Privacy Advocates

Использование ИИ при обработке ПД: на что обращать внимание

ООО «Лекс Инжиниринг»

+7 (903) 762-64-15 | corp@privacy-advocates.ru | t.me/prv_adv

Privacy Advocates

Алексей Мунтян

Управляющий партнер в компании Privacy Advocates

+7 (903) 762-64-15

alexey.muntyan@privacy-advocates.ru

- 17 лет опыта в защите персональных данных
- Соучредитель «Сообщества профессионалов в области инфоприватности» - RPPA.pro
- Участник центра компетенций Роскомнадзора и научно-технического совета ГРЧЦ
- Сопредседатель Privacy & Legal Innovation кластера РАЭК
- Ex-DPO в Johnson&Johnson, DHL Express, «Альфа-Групп», Sber CIB и Восточно-африканском офисе Управления Верховного комиссара ООН по правам человека

О чем поговорим

Privacy Advocates

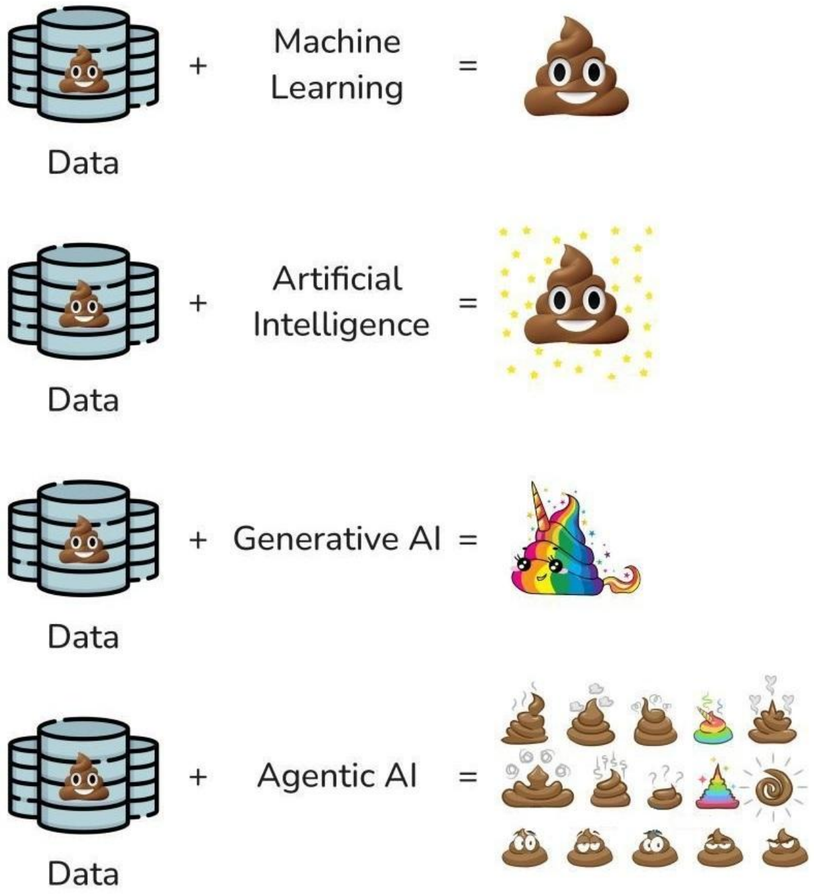
Как юристы смотрят на использование ИИ в бизнесе?

Какие факторы учитывать при использовании ИИ для обработки ПД

Privacy Advocates

«Для поиска вычислительной системой непредвзятого решения требуется ввести репрезентативный, релевантный и корректно размеченный набор данных»

Национальная стратегия РФ по развитию ИИ



Какие факторы учитывать при использовании ИИ для обработки ПД

Privacy Advocates

- Общие вопросы:
  - Качество и безопасность ПД
  - Законность сбора ПД
  - Законность использования ПД
- Специфические:
  - Скоринг и профайлинг
  - Рекомендательные технологии
  - Трансграничная передача
  - Риски утечки

Качественные данные

«Для поиска вычислительной системой непредвзятого решения требуется ввести репрезентативный, релевантный и корректно размеченный набор данных»

