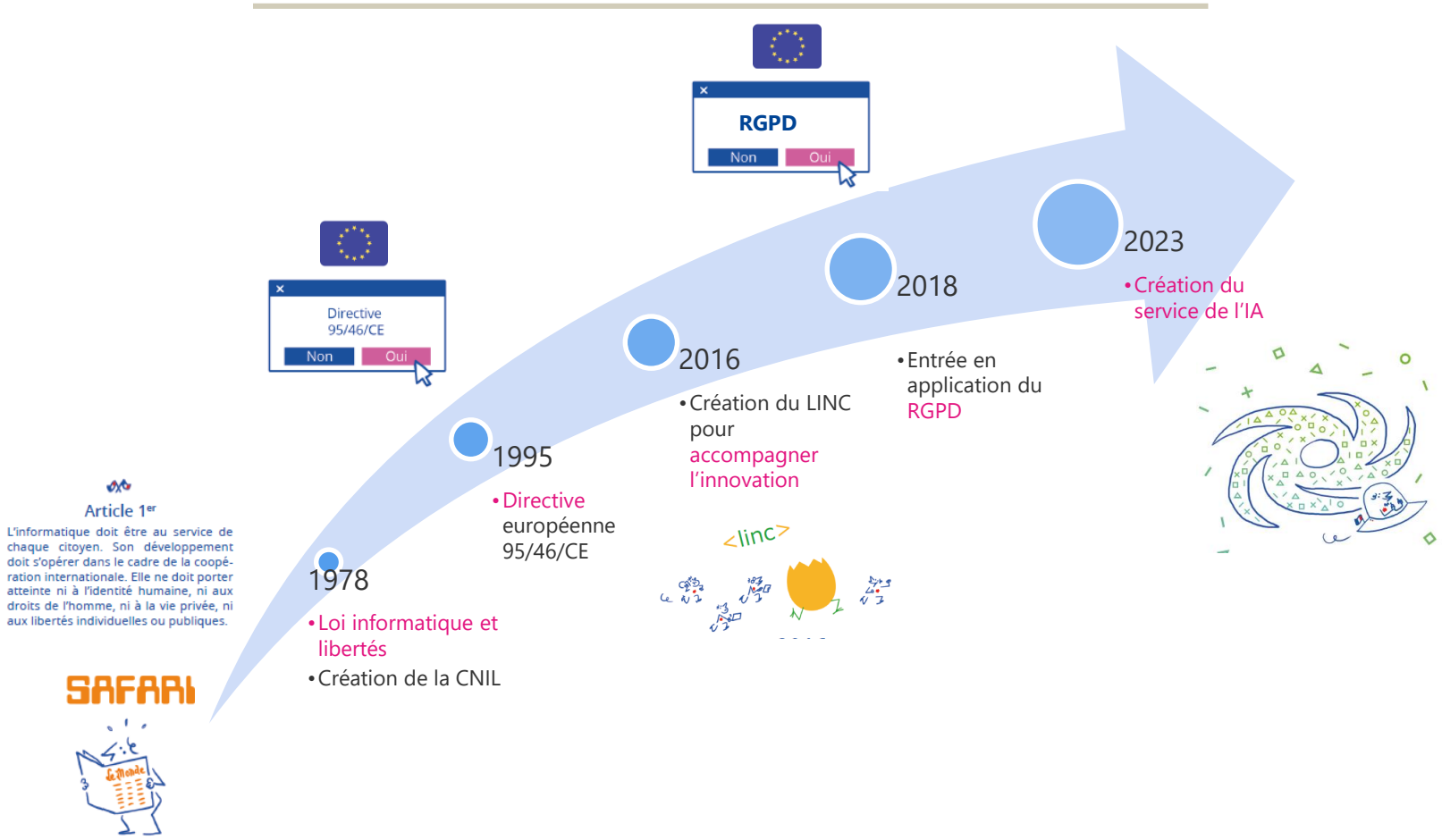
CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

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

Intelligence artificielle et protection des données
Anticiper et répondre aux enjeux

Félicien Vallet
Service de l'Intelligence Artificielle

Une brève histoire de la protection des données



MISSIONS DE LA CNIL

Informer les personnes et protéger leurs droits

Accompagner la conformité et conseiller

Contrôler et sanctionner

Anticiper et innover

MISSIONS DE LA CNIL

Informer les personnes et protéger leurs droits

Accompagner la conformité et conseiller

Contrôler et sanctionner

Anticiper et innover

Service de l'intelligence artificielle

La CNIL en 2023

Accompagner et conseiller

- 151 délibérations (dont 102 avis sur des projets de texte)
- 520 dossiers traités en santé et recherche
- 4 668 notifications de violations de données +14%

