CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

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

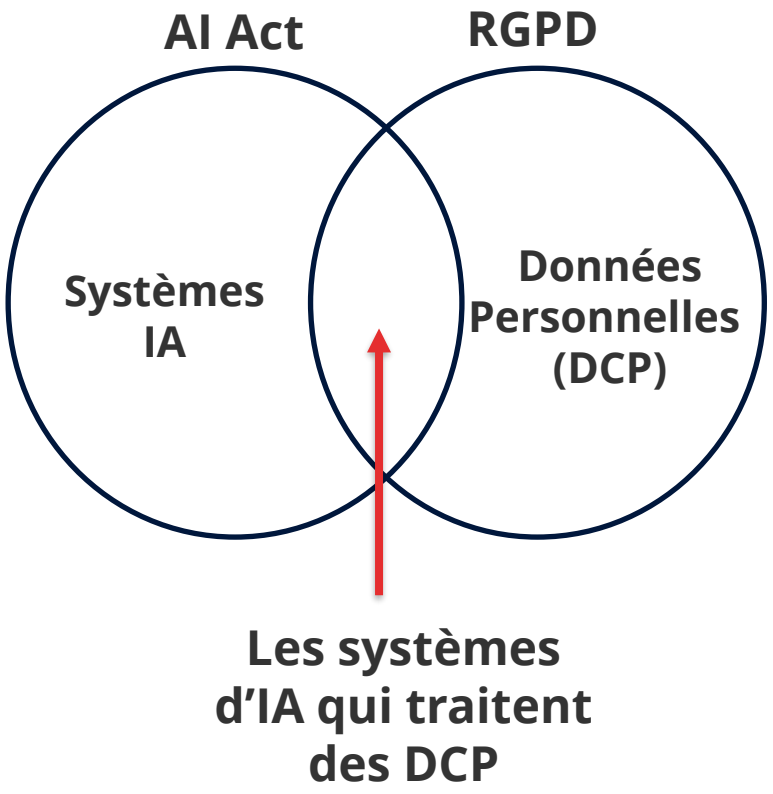
Intelligence artificielle et Protection de Données à Caractère Personnel

Seminaire AEFR
05 Juin 2024

Claude Castelluccia, commissaire à la CNIL

Introduction (1)
AI Act et RGPD

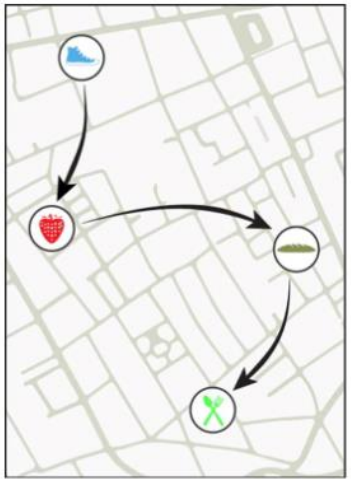
- La CNIL participe activement aux **travaux du CEPD sur l'articulation entre le RGPD et le futur règlement européen sur l'IA**.



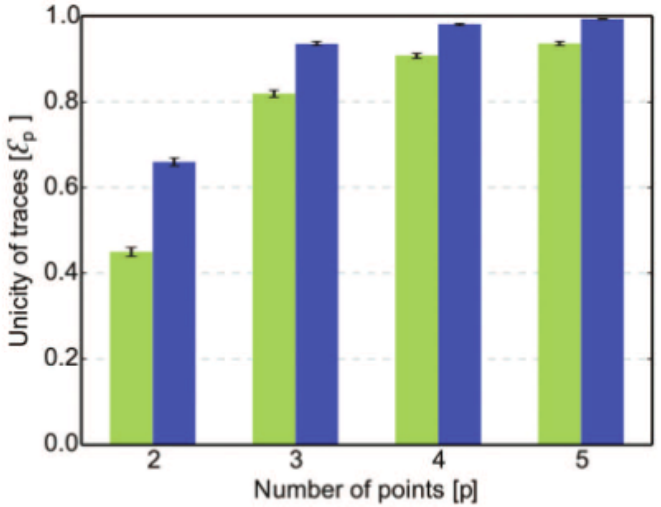
Introduction (2)
Rappel RGPD

- GDPR s'applique en cas de traitement de données à caractère personnel.
- GDPR ne s'applique pas si les données sont anonymisées, mais:
  - La pseudonymisation n'est pas de l'anonymisation
  - L'anonymisation des données (notamment financières) est très complexe
    - Compromis protection/utilité des données
    - Voir études de Y.A. De MontJoye…

