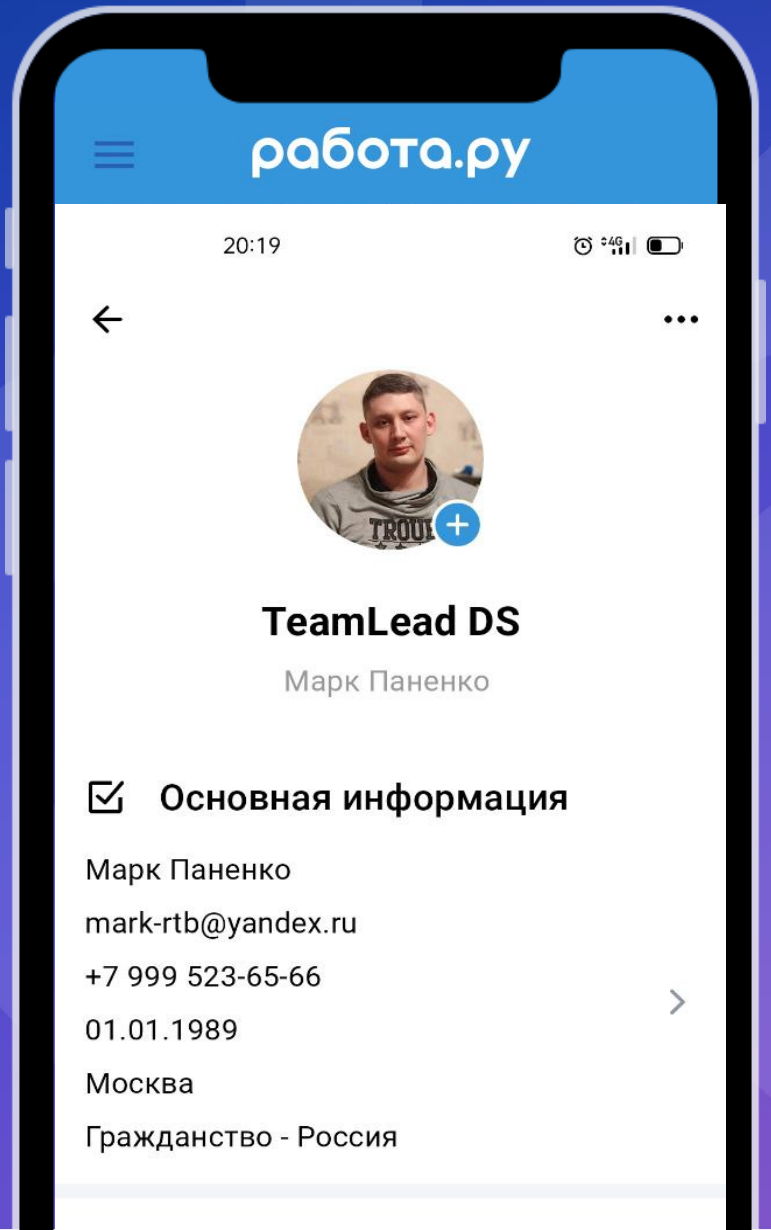
работа.ру

"Конфиденциальность персональных данных в машинном обучении: проблемы и решения"

работа.ру

Марк Паненко

- **Team Lead – Rabota.ru (Saint-Petersburg)**
- **Machine learning Teacher ITMO University**



