данных. Достижение такого баланса предполагает не ограничение технологического развития как такового, а выработку правовых механизмов, способных направить его в русло, совместимое с принципами уважения человеческого достоинства, информационной автономии личности и верховенства закона.

В цифровую эпоху определение правового статуса персональных данных имеет большое значение для их защиты

В ЕС статья 4 Общего регламента по защите данных (General Data Protection Regulation – далее по тексту «GDPR») определяет персональные данные как любую информацию, относящуюся к человеку, которая идентифицирует или может идентифицировать человека. В GDPR право субъекта данных на его персональные данные характеризуется как «право на неприкосновенность частной жизни в отношении обработки персональных



данных»¹. Такое право считается основным и не может быть перевешено другими ценностями. Кроме того, статья 16 Договора о функционировании Европейского союза обязывает ЕС устанавливать правила, касающиеся защиты лиц в отношении обработки персональных данных².

В китайском законодательстве определение персональных данных закреплено в Законе Китая о кибербезопасности³. Согласно статье 67(5) Закона, персональные данные охватывают различные сведения, к которым относятся, в частности, имя, дата рождения, персональный идентификационный номер, биометрические характеристики, место проживания и контактный телефон. В КНР защита персональных данных не рассматривается как неотъемлемое право, в отличие от права на частную жизнь или собственности, и уровень ее охраны остается сравнительно низким. Это связано с несколькими факторами. Во-первых, в отличие от ЕС, китайское законодательство не признает персональные данные основополагающим правом человека. Власти Китая, как крупнейший оператор данных, считают, что право граждан на защиту своей информации должно быть ограничено, если оно мешает государству собирать, обрабатывать, хранить и использовать эти данные. Во-вторых, Конституция Китая предоставляет минимальные гарантии защиты личной информации, включая лишь место жительства, свободу и тайну переписки. Однако персональные данные охватывают гораздо более широкий спектр информации, который выходит за рамки этих конституционных положений.

¹ General Data Protection Regulation (GDPR), adopted on April 27, 2016, and enforced since May 25, 2018 // URL: <https://gdpr-info.eu/>

² Treaty on the Functioning of the European Union of 13 December 2007 - consolidated version // URL: https://eur-lex.europa.eu/eli/treaty/tfeu_2012/oj/eng (date of reference: 15.11.2024)

³ Закон о кибербезопасности Китайской Народной Республики. Принят 1.06.2017 г. Baidu. <https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E6%B3%95/16843044?fr=aladdin>



В Республике Казахстан правовой режим защиты персональных данных близок к китайскому подходу, поскольку в Основном законе государства защита персональных данных не отражена как конституционное право человека. В ст. 18 закреплены лишь права на неприкосновенность частной жизни, личную и семейную тайну, тайну личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений⁴

Согласно статье 4 Закона Республики Узбекистан «О персональных данных»⁵, под персональными данными понимается информация, зафиксированная на электронном, бумажном и (или) ином материальном носителе информация, относящаяся к определенному физическому лицу или дающая возможность его идентификации.

Таким образом, правовая природа персональных данных определяет режим защиты этих данных в различных государствах. Разные подходы государств к их определению и защите устанавливают границы возможностей использования данных и степень их конфиденциальности, особенно в эпоху развития искусственного интеллекта и цифровых технологий, в связи с тем, что персональные данные становятся «цифровым ресурсом». Поэтому необходим анализ правовых актов и нормативных рамок использования персональных данных в системах искусственного интеллекта в зарубежных странах для выявления проблем защиты этих данных и возможности адаптации успешных международных практик в Республике Узбекистан.

Европейский союз занимает лидирующие позиции в области правового регулирования защиты персональных данных на международном уровне.

⁴ Конституция Республики Казахстан от 30 августа 1995 года // URL: https://adilet.zan.kz/rus/docs/K950001000_links (дата обращения: 21.11.2024).