Re-Identification des Données de Paiement



shop	user_id	time	price	price_bin
	7abc1a23	09/23	$97.30	$49 – $146
	7abc1a23	09/23	$15.13	$5 – $16
	3092fc10	09/23	$43.78	$16 – $49
	7abc1a23	09/23	$4.33	$2 – $5
	4c7af72a	09/23	$12.29	$5 – $16
	89c0829c	09/24	$3.66	$2 – $5
	7abc1a23	09/24	$35.81	$16 – $49



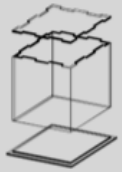
3 mois de relevés de cartes de crédit pour 1,1 million de personnes ont montré que 4 points spatio-temporels suffisent à réidentifier de manière unique ***90% des individus***

Reference: Unique in the Shopping Mall: On the Re-identifiability of Credit Card MetadataYA de Montjoye, L Radaelli, VK Singh, AS Pentland, Science 347

IA et RGPD

Limitation des finalités

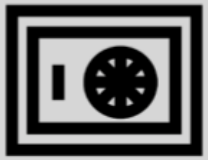
Minimisation des données



Licéité, loyauté, transparence

Exactitude

Limitation de la conservation



Sécurité

+

Respect des droits des personnes:

- Information
- Consentement
- Opposition
- Accès, rectification

Les fiches IA de la CNIL
Concilier intelligence artificielle et RGPD

- De nombreux acteurs ont fait part à la CNIL de **questionnements concernant l'application du RGPD à l'IA**, en particulier depuis l'IA génératives.
- En mai 2023, la CNIL a publié son « plan IA » et a lancé un **travail de clarification du cadre juridique afin de sécuriser les acteurs**.
- Les fiches pratiques ont vocation à répondre aux principales interrogations :
  - Comment entraîner un modèle d'IA sur **de grands volumes de données en respectant le principe de minimisation** ?
  - Comment définir **la finalité d'un système d'IA à usage général ou d'un modèle de fondation** ?
  - A quelles conditions **la réutilisation des données est-elle possible ?**
  - Combien de temps est-il possible de **conserver une base de données d'apprentissage** ?
  - Comment répondre aux **demandes de rectification** sur un modèle?

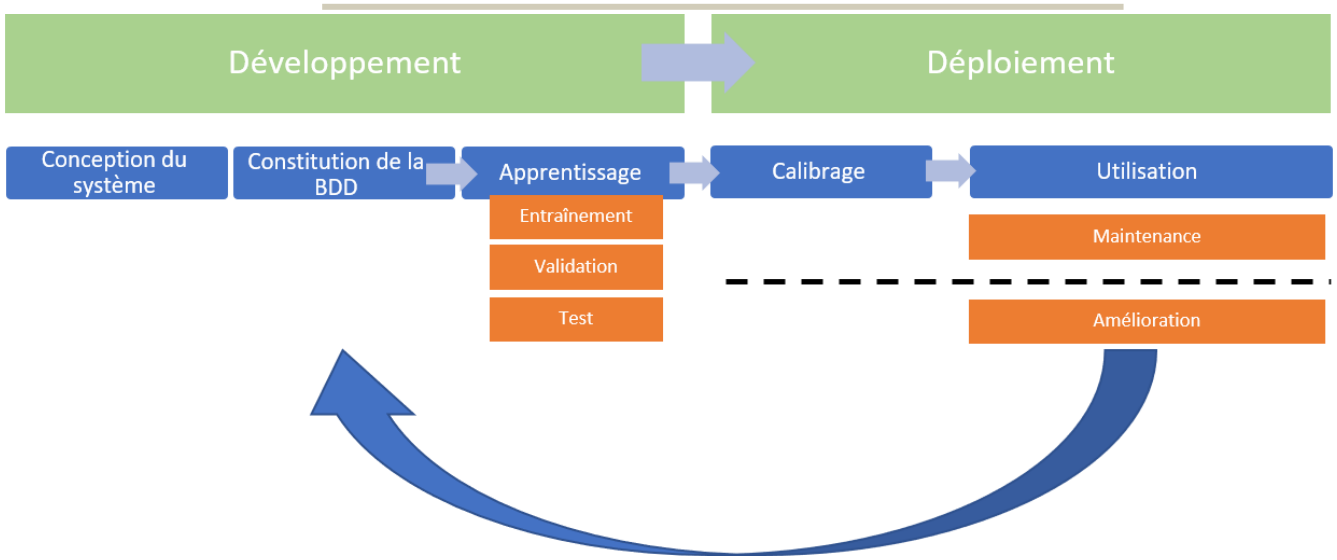
Périmètre des Fiches
Les systèmes d'IA concernés