работа.ру

правовые проблемы в машинном обучении

правовые проблемы в машинном обучении

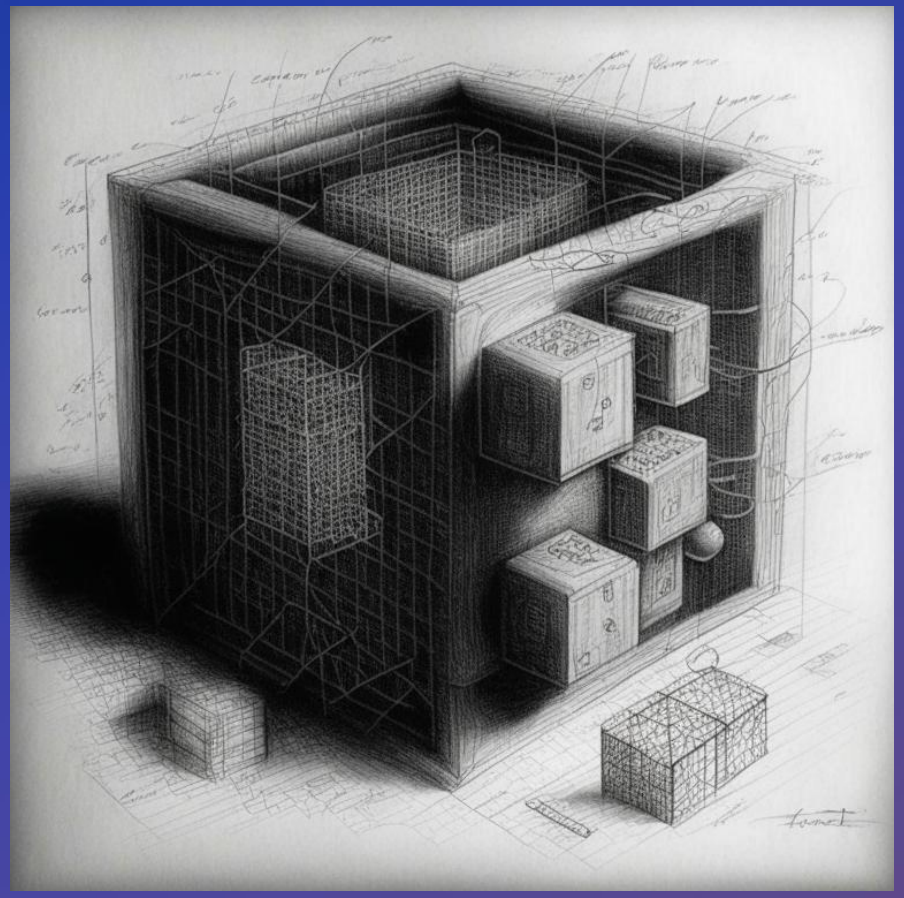
1. Нарушение прав на конфиденциальность и защиту персональных данных

правовые проблемы в машинном обучении

1. Нарушение прав на конфиденциальность и защиту персональных данных
2. Алгоритмическая дискриминация

правовые проблемы в машинном обучении

1. Нарушение прав на конфиденциальность и защиту персональных данных
2. Алгоритмическая дискриминация
3. Непрозрачность работы алгоритмов



правовые проблемы в машинном обучении

1. Нарушение прав на конфиденциальность и защиту персональных данных
2. Алгоритмическая дискриминация
3. Непрозрачность работы алгоритмов
4. Предвзятость данных и признаков

работа.ру

проблема конфиденциальности персональных данных в ML

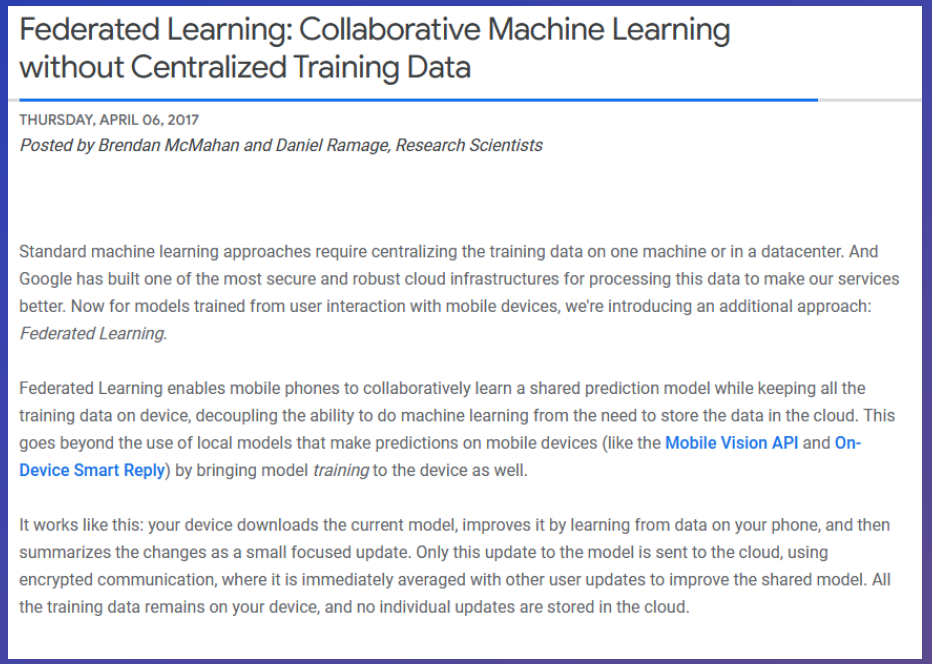
проблема конфиденциальности персональных данных в ML

Существует множество моделей машинного обучения, которые обучаются на глубоко личных данных. Хранить такие данные централизованно, может быть довольно опасно или невозможно с точки зрения закона.