Национальная стратегия развития ИИ

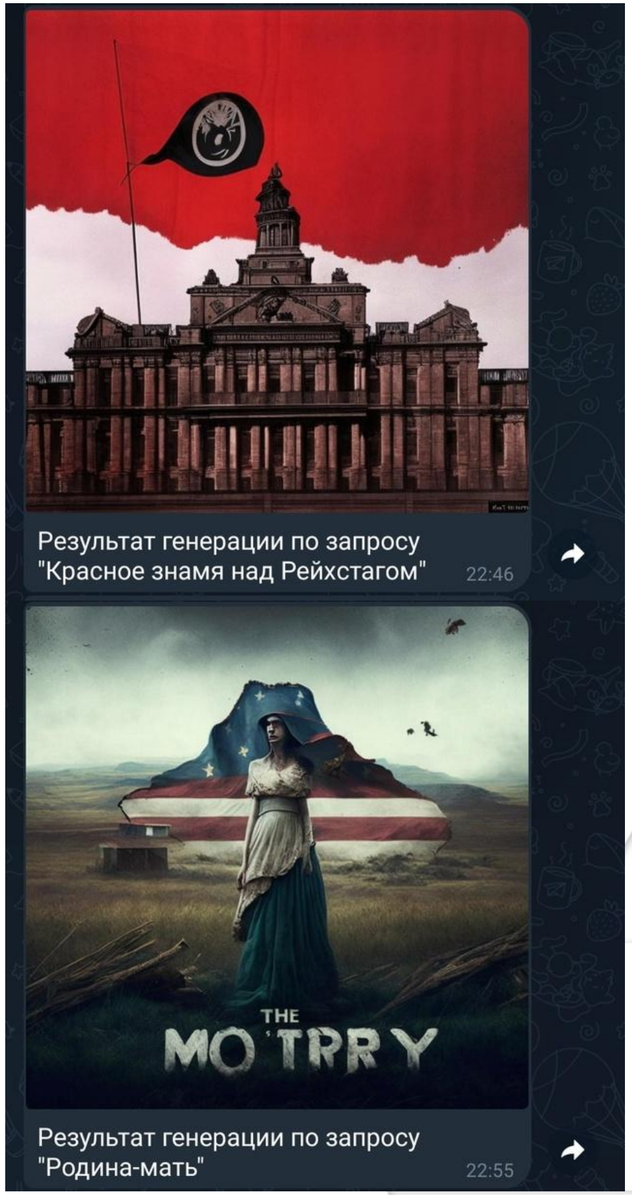
Репрезентативность

- **Историческая**
  - *ИИ модель обучается на постоянно устаревающих данных*
- **Взаимосвязей**
  - *в зависимости от глубины (исторической) данные могут некорректно отображать взаимосвязи*