- Ces recommandations concernent le développement de systèmes reposant sur des techniques d'IA et impliquant un **traitement de données personnelles**.

- En pratique, les systèmes d'IA concernés incluent les **systèmes fondés sur l'apprentissage automatique** (supervisé, non supervisé, par renforcement) et ceux fondés sur la **logique et les connaissances** (bases de connaissance, moteurs d'inférence et de déduction, raisonnement symbolique, systèmes experts, etc.), ainsi que les approches hybrides.

- Elles concernent les phases de développement et de déploiement
  - Souvent différents traitements et Responsable de Traitement (RT)

Périmètre des Fiches (2)



- Ces premières fiches concernent exclusivement les **traitements de données en phase de développement**. Cela inclut :
  - Les cas où l'usage opérationnel est défini dès la phase de développement et **les systèmes d'IA à usage général** (*general purpose AI)*
  - Les systèmes qui impliquent un **apprentissage continu** (où les données collectées lorsque le système est déployé sont réutilisées pour l'amélioration itérative du système)
  - Les traitements consistant à **entraîner ou à ajuster (*fine tuning/transfer learning*) des modèles d'IA existants**, dès lors qu'ils impliquent des données personnelles.

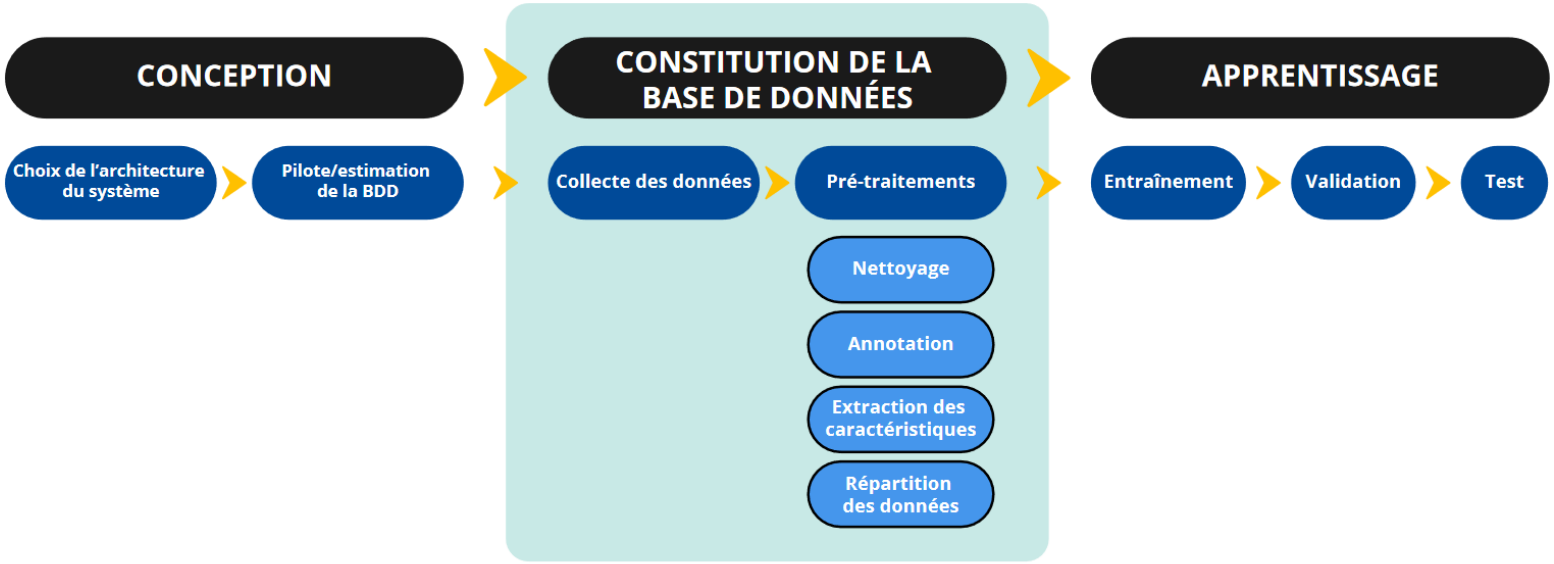
8 Fiches Publiés

- 8 fiches ont été élaborées après une série de rencontres avec les différents acteurs de l'écosystème ainsi qu'une **consultation publique de deux mois**.

- Ces 8 fiches permettent de:
  - déterminer le **régime juridique** applicable ;
  - définir une **finalité** ;
  - déterminer la **qualification juridique** des acteurs ;
  - définir une **base légale** ;
  - effectuer des tests et vérifications en cas de **réutilisation des données** ;
  - réaliser une **analyse d'impact** si nécessaire ;
  - tenir compte de la **protection des données dès la conception du système** ;
