ИНСТИТУТ ЭКОНОМИЧЕСКОЙ ПОЛИТИКИ имени Е.Т. ГАЙДАРА

Лаборатория анализа лучших международных практик

Мониторинг международных трендов правового регулирования для развития законодательства в сфере цифровой экономики в России

Международное регулирование дипфейков, квантовых технологий и использования технологий искусственного интеллекта в трудовых отношениях

Мониторинг №2 (Февраль 2024)

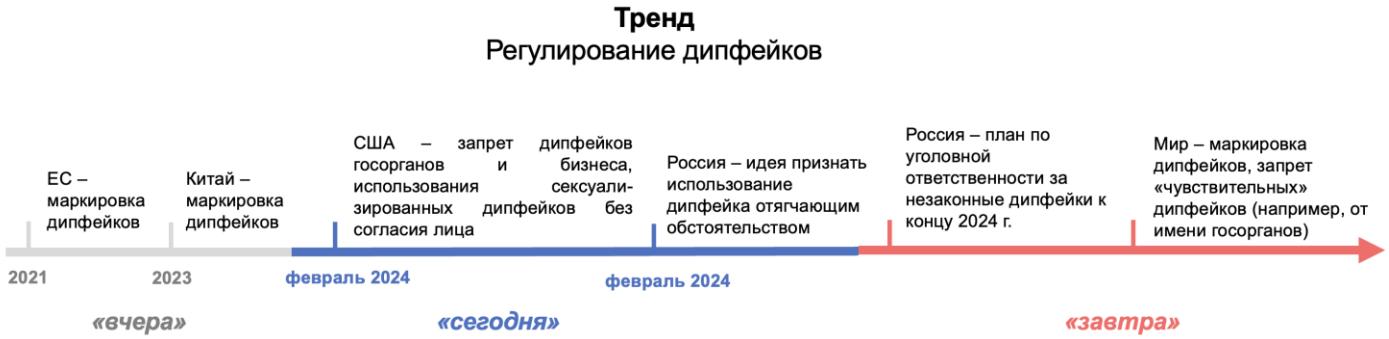
10 МАРТА, 2024

«Наше поколение веровало в идею прогресса…а материалисты окорнали ее, свели до идеи прогресса технического»
М. Горький

В феврале 2024 г. можно выделить 3 события, которые определяют тренды развития регулирования цифровой экономики

Тренд №1. Регулирование дипфейков

В России в феврале текущего года МВД, Минцифры и Роскомнадзор заявили[1] о необходимости более строгого регулирования дипфейк-технологий: включение в перечень отягчающих обстоятельств использование ИИ при совершении преступлений[2], запрет дипфейков и установление ответственности за незаконный синтез голоса. В США в этом же месяце на федеральном уровне, а также на уровне штатов был выдвинут ряд законопроектов о запрете создания дипфейков от имени госорганов и бизнеса, а также о запрете создания и распространения дипфейка физического лица, имеющего сексуализированный характер, без согласия на это лица.



Тренд №2. Защита прав работников в случаях использования ИИ

США – одна из первых стран, где планируют урегулировать факт использования технологий ИИ при принятии решений в отношении работников. В феврале такие законопроекты рассматривались в сенатах штатов Нью-Джерси, Нью-Йорка, Массачусетса, Иллинойса. Другие страны пока не выпускали схожее регулирование. Сегодня такие программные продукты, в основе которых лежат машинное обучение, ИИ, анализ больших данных, позволяют принимать решения в отношении трудоустройства работника, а также регулировать трудовые отношения с работниками (повышение, увольнение). Идея состоит в том, чтобы обязать работодателей предупреждать работников или соискателей о применении таких технологий, разъяснять как она работает.