Contrôler et sanctionner

- 340 contrôles ont été effectués
- 168 mises en demeure
- 33 rappels aux obligations légales
- 42 sanctions (36 amendes)

Informer et protéger

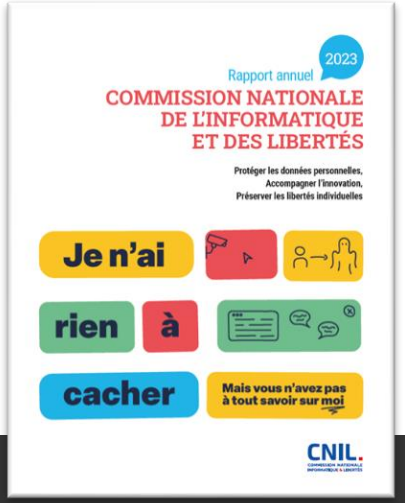
- 47 111 appels traités
- 15 388 demandes écrites traitées
- 16 433 plaintes reçues +35%

Anticiper et innover

- Conférence internationale **Privacy Research Day**
  - 76 contributions reçues (articles, projets de recherche, démonstrations de technologies)
  - 4439 participants sur place et à distance
- Évènement air2023
  - + de 1700 participants (présentiel et distanciel)
- Site linc.cnil.fr
  - 32 dossier et articles

Ressources humaines et financières

- Budget : 26,3 millions €
- 288 emplois



L'IA et la CNIL

Retour sur une histoire (déjà) riche

L'IA et la CNIL
Au commencement…

Article 1 de la Loi Informatique et Libertés :

L'informatique doit être au service de chaque citoyen.
Son développement doit s'opérer
dans le cadre de la coopération internationale.
Elle ne doit porter atteinte ni à l'identité humaine,
ni aux droits de l'homme, ni à la vie privée,
ni aux libertés individuelles ou publiques.

Depuis sa création en **1978**, l'idée pour la CNIL d'un rôle de régulateur des systèmes algorithmiques

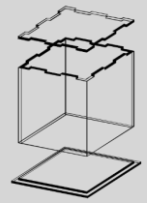
L'IA et la CNIL
Un poste d'observation privilégié

* Au fil des ans, l'opportunité d'observer le recours à l'IA dans de multiples secteurs, par exemple :
  * **Santé :** aide au diagnostic (cancer de la prostate), assistance en imagerie médicale, codage d'actes médicaux (PMSI)
  * **Justice :** projet DataJust (création d'un référentiel pour l'indemnisation de victimes de préjudice corporels)
  * **Administration fiscale :** projet CFVR (ciblage de la fraude et valorisation des requêtes pour l'amélioration de l'efficacité des opérations de contrôle fiscal)
  * **Smart city :** détection de comportements (circulation en sens inverse, attroupements, dépôts d'ordure sauvage, etc.
  * **Transports :** usage de la reconnaissance faciale dans les aéroports, aide au suivi de personnes en gare, détection du port du masque, etc.
  * **RH et recrutement :** évaluation automatique d'entretiens vidéo, anticipation du départ de collaborateurs
  * **Education :** développement d'outils pédagogiques adaptés aux rythme d'apprentissage de l'élève
  * **Retail :** comptage et segmentation du public dans les centre commerciaux

L'IA et la CNIL
Des questions inédites…

Limitation des finalités

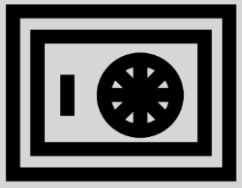
Minimisation des données



Licéité, loyauté, transparence

Exactitude

Limitation de la conservation



Sécurité

+

Respect des droits des personnes:
- Information
- Consentement
- Opposition
- Accès, rectification

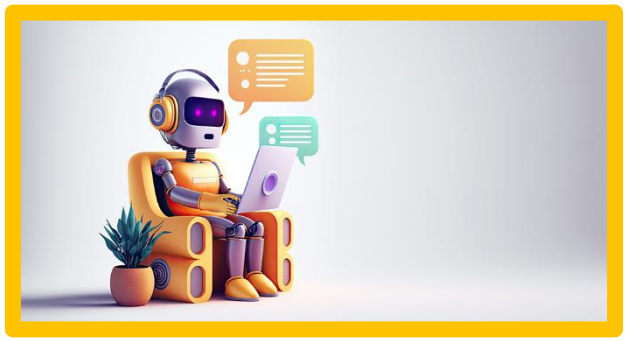
L'IA et la CNIL
Des questions inédites…

* Quel application concrète du principe de **minimisation** des données ?
* Quelle **transparence** pour les systèmes d'IA ?
* Comment prendre en compte les questions de **discrimination** et de gestion des **biais** ?
* Quelles **mesures de sécurité** mettre en œuvre pour se prémunir des risques spécifiques à l'IA ?
* Comment permettre aux individus d'exercer efficacement leurs **droits** (consentement, opposition, accès, etc.) ? De ne pas faire l'objet d'une **décision automatisée** ?
* Comment constituer une **base de données** pour le développement et l'entrainement d'un système ?
* Quel est le **statut des modèles** appris a partir de données personnelles ? Des contraintes pèsent-elle sur leur diffusion ?
* Comment **contrôler/auditer** des systèmes d'IA ?