  - tenir compte de la **protection des données dans la collecte et la gestion des données**.

- Une synthèse des contribution est disponible sur le site de la CNIL.

Exemple : Fiche 7 – Tenir compte de la protection des données dans la collecte et la gestion des données (0/2)



Exemple : Fiche 7 – Tenir compte de la protection des données dans la collecte et la gestion des données (1/2)

Lors du prétraitement

Nettoyer les données,

Identifier les caractéristiques pertinentes, par des techniques comme l'analyse en composantes principales (PCA) ;

Sélectionner les données pendant l'apprentissage, par des techniques comme l'*active learning.*
Réduire le volume de données sans impact sur les performances.

Suivre les données au cours du temps

Identifier une dérive de données : changements de processus (remplacement d'un capteur, changement par rapport à la configuration d'étalonnage), **perte de qualité des données** (capteur détérioré), **dérive naturelle** (variations saisonnières), **changements soudains** (apparition des masques lors du COVID-19), **évolution des corrélations entre les caractéristiques, empoisonnement des données**.

Identifier les évolutions des données : mise à jour dans un profil de réseau social.
Nouvelles méthodes nécessitant moins de données.

Exemple : Fiche 7 – Tenir compte de la protection des données dans la collecte et la gestion des données (2/2)

Documenter les données

A destination des **équipes techniques et des utilisateurs,**
Pour **faciliter l'utilisation, démontrer que la collecte est légale,** faciliter **le suivi** des données au fil du temps**,** réduire le **risque d'utilisation imprévue, permettre l'exercice des droits,** identifier **les améliorations prévues ou possibles.**

Gebru et al., 2021 («Datasheets for datasets»), Arnold et al., 2019, Bender et al., 2018, Dataset Nutrition Label, CrowdWorkSheets.