проблема конфиденциальности персональных данных в ML

В 2017 году компания Google опубликовала очень интересную статью

Компанией было предложено рассмотреть вопрос: что если вместо сбора данных в одном месте, попытаться перенести модель в данные?



Federated Learning: Collaborative Machine Learning without Centralized Training Data

THURSDAY, APRIL 06, 2017

Posted by Brendan McMahan and Daniel Ramage, Research Scientists

Standard machine learning approaches require centralizing the training data on one machine or in a datacenter. And Google has built one of the most secure and robust cloud infrastructures for processing this data to make our services better. Now for models trained from user interaction with mobile devices, we're introducing an additional approach: *Federated Learning*.

Federated Learning enables mobile phones to collaboratively learn a shared prediction model while keeping all the training data on device, decoupling the ability to do machine learning from the need to store the data in the cloud. This goes beyond the use of local models that make predictions on mobile devices (like the Mobile Vision API and On-Device Smart Reply) by bringing model *training* to the device as well.

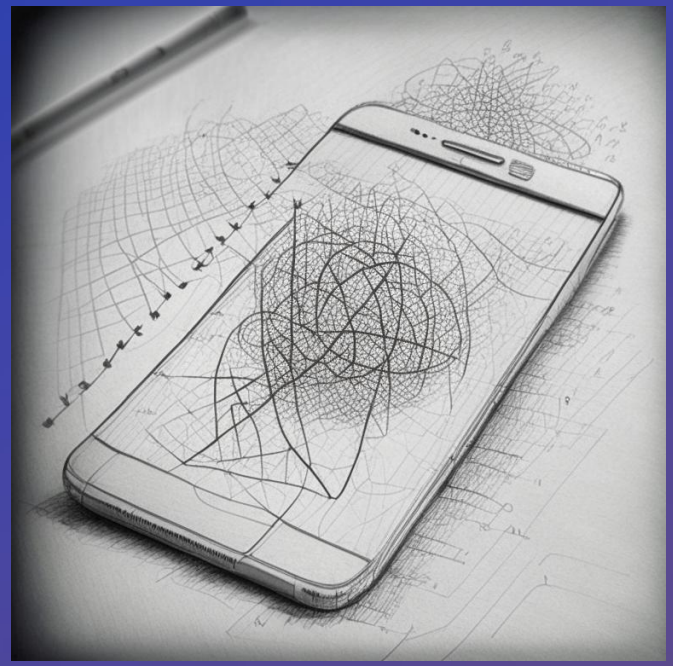
It works like this: your device downloads the current model, improves it by learning from data on your phone, and then summarizes the changes as a small focused update. Only this update to the model is sent to the cloud, using encrypted communication, where it is immediately averaged with other user updates to improve the shared model. All the training data remains on your device, and no individual updates are stored in the cloud.

проблема конфиденциальности персональных данных в ML

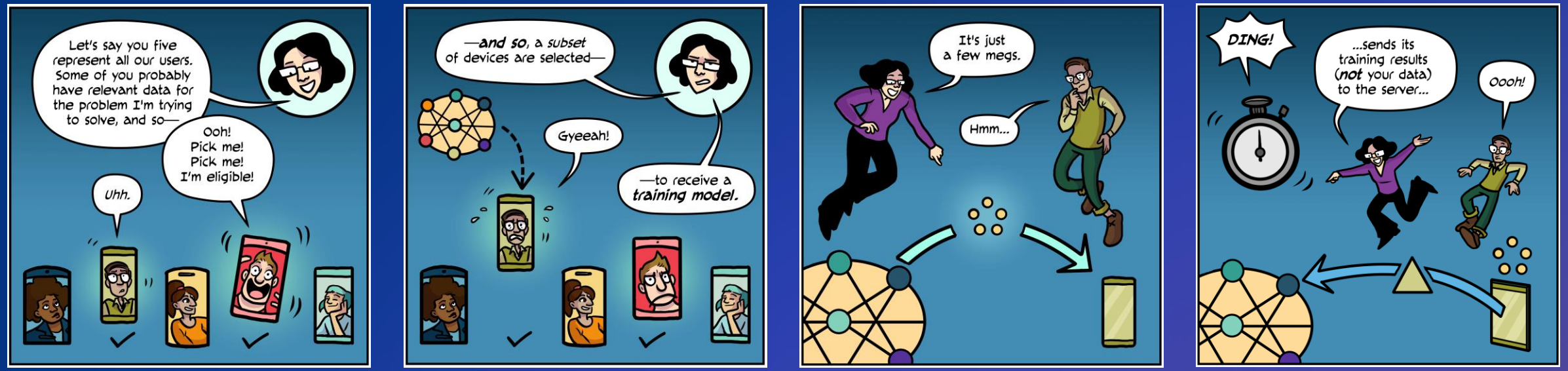
В 2017 году компания Google опубликовала очень интересную статью