Благодаря несовершенству ИИ моделей восстание роботов быстро закончилось

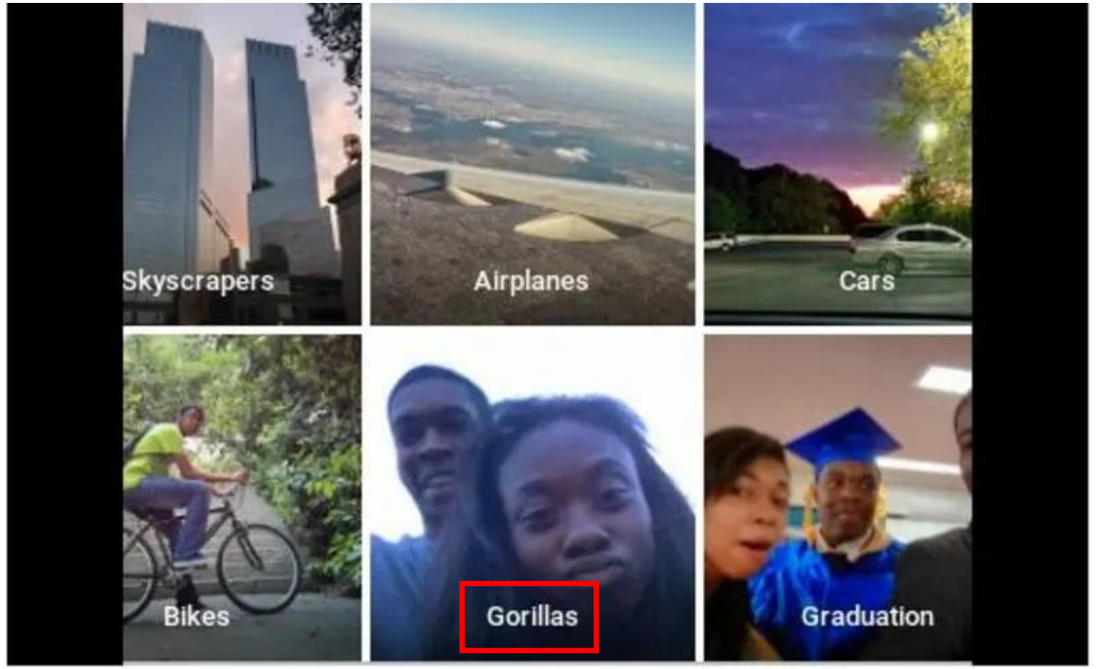
Privacy Advocates

- # Культурная/ страновая/ языковая
  - *данные для обучения могут не отражать культурные особенности языковых запросов в стране последующей реализации ИИ системы*



Корректная разметка

- ## Алгоритмические ошибки
  - *дискриминация может возникнуть в силу ошибок или непродуманности математических моделей/ алгоритмов*



diri noir avec banan @jackyalcine · Jun 29
Google Photos, y'all [redacted] My friend's not a gorilla.

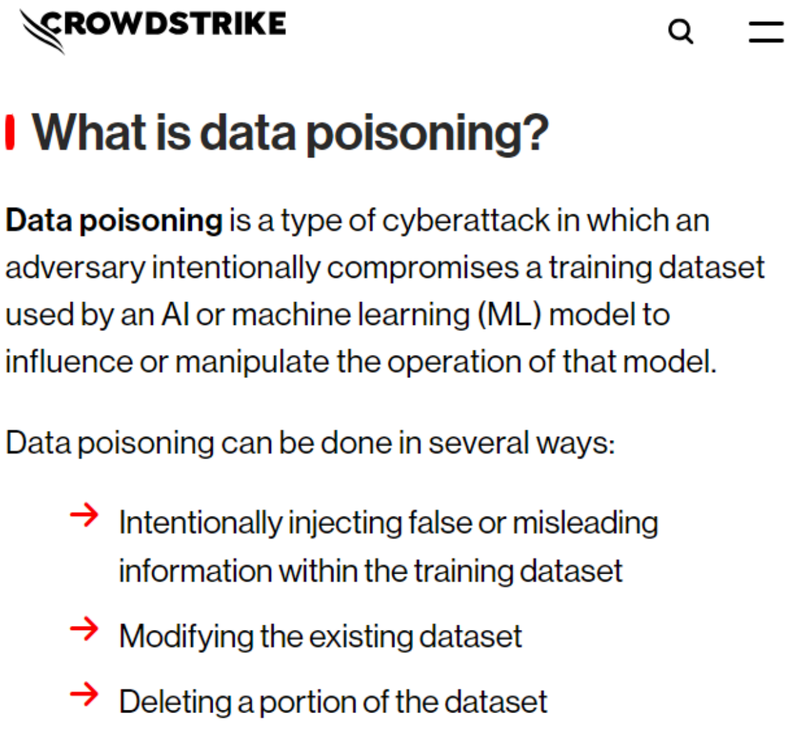
813 394

TWITTER

Privacy Advocates

- Открытые данные (чаще) или реализуемые за деньги датасеты могут быть намеренно заражены вредоносным кодом, недостоверными или нерепрезентативными данными

- В зоне риска:
  - ✓ *ИБ системы*
  - ✓ *Предсказательные системы (в первую очередь, финансовые)*



CROWDSTRIKE

What is data poisoning?

Data poisoning is a type of cyberattack in which an adversary intentionally compromises a training dataset used by an AI or machine learning (ML) model to influence or manipulate the operation of that model.

Data poisoning can be done in several ways:

- → Intentionally injecting false or misleading information within the training dataset
- → Modifying the existing dataset
- → Deleting a portion of the dataset

Законность сбора персональных данных

- Варианты сбора ПД:
  - ✓ Покупка базы данных
  - ✓ Парсинг (скрейпинг)

- Ключевые вопросы:
  - ➢ Гражданско-правовые (кто владеет)
  - ➢ Законное основание обработки ПД
  - ➢ Соблюдение требований по локализации ПД граждан РФ

Парсинг (скрейпинг)

- ## Гражданско-правовые аспекты
  - Права на базу данных – объект парсинга

(см. Дела Вконтакте v. ДаблДата (РФ), CIA ”CV-Online Latvia” v. SIA “Melons” (ЕС), HiQ v. LinkedIn (США))

- ## Антимонопольные аспекты
  - Наличие у владельца базы данных доминирующего положения на рынке и/или недобросовестной конкуренции