⁵ Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года № ЗРУ-547, статья 4 <https://lex.uz/docs/4396428>



Принятие Общего регламента по защите данных (GDPR) стало значимой вехой в укреплении права человека на защиту персональной информации в условиях цифровой экономики. Регламент преследует двуединую цель — гарантировать гражданам ЕС эффективную защиту их информационных прав, а также — унифицировать правила обработки данных для организаций и государственных органов, устранив правовую фрагментацию, существовавшую в рамках различных национальных правовых порядков, и тем самым снизив излишнюю административную нагрузку на участников цифрового рынка. Принципиально важно, что сфера действия GDPR не ограничена территорией Европейского союза, то есть регламент распространяется на любую организацию, осуществляющую обработку персональных данных граждан ЕС, вне зависимости от места её нахождения. Вместе с тем регламент оперирует терминологией, связанной с использованием сети Интернет, социальных сетей и веб-платформ, однако не содержит понятий, относящихся к технологиям искусственного интеллекта. Это обстоятельство свидетельствует о том, что GDPR разрабатывался прежде всего в целях урегулирования проблем конфиденциальности, тогда как вопросы, связанные с применением искусственного интеллекта и приобретшие широкую социальную значимость лишь в последние годы, остались за рамками его регулирования, что обуславливает необходимость дальнейшего совершенствования европейского законодательства в данной сфере.

Однако именно экстерриториальный характер GDPR и его ориентация на защиту персональных данных создали нормативную основу для последующего осмысления более сложных цифровых процессов, связанных с использованием алгоритмических систем и искусственного интеллекта. В условиях стремительного развития технологий обработки данных особую актуальность приобрёл вопрос допустимости принятия решений



исключительно на основе автоматизированной обработки информации, поскольку такие механизмы способны напрямую затрагивать права и законные интересы физических лиц. В этой связи всё большее внимание уделяется проблеме автоматизированного принятия решений (Automated Decision-Making, ADM), рассматриваемой как одно из ключевых направлений правового регулирования искусственного интеллекта.

Автоматизированные алгоритмические решения (Automated Decision-Making, ADM) представляют собой процесс выработки юридически значимых результатов с использованием алгоритмических систем без существенного вмешательства человека. Распространение таких систем в кредитовании, страховании, трудоустройстве и государственном управлении ставит принципиальные правовые вопросы о субъектности, ответственности и защите лиц, чьи права затрагиваются этими решениями.

Указанные риски обусловили необходимость формирования правовых механизмов, направленных на ограничение полностью автономного принятия решений и обеспечение гарантий защиты прав субъектов данных. В связи с этим в ряде государств уже закреплены нормы, устанавливающие пределы использования искусственного интеллекта при принятии решений, способных оказать существенное влияние на правовой статус лица. Показательным примером является законодательство Великобритании, в рамках которого отдельные гарантии против автоматизированного принятия решений предусмотрены в сфере защиты персональных данных.

По состоянию на начало 2026 года в Великобритании нет общих правил для искусственного интеллекта, хотя некоторые законы накладывают ограничения на его использование, например Закон «О защите данных»⁶ 2018

⁶ Data Protection Act 2018. URL: <https://www.legislation.gov.uk/ukpga/2018/12/part/3/chapter/3/crossheading/automated-individualdecisionmaking/enacted>



года включает «право не подвергаться автоматизированному принятию решений». Фактически это означает, что искусственный интеллект не может использоваться для принятия значимых решений в отношении лица, к которому относятся данные.

Право субъекта данных не подвергаться автоматизированным решениям впервые было расширено в статье 22 GDPR⁷: субъект данных вправе не быть объектом решения, основанного исключительно на автоматизированной обработке, если такое решение производит в отношении него правовые последствия или существенным образом на него влияет.

Аналогический запрет содержится в Законе Республики Узбекистан «Об информатизации». В частности, статья 7¹ установлено, то при принятии юридически значимых решений, затрагивающих права и свободы человека, не допускается ссылаться исключительно на заключения информационных ресурсов и информационных систем, созданных на основе технологий искусственного интеллекта⁸.