Компанией было предложено рассмотреть вопрос: что если вместо сбора данных в одном месте, попытаться перенести модель в данные?

Этот новый раздел машинного обучения получил название федеративное обучение (federated learning)

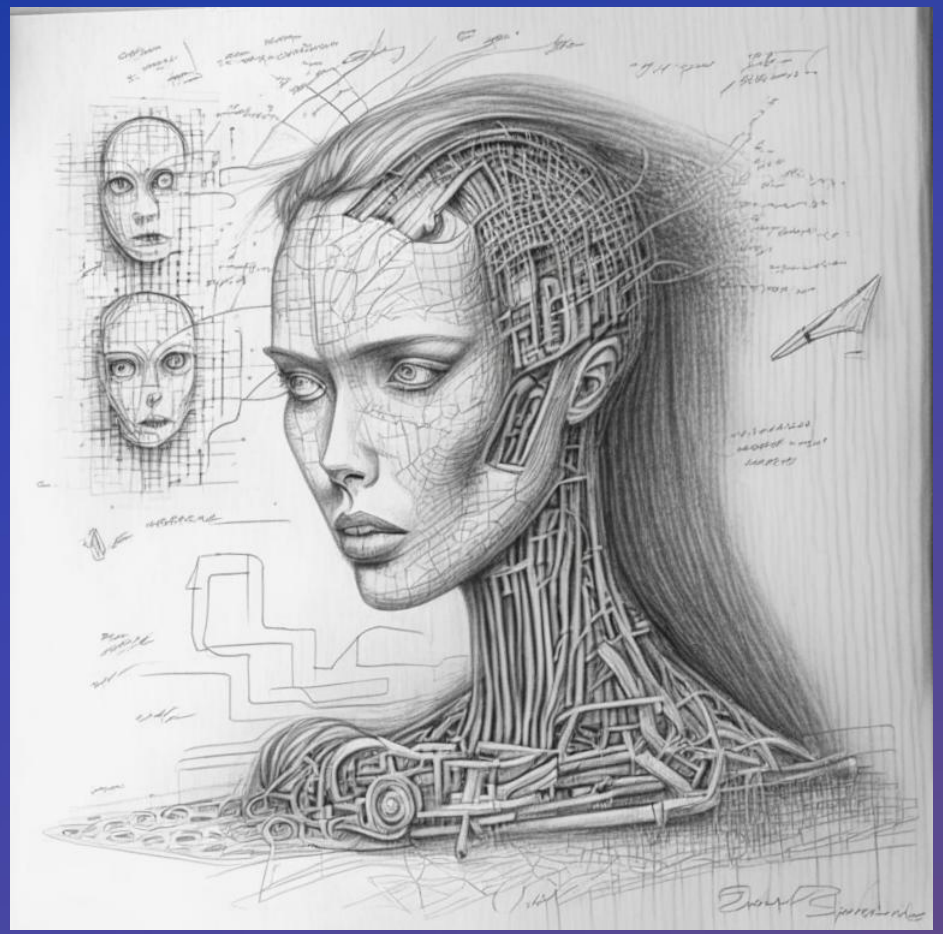


Федеративное обучение



Федеративное обучение

Можно ли взломать такую модель?



