Veille technologique – PANAME

L'intelligence artificielle se développe grâce à la collecte de données (textes, images, vidéos...). Cela pose un risque pour la vie privée lorsqu'elle peut révéler des données personnelles notamment au regard de la RGPD. C'est pour cela que le projet PANAME répond à ce problème.

Pour répondre à cette problématique, la Commission nationale de l'informatique et des libertés (CNIL), en partenariat avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et Inria, a créé le projet PANAME. L'objectif est de développer un outil technique permettant de tester si un modèle d'IA peut faire ressortir des données personnelles issues de son utilisation. Cet outil doit aider les organisations à vérifier concrètement la conformité de leurs modèles au RGPD. L'ANSSI et Le CNIL mettent en place cette outils sous forme de demande de la part des organisations pour tester leur prototype en situations réels et permette d'éventuelle amélioration et point à corriger. Ce projet montre une évolution importante : la conformité des systèmes d'IA ne repose plus uniquement sur des faits juridiques, mais aussi sur des tests techniques mesurables pour vérifier leur validité.

La performance des modèles d'IA repose sur la collecte de données. Toutefois, ces pratiques peuvent créer des risques pour la vie privée si des données personnelles sont révélées. Le projet PANAME illustre une nouvelle approche : vérifier techniquement les modèles pour garantir leur conformité au RGPD et mieux protéger les individus.

Sources :

- https://www.cnil.fr/fr/projet-paname-participez-aux-tests-dun-outil-daudit-rgpd-des-modeles-dia
- https://www.lemondeinformatique.fr/actualites/lire-l-anssi-et-la-cnil-appellent-a-tester-leur-outil-d-audit-de-confidentialite-des-modeles-ia-99497.html
- https://www.usine-digitale.fr/article/lancement-du-projet-paname-face-au-risque-de-memorisation-indesirable-des-ia.N2234311