CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

Utilisations de l'IA dans le domaine de la santé
Quels défis pour la CNIL ?

Félicien Vallet

CNIL et IA

- Rapport éthique (2017)
  - Un grande consultation publique
    - 3000 personnes
    - 60 événements
    - Universités, syndicats, administrations, fédérations, etc.
  - Deux piliers :
    - Loyauté
    - Vigilance
  - Six recommandations
- Une approche *top-down* inhérente à ce type de rapports

CNIL.

LES QUESTIONS QUE L'IA POSE À LA CNIL

Colloque DRIAS

22 juin 2021

Les questions que l'IA pose à la CNIL

Exemple illustratif n°1

- **DATAJUST :** demande d'avis soumise à la CNIL concernant la mise en œuvre par le ministère de la Justice d'un algorithme charger de recenser les montants alloués en indemnisation du préjudice corporel des victimes et de proposer des référentiels pour les professionnels et le grand public.

  - Comment s'assurer de l'absence de biais potentiellement préjudiciables ?
  - Quelles mesures et pratiques à recommander pour éliminer ou a minima réduire ce risque ?

Les questions que l'IA pose à la CNIL

Exemple illustratif n°2

- **Startup ABC :** suite à un contrôle, la CNIL a constaté que des données personnelles avaient été illégalement collectées et avaient servi à l'apprentissage d'un modèle d'IA.

  - Quel statut légal pour cet objet ?
  - Donnée(s) personnelle(s) ou anonyme(s) ?

Les questions que l'IA pose à la CNIL

Exemple illustratif n°2 bis

- **Startup DEF :** demande de conseil d'une société commercialisant un outil mettant en œuvre des méthodes d'apprentissage automatique pour le codage des actes médicaux (codage PMSI)

  - Ok pour déploiement dans un centre X si l'apprentissage et le modèle restent dans les locaux du centre.
  - La startup peut-elle transférer le modèle appris dans le centre X dans un centre Y et l'y adapter ?
  - Si envisageable, quelles mesures et pratiques recommander pour pouvoir minimiser les risques ?

Les questions que l'IA pose à la CNIL

Exemple illustratif n°3

- **Laboratoire pharmaceutique GHI:** demande d'autorisation pour réaliser une étude observationnelle portant sur le cancer de la prostate et la réutilisation des dossiers médicaux électroniques. Pour cela, le traitement de toute la file active des patients reçus dans les centres testés, patient atteints ET non-atteints devait être utilisées pour collecter un nombre important de « vrais négatifs » (> 100 millions de dossiers médicaux incluant ceux de personnes de sexe féminin)

  - Refus de la CNIL pour non-respect du principe de minimisation.
  - Ou placer le curseur ?

Les questions que l'IA pose à la CNIL

Exemple illustratif n°4

- **Startup JKL:** Demande de conseil sur une solution de détection automatisée du vol en magasin. Le fournisseur de solution souhaiterait accéder au données de vidéoprotection dont dispose son client pour entrainer son système.

  - Comment encadrer la constitution de données d'apprentissages issus de caméras de vidéoprotection ?
  - Quelles modalités pour « anonymiser » les données vidéos (floutage, masquage de l'arrière-plan, post-traitements colorimétriques, utilisation de GANs pour substitution de visages) ?

CNIL.

LES ACTIONS DE LA CNIL (EN COURS ET À VENIR)

Projet de régulation de l'IA (1)

- **2017-2020 :** prises de positions du Conseil européen et du Parlement
- **2018-2020 :** constitution et travaux du AI HLEG (52 experts)
  - Concept de "Trustworthy AI"
  - Publication de guidelines (*HLEG Ethics Guidelines for Trustworthy AI*)
  - Publication de l'outil ALTAI : Assessment List for Trustworthy AI (testedby 350 organisations)
- **Novembre 2019 :** Election d'Ursula von der Leyen
  - 100 jours pour définir une approche européenne des implications humaines et éthiques de l'IA
- **Février 2020 :** Livre blanc de la Commission sur l'IA
  - ~1200 contributions de sociétés, associations civiles et professionnelles, instituts de recherche, autorités publiques, individus, etc.)
- **Avril 2021 :** Publication par la Commission d'un plan coordonné sur l'IA de la Commission **incluant un projet de régulation**
  - Axée sur les IA à haut-risque et avec une logique produit (marquage CE, etc.)