Федеративное обучение

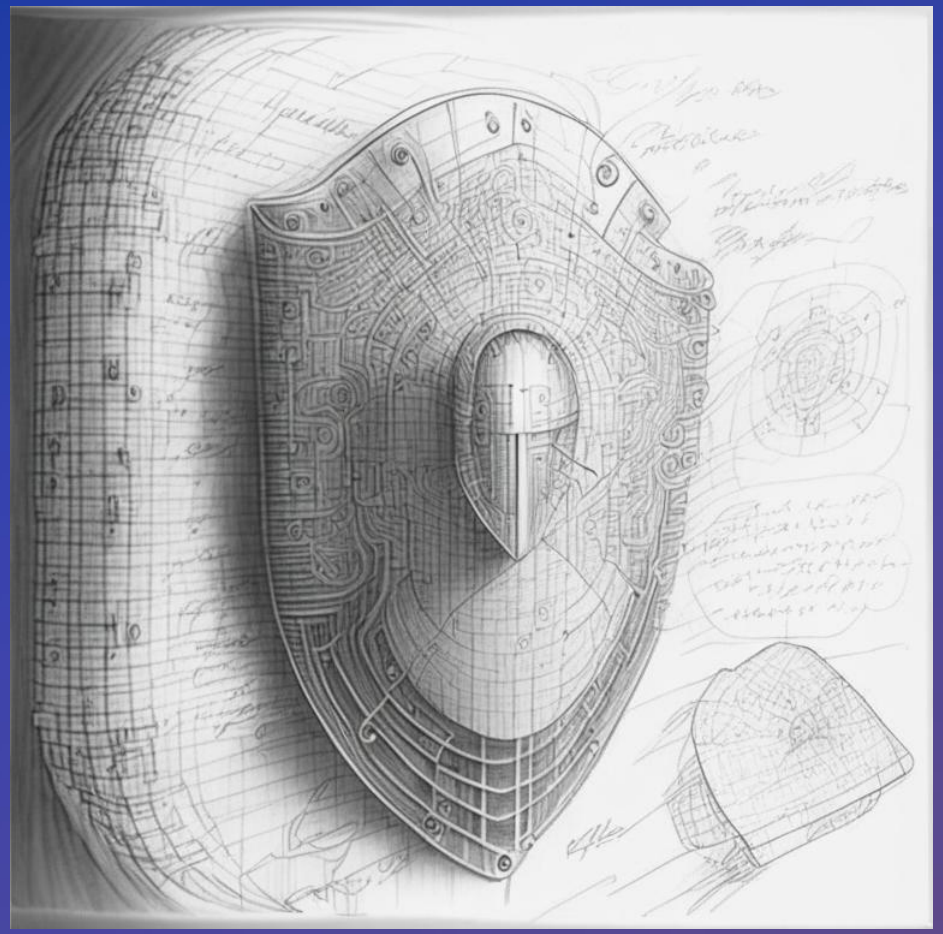
Можно ли взломать такую модель?

Да!

Посмотрев, какие
весовые коэффициенты изменились

Федеративное обучение

Можно ли защититься от взлома ?