Тренд №3. Регулирование квантовых технологий

[1] https://www.vedomosti.ru/technology/articles/2024/02/16/1020587-mintsifri-s-mvd-i-roskomnadzorom-opredelyat-nakazanie-za-dipfeiki
[2] https://pravo.ru/news/251582/

В феврале 2024 г список стран, которые поставили для себя задачу регулирования квантовых технологий, пополнился еще одним государством. Еще с конца 2010 г. в странах мира определена задача поддержки развития квантовых технологий. Для цифровой экономики квантовые технологии дают возможности экспоненциального роста в сфере кибербезопасности и машинного обучения, а также для оптимизации процессов в различных отраслях. США (2018 г.), Китай и Россия (2023 г.) приняли программные документы для развития квантовых технологий, но не законы. В феврале 2024 г. к числу стран, выразивших готовность к регулированию квантовых технологий, присоединилась Великобритания. В связи с увеличением числа стран, развивающих квантовые технологии, формируется запрос на разработку международных правил и стандартов в данной сфере, в том числе с целью трансграничного использования квантовых технологий.

Важно, что принимаемые в настоящее время большинством стран меры в основном направлены на ускорение развития, а не на урегулирование рисков, которые несут квантовые технологии. Это означает, что на текущем этапе вопросы лидерства в данной сфере имеют приоритет перед созданием законодательства. Внимание уделяется стандартизации в области квантовых технологий. Таким образом, страны признают необходимость унификации понятийного аппарата и требований к оборудованию и программному обеспечению, используемых в данной сфере.

Тренд

Развитие регулирования квантовых технологий

Ключевые аспекты

1. Регулирование дипфейков

Опыт США, ЕС и Китая

Дипфейк – это ненастоящее реалистичное представление изображения, речи или поведения человека, созданное с помощью технологии (ИИ или иной) (ОЭСР)[3].

В феврале был предложен ряд законопроектов по регулированию дипфейков. Федеральная торговая комиссия США предложила ввести запрет распространения дипфейков от имени правительства или бизнеса (Impersonation Rule). Чуть ранее было внесено на рассмотрение еще 2 законопроекта – *No AI Fraud Act*[4] (интеллектуальные права лиц на собственные изображение и голос; обязанность третьих лиц, которые хотят сделать цифровые копии изображения или голоса этого лица, брать его согласие), *DEFIANCE Act* (о запрете на создание и распространение сексуализированных дипфейков без разрешения лица).

В соответствии с подходом стран понятие «дипфейк» содержит следующие характеристики:

1) представляют собой имитирование людей (Китай, США, ЕС), а также могут использоваться для создания любых фейковых новостей (Китай);

2) изображения или звуки на самом деле не являются подлинными, например, содержат изображение или голос человека, который говорит или делает то, чего он на самом деле не говорил или не делал;

3) имитация настолько реалистична, что могут показаться разумному человеку правдивыми или подлинными.

При этом, в соответствии с подходом Китая, ЕС и России, дипфейки создаются с помощью ИИ, включая машинное обучение. Законодатели США расширяют подход – дипфейк можно создать не только с помощью ИИ, но и любой другой технологии (например, квантовых вычислений, технологии анализа метаданных) и ПО.

Страны устанавливают следующее регулирование дипфейков:

1. Отдельные виды запретов на дипфейки:
   - запрет на использование дипфейков от имени государственных органов или бизнеса в коммерческих целях (США);
   - запрет на создание и распространение дипфейков сексуализированного, характера, если лицо не дало согласие на создание или распространение таких дипфейков (США);
   - запрет на создание и распространение дипфейков, содержащих запрещенный законодательством контент, либо направленных на запрещенную законодательством деятельность (Китай).
2. Устанавливаются специальные права на собственное изображение и голос лица, которое позволяет передавать такие права третьим лицам (Китай, США).
3. Обязательная маркировка дипфейков (ЕС, Китай).

Фото, голос, видео представляют собой персональные данные человека, поэтому в США, ЕС и Китае также применяются соответствующие законы.

Опыт России

В феврале текущего года МВД, Минцифры и Роскомнадзор заявили[5] о проработке вопросов правового регулирования дипфейк-технологий. При этом месяцем ранее в первом чтении были приняты поправки об уголовной ответственности за использование, передачу, сбор и хранение персональных данных, полученных незаконным путем, и за создание информационных ресурсов, их распространяющих – ст. 272.1 УК РФ[6].