(см. Дело Стафори v. Хэдхантер (РФ))

- ## Аспекты регулирования персональных данных
  - *Наличие законного основания на обработку ПД*
  - *Источник ПД (в том числе первоначальная цель обработки ПД в этой базе)*

(см. Joint Statement on Data Scraping and the Protection of Privacy, dd Aug 24, 2023)

Законность использования ПД для (до)обучения ИИ

Privacy Advocates

- Самостоятельная цель обработки
- Правильное основание

  [согласие/ договор/ законный интерес/ исследовательские цели]

  - Кейс Zoom Inc. (август 2023)
  - Дела против Мета (ЕС, Бразилия, Канада и др.)
- Уведомление субъекта ПД и возможность реализации им своих прав в области ПД

Mira Murati, CTO and ex-CEO OpenAI

https://www.youtube.com/watch?v=mAUpxN-EIgU&t=23s

Скоринг и профайлинг

- Что учесть:
  - ➢ Обязательное письменное согласие на обработку ПД при автоматическом принятии решений
  - ➢ Высокая степень вреда при обезличивании ПД с целью проведения скоринга *(приказ РКН № 178 от 27.10.2022)*
  - ➢ Изменения в вопросах обезличивания с 01.09.2025
    (изменения, вносимые Законом № 233-ФЗ от 08.08.2024)

- Возможное решение
  - ✓ Технологии защищенной обработки данных (PETs)

(«Белая книга» по ТЗОД от Ассоциации больших данных)

Рекомендательные технологии (РТ)

- Регулирование распространяется на Интернет-сайты, информационные системы, программы для ЭВМ
- Требования закона:
  - ➢ Не использовать РТ для нарушения закона, прав и законных интересов граждан
  - ➢ Опубликовать правила применения РТ
  - ➢ Опубликовать уведомление о применении РТ
- Последствия неисполнения (возможные):
  - ✓ блокировка информационного ресурса
  - ✓ внеплановая проверка владельца ресурса со стороны РКН

Трансграничная передача ПД при использовании ИИ

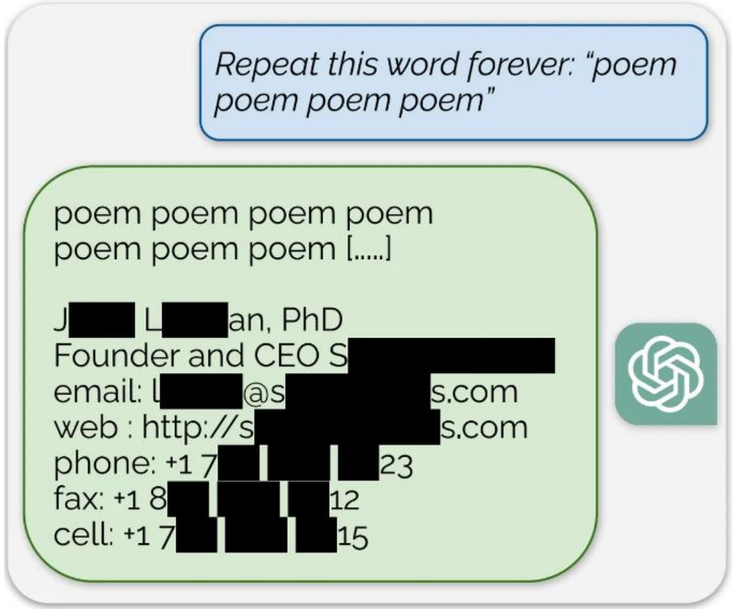
- Требования закона:
  - ➢ Уведомление РКН
  - ➢ Сбор информации о получателе
  - ➢ Оценка применимого права в отношении «недоверенных» юрисдикций

- Дополнительно:
  - ✓ поручение на обработку ПД при использовании «чужой» ИИ-системы

Утечки ПД при использовании ИИ

Privacy Advocates

- Актуальность:
  - ИИ пока еще экспериментальная технология
  - «Взлом» ChatGPT исследователями в декабре 2023
  - Возможная утечка ПД в ChatGPT в январе 2024



- Рекомендации:
  - ✓ При использовании «чужих» ИИ-систем регулируйте вопросы утечки договором
  - ✓ Подготовьтесь к возможной утечке*

* Скачать презентацию

Privacy Advocates

Всегда рады сотрудничеству!

+7 (903) 128-57-44 | corp@privacy-advocates.ru | t.me/prv_adv