L'IA à la CNIL

LE SERVICE IA

SERVICE DE L'IA

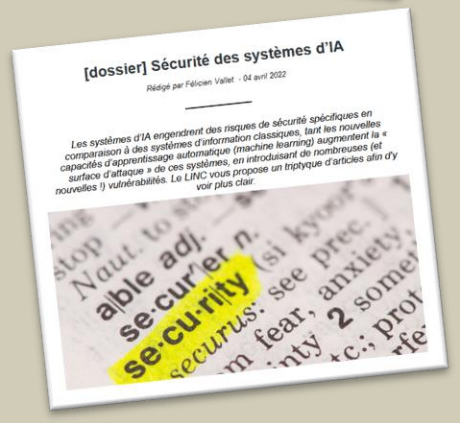


* Le point de départ :
  * Mission d'accompagnement de la CNIL
* Notre objectif ?
  * Anticiper et répondre aux enjeux soulevés par l'IA
* Création d'un SIA en 2023
  * 5 personnes avec des compétences complémentaires (juridique, IA/ML, sciences cognitives, etc.)
* Plan d'action en 4 volets :
  * appréhender, guider, fédérer, auditer

PLAN D'ACTION IA DE LA CNIL

1) APPRÉHENDER

- **Assurer une veille technologique**
- **Acculturer l'institution sur les sujets IA**
- **Produire des contenus pédagogiques**
  - Sensibiliser le grand public
  - Echanger avec les spécialistes (articles LINC)



PLAN D'ACTION IA DE LA CNIL

2) GUIDER

- **Publier des contenus pratiques (guides, lignes directrices, etc.)**
- **Former les professionnels (webinaires, journées de sensibilisation)**
- **Travaux sur le développement de système d'IA (consultation publique)**

PLAN D'ACTION IA DE LA CNIL

3) FÉDÉRER ET ACCOMPAGNER

- Instaurer un dialogue de confiance avec les acteurs
- Animer des communautés à différents niveaux (institutions partenaires, au sein de l'écosystème IA, etc.)
- Proposer des dispositifs pour soutenir les acteurs

PLAN D'ACTION IA DE LA CNIL

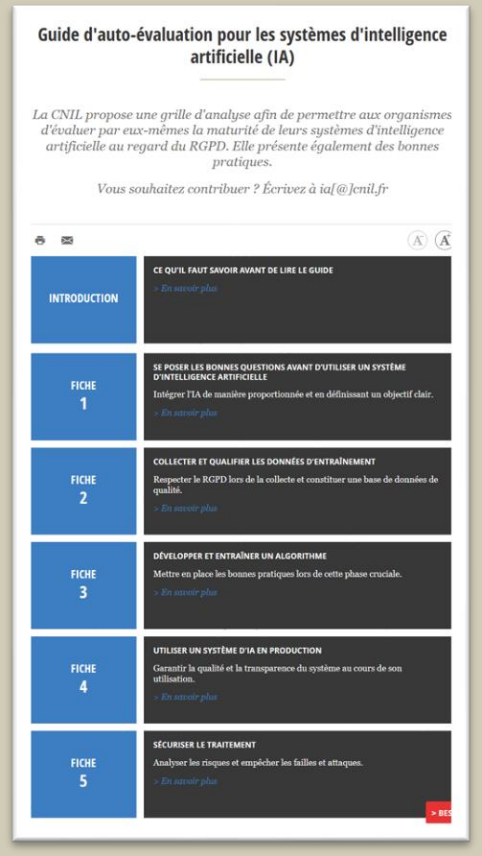
4) AUDITER

- **Développer des méthodologies d'audit et d'enquête**
- **Outiller les contrôleurs en interne**
- **Anticiper les exigences du règlement IA et les systèmes de certification à venir**


[Algaudit] 2 - Expérimenter une solution d'audit algorithmique

Rédigé par Félicien Vallet & Clément Henin - 10 août 2022

Comment pourrait se dérouler un audit de système d'IA ? Après une présentation du contexte et des outils IBEX et Algocate développés par Clément Hénin* dans l'article précédent, passons à l'expérimentation « grandeur nature » qu'ont décidé de lancer la CNIL et Inria. Ce test a mis à contribution des agents de la CNIL : en voici les « règles du jeu ».