Сегодня предложены следующие подходы к регулированию дипфейков:

[3] https://oecd.ai/en/incidents/58608
[4] https://www.congress.gov/bill/118th-congress/house-bill/6943/text?s=1&r=3
[5] https://www.vedomosti.ru/technology/articles/2024/02/16/1020587-mintsifri-s-mvd-i-roskomnadzorom-opredelyat-nakazanie-za-dipfeiki
[6] https://sozd.duma.gov.ru/bill/502113-8#bh_note

1) включение в перечень отягчающих обстоятельств (ст. 63 УК РФ) при совершении преступлений использование продуктов ИИ[7];

2) запрет дипфейков и ответственность за незаконный синтез голоса.

Подход в России состоит в том, чтобы запретить использование дипфейков, тогда как подход ЕС и Китая – в маркировке дипфейков, чтобы пользователь мог отличить дипфейк от достоверной информации. В США вводится запрет на создание сексуализированных дипфейков без согласия лица и дипфейков от имени госорганов, однако при наличии согласия лица дипфейк может быть создан и распространен.

2. Защита прав работников при использовании ИИ

Опыт США

В США за последние несколько лет произошел ряд судебных тяжб, связанных с дискриминацией работников в связи с использованием решений систем искусственного интеллекта. Например, в 2022 г. в США признали нарушение компанией iTutorGroup Закона о возрастной дискриминации: программное обеспечение на основе ИИ для подбора персонала отклонило более 200 кандидатов старшего возраста. В результате компания выплатила 365 тыс. долл. заявителям, которым было отказано по причине возраста.

По этой причине в США активно развивается тренд регулирования использования ИИ и связанных с ним технологий при принятии решений на рабочем месте. На февраль текущего года такие законопроекты рассматривались в США в сенатах Нью-Джерси[8] и Нью-Йорке [9][10][11], в Массачусетсе[12], в Иллинойсе.

В центре регулирования – использование автоматизированного инструмента принятия решений о приеме на работу (*Automated employment decision tool, далее – AED*). В основе инструмента AED лежит технология ИИ и связанные с ней технологии. Инструмент автоматически фильтрует потенциальных кандидатов при приеме на работу, либо регулирует трудовые отношения с работниками.

Основные цели регулирования: (1) предотвратить дискриминацию на рабочем месте при использовании технологий ИИ и связанных с ним технологий; (2) обеспечить человеческий контроль над инструментами AED и его решениями; (3) обеспечить транспарентность и понимание работы инструментов AED.

Можно выделить следующие направления, которые акцентируются в рамках регулирования:

1) обязательное уведомление кандидата / работника о том, что используется инструмент AED;

2) запрет или ограничение на использование технологий, которые позволяют считывать эмоции или проводить анализ поведения человека;

3) установление человеческого контроля в отношении сгенерированных решений. Так, в Массачусетсе работодатель не может полностью полагаться на решения, сгенерированные инструментом AED, особенно при определении заработной платы сотрудников и принятии решения о найме, продвижении по службе, увольнении или дисциплинарном взыскании;

4) проведение аудита инструментов AED на ежегодной основе. Такой аудит направлен на предотвращение дискриминации работников, включая возраст, расу и пр., и на выявление ошибок, отклонений, нарушений прав работников.

5) введение специального регулирования для работодателей, которые просят соискателей записывать видеоинтервью и проводят анализ таких видеороликов с помощью ИИ, либо используют сервисы распознания лиц.

Опыт России

В России в настоящее время отсутствует регулирование ИИ при найме на работу, хотя в стране распространены подобные технологии (например, используется робот-рекрутер («Вера»).

[7] https://pravo.ru/news/251582/

[8] https://www.njleg.state.nj.us/bill-search/2024/S1588/bill-text?f=S2000&n=1588_I1

[9]https://assembly.state.ny.us/leg/?default_fld=&bn=A07859&term=2023&Summary=Y&Actions=Y&Text=Y&Committee%26nbspVotes=Y&Floor%26nbspVotes=Y#A07859

[10] https://www.nysenate.gov/node/12029882

[11] https://legislation.nysenate.gov/pdf/bills/2023/s7623a

[12] https://malegislature.gov/Bills/193/H1873

В России можно рекомендовать дополнить Трудовой кодекс (197-ФЗ) ст. 22.4 закрепив право работника или соискателя знать, что работодатель использует автоматизированные инструменты принятия решений на основе ИИ или других аналогичных технологий, установить запрет на использование таких технологий в целях дискриминации работника, либо в целях, не связанных с трудовыми. Также важно проведение аудита автоматизированных технологий.