С правовой точки зрения ИИ не признается субъектом права, поскольку не обладает правосознанием и волей. Соответственно, ответственность за причиненный им вред возлагается на разработчиков, владельцев или пользователей

Таким образом, стремительно развитие искусственного интеллекта и его способность принимать решения на основе анализа больших данных и обработки персональных данных требует переосмысления принципов ответственности за принятие таких решений. Автоматизированные решения, влияющие на жизнь граждан, должны быть прозрачными и подконтрольными,

⁷ Regulation (EU) 2016/679 (GDPR), Article 22(1).

⁸ Закон Республики Узбекистан «Об информатизации» от 11 декабря 2003 г. № 560-П [Электронный ресурс] // Национальная база данных законодательства Республики Узбекистан <https://lex.uz/docs/82956#8017195>



обеспечивая возможность обжалования и получения мотивированного ответа, раскрывающего алгоритмическую логику. Необходимо законодательно закрепить право уполномоченных органов и лиц на отказ от рекомендаций искусственного интеллекта, гарантируя приоритет человеческого суждения над машинным. В целях повышения доверия к алгоритмам и снижения рисков, связанных с их автономностью, следует обеспечить открытость исходного кода и создать независимые этические комитеты, ответственные за оценку потенциальных последствий. Однако, при регулировании искусственного интеллекта важно помнить о принципе умеренности: чрезмерно строгие нормы могут задушить инновации, а их отсутствие – создать благоприятную почву для злоупотреблений.

Одновременно развитие искусственного интеллекта порождает не только проблему автономного принятия решений, но и иные вызовы, связанные с созданием и распространением результатов деятельности систем искусственного интеллекта, способных оказывать влияние на права и законные интересы участников гражданского оборота. Особую актуальность в этой связи приобретает вопрос гражданско-правового регулирования синтетического контента, включая тексты, изображения, аудио- и видеоматериалы, создаваемые с использованием систем искусственного интеллекта. Распространение подобных технологий ставит перед правом новые задачи, связанные с определением правового режима таких объектов, распределением ответственности за причинение вреда, а также обеспечением защиты личности, деловой репутации и авторских прав в условиях цифровой среды.

Синтетический контент представляет собой информационные материалы, созданные или существенно изменённые с использованием технологий искусственного интеллекта таким образом, что они имитируют



реальность или подлинные высказывания реальных лиц. Данный феномен охватывает: дипфейки — реалистичные подделки видео и аудио; синтетические лица, генерируемые искусственным интеллектом; тексты, создаваемые большими языковыми моделями и выдаваемые за подлинные высказывания реального лица; синтетические медицинские изображения.

Распространение синтетического контента порождает комплекс гражданско-правовых вопросов, связанных не только с защитой личности и предотвращением дезинформации, но и с определением правового режима результатов, создаваемых искусственным интеллектом. В этой связи особую значимость приобретает вопрос о возможности признания подобных материалов объектами интеллектуальной собственности и предоставления им правовой охраны в рамках авторского права.

Согласно статье 8 Закона Республики Узбекистан «Об авторском праве и смежных правах»⁹, результаты, полученные с использованием технических средств без осуществления человеком творческой деятельности, не признаются объектами авторского права. Соответственно, материалы, полностью сгенерированные искусственным интеллектом без непосредственного творческого участия человека, не рассматриваются в качестве результатов интеллектуальной деятельности и не подлежат правовой охране в рамках действующего авторского законодательства. Данный подход отражает традиционную концепцию авторского права, основанную на признании творческого вклада человека обязательным условием возникновения субъективных авторских прав.