Limiter la conservation dans le temps

Définir une durée **pour la conception,**
et **une durée pour la maintenance** (comme pour la surveillance des biais)**.**

Adapter **les conditions de conservation et de sécurité à chaque phase,**
Effectuer **une nouvelle sélection** des données **entre les deux phases.**

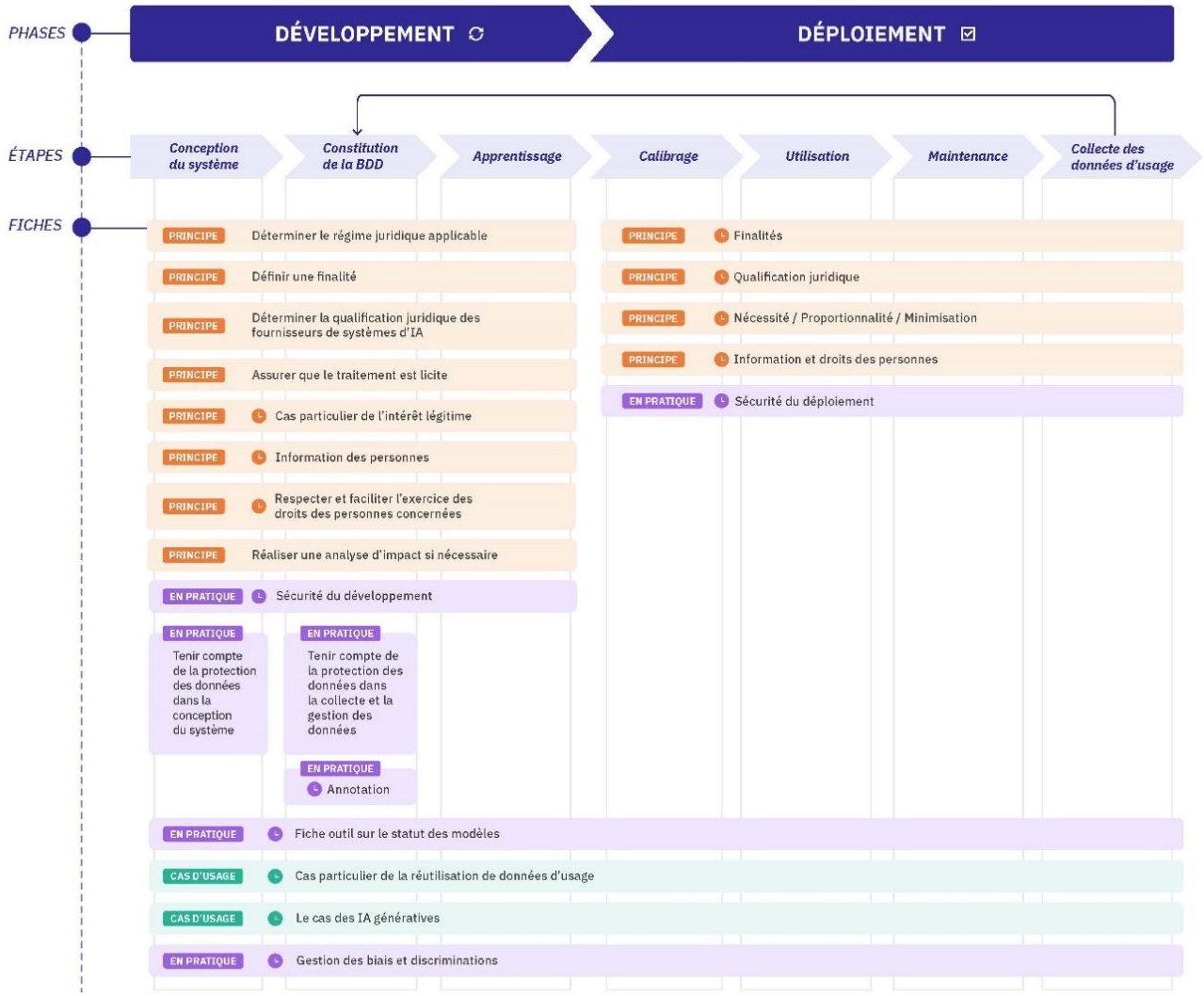
Supprimer ou anonymiser les données après cela.

