ID de Contribution: **1** Type: **Non spécifié**

# Keynote d'ouverture : Sujet sur l'utilisation des données personnelles avec l'IA

*jeudi 21 novembre 2024 09:35 (40 minutes)*

La protection des données personnelles est souvent en opposition avec la collecte massive pour l'entraînement des modèles d'apprentissage automatique.
L'apprentissage fédéré ou décentralisé réduit les risques de fuites de grandes bases de données : il permet l'entraînement de modèles via la collaboration des utilisateurs, sans centraliser directement leurs données.
Cependant, des risques comme la mémorisation involontaire de données persistent et doivent être pris en compte pour assurer une protection efficace des utilisateurs.
La confidentialité différentielle fournit des garanties mathématiques visant à formaliser cette protection.

**Orateur:** Mme CYFFERS, Edwige (CRIStAL)