ЕС ставит под сомнение законность обработки данных ChatGPT.

Европейский совет по защите данных (EDPB), более года изучавший, как правила защиты данных Евросоюза применяются к популярному чат-боту ChatGPT – это чат-бот, который работает на модели искусственного интеллекта GPT (Generative Pre-trained Transformer), разработанной компанией OpenAI. Модель обучена на большом объёме текстовых данных и предназначена для генерации человекоподобных ответов на заданные вопросы или фразы.

 ChatGPT всегда старается понять контекст вопроса и сгенерировать подходящий ответ. Чат-бот способен генерировать текст в различных стилях и тематиках, может использоваться в различных сферах и областях для облегчения рутинных или даже творческих задач, выполняемых человеком.

 Несмотря на всю «крутость» платформы, ChatGPT может давать неточные или неправильные ответы. Также нейросеть может проявлять предвзятость или генерировать контент, который не соответствует этическим нормам. Поэтому ChatGPT необходимо использовать с осторожностью и критически оценивать любую получаемую информацию." data-html="true" data-original-title="ChatGPT" >ChatGPT, представил предварительные выводы расследования.

Регуляторы все еще не определились с ключевыми юридическими аспектами – законность и справедливость обработки данных OpenAI – это компания, которая занимается исследованиями и разработкой в области искусственного интеллекта. Она была основана в 2015 году и создана с целью сделать искусственный интеллект более доступным и безопасным для людей. Компания разрабатывает и использует нейронные сети и другие методы искусственного интеллекта для решения различных задач, включая анализ данных, генерацию текста, голоса, изображений и т.д." data-html="true" data-original-title="OpenAI" >OpenAI. Вопрос имеет критическое значение, так как штрафы за подтвержденные нарушения могут достигать 4% от глобального годового оборота компании.

Надзорные органы могут приказывать прекратить обработку данных, если она не соответствует требованиям. Теоретически, OpenAI сталкивается с серьезным регуляторным риском в регионе, когда специальные законы для ИИ все еще разрабатываются.

Без четких указаний со стороны европейских регуляторов по защите данных о том, как текущие законы применяются к ChatGPT, OpenAI, вероятно, будет продолжать свою деятельность без изменений, несмотря на растущее число жалоб на нарушение GDPR — это регламент, введенный ЕС в 2018 году для того, чтобы дать пользователям больше контроля над своими личными данными. Он применяется ко всем организациям,

которые обрабатывают личные данные жителей ЕС. Компании должны выполнять следующие требования:
  получать согласие пользователя на обработку персональных данных; предоставлять свободный доступ к данным; принимать меры безопасности; уведомлять соответствующие органы об утечках данных; назначать ответственного за организацию обработки персональных данных (DPO). Несоблюдение правил регламента может привести к крупным штрафам." data-html="true" data-original-title="GDPR" >GDPR. Например, в Польше расследование началось после жалобы на то, что чат-бот придумал информацию об одном человеке и отказался исправить ошибки. Подобная жалоба недавно поступила и в Австрии.

Согласно GDPR, обработка персональных данных допустима только при наличии законного основания. Однако в случае с OpenAI большинство оснований неприменимы. Итальянский орган по защите данных уже указал, что OpenAI не может ссылаться на договорную необходимость для обработки данных людей для обучения своих моделей, оставив лишь два возможных законных основания: согласие пользователей или законные интересы.

После вмешательства Италии, OpenAI перешла к утверждению, что у нее есть законные интересы для обработки персональных данных, используемых для обучения моделей. Однако в январе итальянский орган обнаружил нарушение GDPR со стороны OpenAI, хотя детали пока не разглашаются.

В отчете рабочей группы обсуждаются этапы обработки данных, включая сбор данных для обучения, предварительную обработку, само обучение, запросы пользователей и ответы ChatGPT. Три первых этапа несут особые риски для фундаментальных прав людей.

Рабочая группа рекомендует применять «адекватные меры безопасности», такие как технические меры и ограничение сбора данных, чтобы минимизировать влияние на частную жизнь. Также предлагается удалять или анонимизировать персональные данные, собранные через веб-скрейпинг, до этапа обучения. OpenAI должна четко информировать пользователей о том, что их запросы могут использоваться для обучения.

Без четких рекомендаций от регуляторов, как улучшить возможности пользователей по реализации своих прав на данные, ситуация остается неопределенной. Рабочая группа лишь общими словами рекомендует OpenAI применять «адекватные меры», чтобы соответствовать требованиям GDPR.

Рабочая группа была создана в апреле 2023 года после вмешательства итальянского регулятора, чтобы координировать применение правил защиты данных к новым технологиям. Несмотря на независимость регуляторов, видна некоторая осторожность в их действиях. Например, польский регулятор в интервью местным СМИ намекнул, что его расследование в отношении OpenAI будет ждать завершения работы рабочей группы. В то время как представитель EDPB отметил важную роль группы в содействии сотрудничеству между регуляторами.

OpenAI открыла представительство в Ирландии, чтобы воспользоваться механизмом, который позволяет сосредоточить рассмотрение жалоб на нарушение GDP в одном регуляторе. Ирландский регулятор славится дружелюбным отношением к крупным технологическим компаниям, что может сыграть на руку OpenAI.

Пока не ясно, как быстро и эффективно регуляторы будут действовать в отношении ChatGPT. На фоне множественных жалоб и медленной реакции надзорных органов, будущее OpenAI в Европе остается неопределенным. OpenAI пока не дала комментариев на запрос по поводу предварительного отчета рабочей группы EDPB.