Travaux en cours:
Deuxième série de fiches pratiques IA

- Ces premières recommandations seront complétées par **une deuxième série de fiches pratiques** :
  - Mobiliser la base légale de l'intérêt légitime pour le développement des systèmes d'IA, avec un focus sur l'*open source* et le moissonnage des données (*web scraping*) ;
  - Informer les personnes ;
  - Garantir et faciliter l'exercice des droits des personnes ;
  - L'annotation des données ;
  - La sécurité des traitements en phase de développement
  - Le statut des modèles
  - …

- **Ces fiches seront publiées prochainement pour consultation publique.**

- La CNIL **poursuit également ses travaux doctrinaux** pour les traitements en **phase de déploiement**, pour certains cas d'usage plus précis (réutilisation des données, l'IA générative, etc.) et l'articulation entre les exigences du RGPD et du futur règlement européen sur l'IA.


PHASES
DÉVELOPPEMENT
DÉPLOIEMENT
ÉTAPES
Conception du système
Constitution de la BDD
Apprentissage
Calibrage
Utilisation
Maintenance
Collecte des données d'usage
FICHES
PRINCIPE Déterminer le régime juridique applicable
PRINCIPE Définir une finalité
PRINCIPE Déterminer la qualification juridique des fournisseurs de systèmes d'IA
PRINCIPE Assurer que le traitement est licite
PRINCIPE Cas particulier de l'intérêt légitime
PRINCIPE Information des personnes
PRINCIPE Respecter et faciliter l'exercice des droits des personnes concernées
PRINCIPE Réaliser une analyse d'impact si nécessaire
EN PRATIQUE Sécurité du développement
EN PRATIQUE Tenir compte de la protection des données dans la conception du système
EN PRATIQUE Tenir compte de la protection des données dans la collecte et la gestion des données
EN PRATIQUE Annotation
EN PRATIQUE Fiche outil sur le statut des modèles
CAS D'USAGE Cas particulier de la réutilisation de données d'usage
CAS D'USAGE Le cas des IA génératives
EN PRATIQUE Gestion des biais et discriminations
PRINCIPE Finalités
PRINCIPE Qualification juridique
PRINCIPE Nécessité / Proportionnalité / Minimisation
PRINCIPE Information et droits des personnes
EN PRATIQUE Sécurité du déploiement
LÉGENDE
Étape
CLASSIFICATION DES FICHES
PRINCIPE Respect des principes
EN PRATIQUE Mise en oeuvre pratique
CAS D'USAGE Cas d'usage
STATUT DES FICHES
À venir

Accompagnement renforcé
la CNIL lance un nouvel appel à projets

- **Accompagnement** des lauréats sur 6 mois sur les conditions de mise en œuvre de leurs traitements ou de leurs projets au regard du RGPD
- **3 principales modalités** :
  - un appui juridique et technique dans des délais rapides
  - une revue de conformité des traitements mis en œuvre
  - des actions de sensibilisation
- L'accompagnement renforcé vise à apporter aux entreprises sélectionnées des réponses concrètes, adaptées à leurs enjeux, et de la sécurité juridique sur leurs activités impliquant des données personnelles.

- *La session de candidatures est ouverte **jusqu'au 23 juin 2024**.*

Conclusion

- L'IA est **source de progrès**
- … mais génère de **nouveaux risques**
  - Vie privée, mais aussi en Sécurité, sureté, sociétaux, etc.

- Il est important de **contrôler et accompagner** le développement de l'IA
  - Pour des raisons démocratiques
  - Mais aussi pour instaurer la confiance des utilisateurs

- **La CNIL accompagne** les acteurs du domaine
  - Création d'un service IA (le SIA) (en 2023)
  - Commissaire spécifiquement en charge de l'IA (depuis Fév. 2024)
  - Plusieurs programmes d'accompagnement
  - Mise en place de bacs à sable…
  - …

CNIL.

Contact : ia@cnil.fr

CNIL.

MERCI DE VOTRE ATTENTION !

https://www.cnil.fr/fr/technologies/intelligence-artificielle-ia

III. LES RECOMMANDATIONS DE LA CNIL