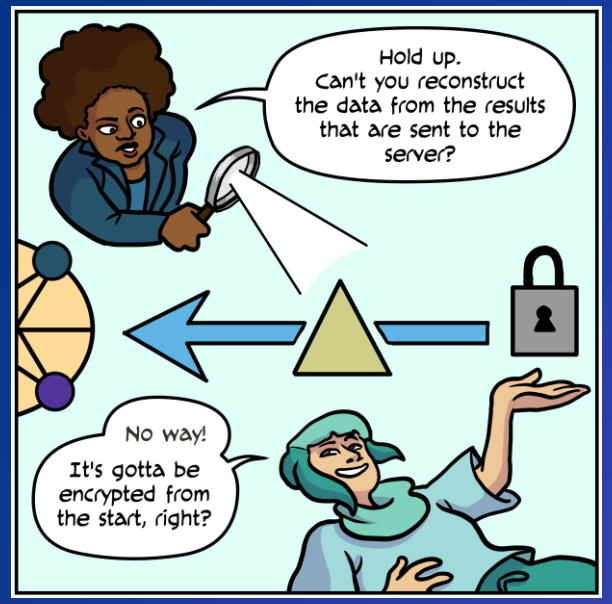


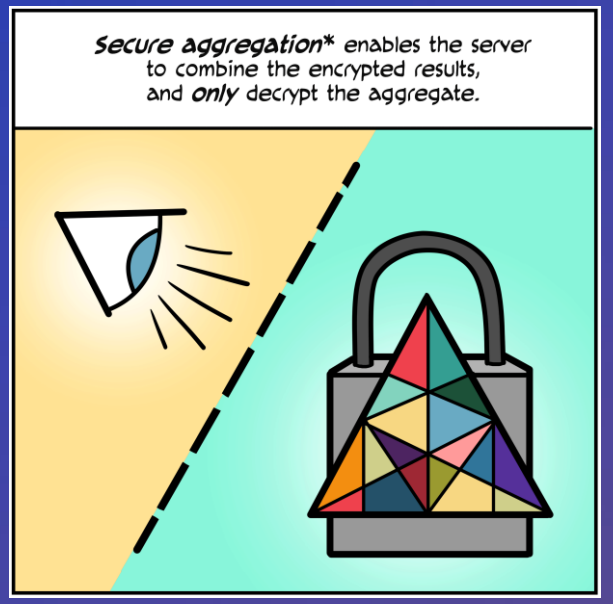
Федеративное обучение

Можно ли защититься от взлома ?

Да!

С помощью Гомоморфного шифрования и агрегирования

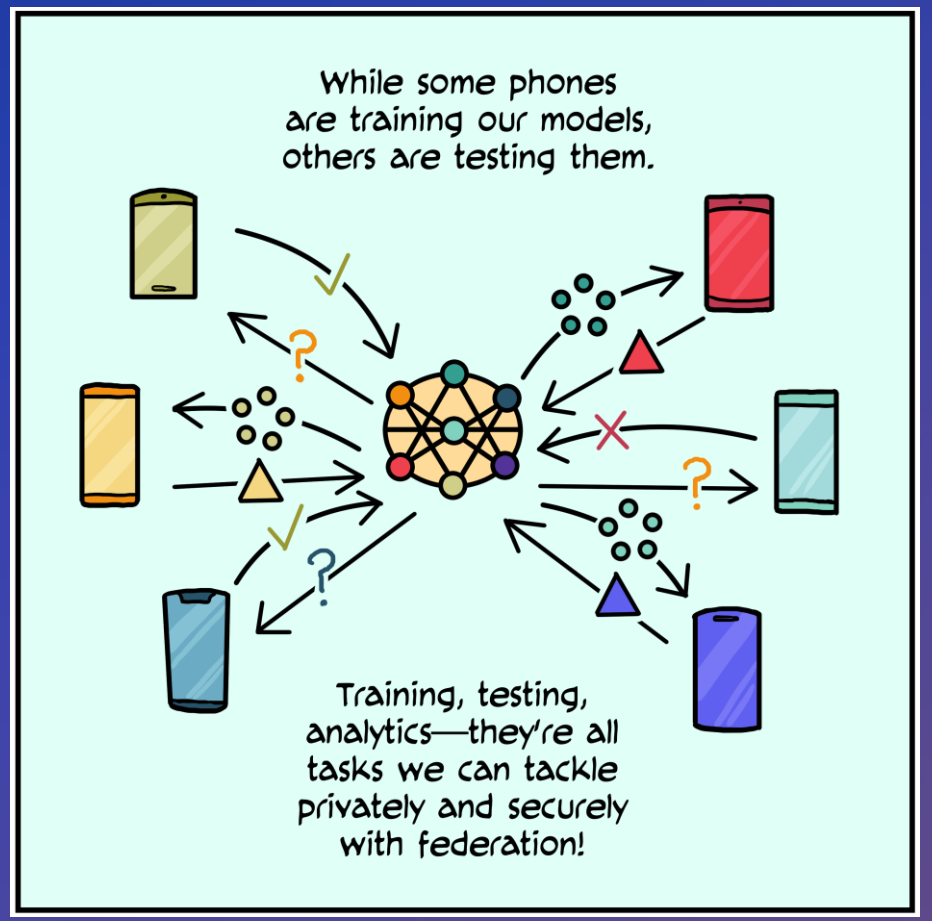




Федеративное обучение

Итоги:

Федеративное обучение позволяет обучать и тестировать модели машинного обучения, не имея централизованных датасетов. Что упрощает работу с чувствительными данными и повышает безопасность как пользователей так и бизнеса.



работа.ру

Перейдем к обсуждению!

telegram: @mark_rtb
email: m.panenko@rabota.ru