→ **Enjeu de l'articulation avec le RGPD**

Projet de régulation de l'IA (2)

- **18 Juin 2021 :** adoption de l'avis conjoint EDPB/EDPS

- **4 points principaux**
  - Une approche par les risques saluée
    - **Systèmes :** interdits / à haut risque / à risque limité / à risque minime
  - Des lignes rouges à renforcer
    - En particulier biométrie dans l'espace public et « social scoring »
  - Une gouvernance à préciser
    - Les CNIL comme autorités nationales compétentes
  - Des mesures pour l'innovation
    - Des mesures à préciser mais dont certaines sont déjà mises en œuvre par les CNIL (« bacs à sable réglementaires »)

« Bac à sable » 2021 – données de santé

- Appel lancé en février 2021
- Accompagnement des lauréats par la CNIL
- Critères de sélection :
  - bénéfice pour le public
  - intérêt pour la protection des données
  - engagement fort dans une approche de la conformité RGPD
- 4 lauréats accompagnés et 8 projets bénéficiant de conseils personnalisés

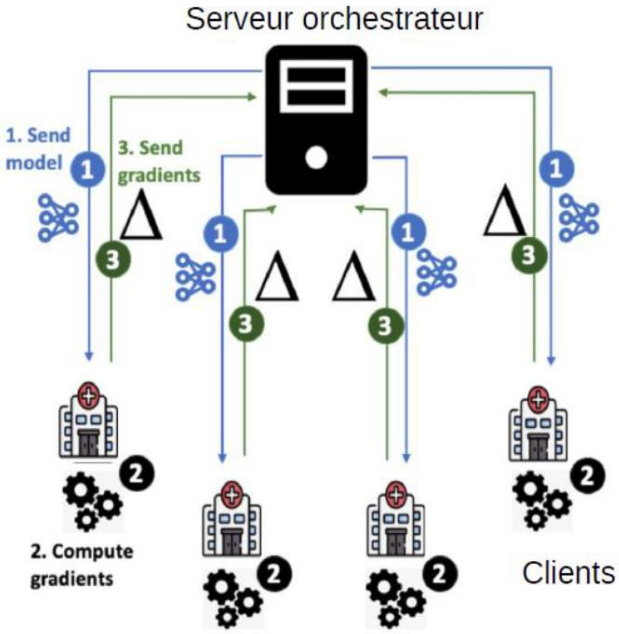
→ Permet également à la CNIL d'affiner sa doctrine sur de nouveaux objets techniques et juridiques

« Bac à sable » 2021 – données de santé

Exemple du projet CHU Lille / Inria Magnet (Federated ML)

- **Fonctionnement en 3 étapes :**
  - Succession de phases d'entraînement local suivies d'agrégations
  - Fin dès qu'un critère d'arrêt est atteint (convergence)

→ Existe toujours un risque d'attaque d'inférence d'appartenance sur les modèles et agrégats (transmis ou calculés)



- **Questions :**
  - Qui est responsable de traitement ?
  - Quel statuts pour les agrégats partagés ?
  - Quelles mesures pratiques déployer ?

- **Evolutions possibles :**
  - Ajouter du bruit entre les échanges clients/serveur (*differential privacy*)
  - Supprimer le serveur orchestrateur (pair à pair)
  - Mettre en œuvre des protocoles cryptographiques pour l'intégrité des calculs d'agrégats locaux

Et d'autres travaux en cours et à venir

- Le potentiel discriminatoire de l'IA et la question des biais
  - Séminaire DDD-CNIL en juin 2020
  - Combinaison de deux droits fondamentaux (vie privée et discriminations)
- La constitution de bases de données d'apprentissage pour l'IA en conformité avec le RGPD
  - Sujet principal pour la CNIL et les RTs
  - Principes de minimisation des données, de finalité et de proportionnalité
  - Dissocier phases d'entraînement et d'exploitation
- L'anonymisation, la génération de données synthétiques et les techniques *privacy preserving pour* l'IA
  - Données synthétiques = données non personnelles ?
  - Simplifie les obligations (information, droits, durée de conservation)
- La présence de données personnelles dans les modèles d'IA
  - Attaques sur les modèles pour inférer/attribuer des données personnelles
  - Critères permettant de déterminer si un modèle contient des données personnelles
- La construction d'un cadre d'audit de solutions d'IA (ex-ante/ex-post)
  - Des obligations dans le projet de règlement IA de la Commission (ex-ante)
  - Des travaux en cours (LNE, IEEE, ISO, etc.)
  - De premiers travaux exploratoire par des régulateurs (ex-post)

CNIL.

MERCI DE VOTRE ATTENTION