3. Развитие регулирования квантовых технологий

Еще в начале 2022 г. *WEF* выделил риски применения квантовых вычислений[13]:

1. Отсутствие субъекта ответственности за действия в связи с процедурами трансформации/изменения или управления при разработке либо внедрении технологий квантовых вычислений;

2. Риски в сфере безопасности:

– механизмы валидации или авторизации, основанные на существующих криптографических методах, например, электронные подписи могут быть нарушены квантовыми технологиями;
– дестабилизация протоколов управления критической инфраструктурой, в том числе основанных на технологии блокчейн;
– риски конфиденциальности, управления данными и т.п.;

3. Риски для персональных данных:

– киберугрозы, исходящие от квантовых компьютеров, в отношении персональных данных, не защищенных безопасной в отношении квантовых технологий криптографией;
– использование мощных алгоритмов анализа для прогнозирования или получения информации без согласия либо авторизации из наборов данных, содержащих персональные данные, в том числе числе путем объединения квантовых компьютеров с другими технологиями, как ИИ.

4. Риск в сфере регулирования интеллектуальной собственности: какими инструментами (патентное, авторское право) и какие элементы технологии защищаются, на какие сроки распространяется защита[14].

Вместе с тем регулирование квантовых технологий в странах мира пошло по другому пути: его преимущественной задачей стало не сокращение данных рисков, а ускорение развития квантовых технологий, в том числе через стандартизацию.

Опыт Великобритании

В феврале Великобритания стала еще одной страной, которая выразила готовность к разработке регулирования квантовых технологий, но не закрытия рисков, о которых говорит *WEF*.[15] Ранее в США был принят Закон о национальной квантовой инициативе (No. 115-368)[16], который поставил цель по развитию квантовых исследований и стандартизации в квантовой сфере, включая вопросы кибербезопасности и защиты данных. В Китае – еще одной стране, претендующей на лидерство в сфере квантовых технологий, в 2023 г. вступил в силу первый в мире национальный стандарт «Квантовые вычисления – терминология и определения». Таким образом и Китай, и США сконцентрировались не на рисках и вызовах технологии, а на стандартизации понятий, используемых в квантовой индустрии, для ускорения ее развития. Великобритания этот тренд поддержала.

В отношении регулирования в Великобритании даны следующие рекомендации:

1) создание испытательных стендов (*testbeds*) и песочниц (*sandboxes*), включающих регуляторные компоненты для выявления и имплементации мер по смягчению проблем безопасности, создаваемых квантовыми компьютерами в сфере криптографии;

2) запуск пилотной сети по квантовым стандартам (*UK Quantum Standards Pilot Network*), в том числе для стандартизации квантовых коммуникаций, включая стандарты совместимости.

[13] Quantum Computing Governance Principles. Insight report. World Economic Forum. January 2022. – https://www3.weforum.org/docs/WEF_Quantum_Computing_2022.pdf.
[14] https://www.allenovery.com/en-gb/global/news-and-insights/publications/the-opportunities-and-legal-risks-of-quantum-computing.
[15] https://www.gov.uk/government/publications/regulatory-horizons-council-regulating-quantum-technology-applications.
[16] https://www.congress.gov/bill/115th-congress/house-bill/6227/text.

Опыт России

В июле 2023 г. В России была утверждена Концепция регулирования отрасли квантовых коммуникаций до 2030 г. для определения основных подходов нормативного регулирования отрасли квантовых коммуникаций, включая квантовую криптографию. Планируется выработка стандартов информационной безопасности; национальных стандартов, регламентирующих единые требования к оборудованию, программному обеспечению и методам их испытания; закрепление понятийного аппарата отрасли квантовых коммуникаций; проведение исследований в рамках экспериментальных правовых режимов в сфере цифровых инноваций. Таким образом, на текущем этапе развития регулирования квантовых технологий российская практика находится в русле мировых тенденций.