Вместе с тем стремительное развитие генеративных технологий демонстрирует, что на практике процесс создания синтетического контента

⁹ Закон Республики Узбекистан «Об авторском праве и смежных правах» от 20 июля 2006 г. № ЗРУ-42 [Электронный ресурс] // Национальная база данных законодательства Республики Узбекистан <https://lex.uz/docs/1023494>



нередко предполагает определённую степень участия человека: постановку задачи, формирование запросов (prompt engineering), отбор и редактирование итогового результата. Это порождает дискуссию относительно того, в какой мере подобное участие может рассматриваться как творческий вклад, достаточный для признания произведения объектом авторского права. Отсутствие в законодательстве Республики Узбекистан специальных норм, регулирующих правовой статус контента, созданного с применением искусственного интеллекта, создаёт правовую неопределённость в вопросах принадлежности имущественных прав, распределения ответственности за нарушение прав третьих лиц, а также защиты интересов авторов оригинальных произведений, использованных при обучении алгоритмов.

Кроме того, проблема синтетического контента выходит за рамки исключительно авторско-правового регулирования и затрагивает сферу защиты чести, достоинства, деловой репутации и персональных данных. Использование дипфейков и иных форм реалистичной цифровой имитации способно причинять значительный репутационный и имущественный вред, а также вводить участников гражданского оборота в заблуждение. В этих условиях возникает необходимость формирования комплексного правового механизма, предусматривающего требования к маркировке синтетического контента, определению субъектов ответственности за его распространение, а также обеспечению эффективных способов защиты нарушенных прав в цифровой среде.

Таким образом, рассмотренные в настоящем параграфе вопросы свидетельствуют о том, что стремительное развитие технологий искусственного интеллекта формирует принципиально новые правовые вызовы в сфере защиты персональных данных, регулирования автоматизированного принятия решений и обращения синтетического



контента. Сравнительно-правовой анализ подходов ЕС, Великобритании, Китая и Республики Узбекистан показывает, что ни один из существующих правовых порядков не выработал исчерпывающего и последовательного ответа на эти вызовы: одни государства признают защиту персональных данных основополагающим правом человека и выстраивают вокруг него разветвлённую нормативную систему, тогда как другие по-прежнему рассматривают её как ограниченную техническую гарантию, подчинённую публичным интересам. Применительно к Республике Узбекистан следует констатировать, что действующее законодательство закрепляет ряд базовых механизмов защиты в данной сфере — запрет исключительно автоматизированных юридически значимых решений, охрану персональных данных и авторских прав, — однако оно не содержит специального регулирования, учитывающего специфику искусственного интеллекта как самостоятельного явления. Отсутствие норм о правовом статусе контента, созданного искусственным интеллектом, о порядке маркировки синтетических материалов и о распределении ответственности в многосубъектных цифровых отношениях порождает правовую неопределённость, преодоление которой требует планомерной законодательной работы с опорой на передовой международный опыт и принципы соразмерности правового регулирования технологическим инновациям.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Гражданский кодекс Республики Узбекистан. Часть первая от 29 августа 1996 года № 256-I (с изменениями). — Ташкент, 2024.
2. Гражданский кодекс Республики Узбекистан. Часть вторая от 29 августа 1996 года (с изменениями). — Ташкент, 2024.



3. Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года № ЗРУ-547 // Национальная база данных законодательства Узбекистана. URL: <https://lex.uz>.
4. Закон Республики Узбекистан «Об информатизации» от 11 декабря 2003 года № 560-II (с изменениями).
5. Закон Республики Узбекистан «Об авторском праве и смежных правах» от 20 июля 2006 года № ЗРУ-42 (с изменениями).
6. Бачило И.Л. Информационное право: учебник. — 3-е изд. — М.: Юрайт, 2016. — 419 с.
7. Исмаилов Б.И. Информационное право Узбекистана: монография. — Ташкент: ТГЮУ, 2018. — 312 с.
8. Лопатин В.Н. Правовая охрана и защита права на неприкосновенность частной жизни. — М.: Юрлитинформ, 2017. — 288 с.