Guide d'auto-évaluation pour les systèmes d'intelligence artificielle (IA)

La CNIL propose une grille d'analyse afin de permettre aux organismes d'évaluer par eux-mêmes la maturité de leurs systèmes d'intelligence artificielle au regard du RGPD. Elle présente également des bonnes pratiques.

Vous souhaitez contribuer ? Écrivez à ia[@]cnil.fr

INTRODUCTION	CE QU'IL FAUT SAVOIR AVANT DE LIRE LE GUIDE
FICHE 1	SE POSER LES BONNES QUESTIONS AVANT D'UTILISER UN SYSTÈME D'INTELLIGENCE ARTIFICIELLE Intégrer l'IA de manière proportionnée et en définissant un objectif clair.
FICHE 2	COLLECTER ET QUALIFIER LES DONNÉES D'ENTRAÎNEMENT Respecter le RGPD lors de la collecte et constituer une base de données de qualité.
FICHE 3	DÉVELOPPER ET ENTRAÎNER UN ALGORITHME Mettre en place les bonnes pratiques lors de cette phase cruciale.
FICHE 4	UTILISER UN SYSTÈME D'IA EN PRODUCTION Garantir la qualité et la transparence du système au cours de son utilisation.
FICHE 5	SÉCURISER LE TRAITEMENT Analyser les risques et empêcher les failles et attaques.

Focus sur les recommandations

Comment déployer un système d'IA générative

FAQ sur l'IA générative ?

* Qu'est-ce que l'IA générative ?
  * Ex. Grands modèles de langage, génération d'image, de son, de vidéo, etc.

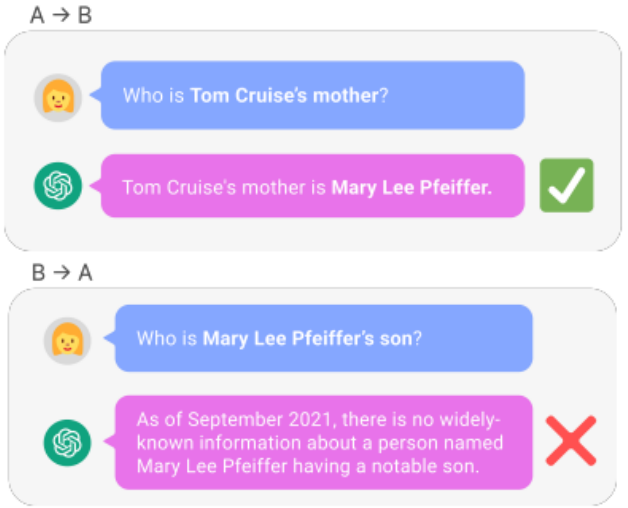
Midjourney Jason Alley

FAQ sur l'IA générative ?

* Qu'est-ce que l'IA générative ?
  * Ex. Grands modèles de langage, génération d'image, de son, de vidéo, etc.

Midjourney Jason Alley

* Quelles sont ses limites ?
  * Logique probabiliste
  * Pas de neutralité technique : ex. potentiels biais discriminatoires
  * Confiance excessive sans vérification



The Reversal Curse: LLMs trained on "A is B" fail to learn "B is A"
Lukas Berglund et al.

FAQ sur l'IA générative ?

Les questions réponses de la CNIL, en synthèse :

* **Partir d'un besoin concret**

FAQ sur l'IA générative ?

Les questions réponses de la CNIL, en synthèse :

* **Partir d'un besoin concret**

* **Choisir un système robuste et un mode de déploiement sécurisé** en fonction des limitations

  Ex: système local > sur serveur dédié > API ou service grand public; modèle de base, ajusté, RAG, etc.

FAQ sur l'IA générative ?

Les questions réponses de la CNIL, en synthèse :

* **Partir d'un besoin concret**

* **Choisir un système robuste et un mode de déploiement sécurisé** en fonction des limitations

  Ex: système local > sur serveur dédié > API ou service grand public; modèle de base, ajusté, RAG,

* **Encadrer les usages**

  Ex: ne pas fournir de données personnelles, ou ne pas confier de prise de décision.

FAQ sur l'IA générative ?

Les questions réponses de la CNIL, en synthèse :

* **Partir d'un besoin concret**

* **Choisir un système robuste et un mode de déploiement sécurisé** en fonction des limitations

  Ex: système local > sur serveur cloud dédié > API ou service grand public / modèle de base, ajusté, RAG,

* **Encadrer les usages**

  Ex: ne pas fournir de données personnelles, ou ne pas confier de prise de décision.

* **Mettre en œuvre une gouvernance adaptée**
  (ex. impliquer dès le début le DPO, le RSSI, les responsables métiers, etc.)
  * **Former et sensibiliser les utilisateurs finaux**
  * **Vérifier le bon respect de ces préconisations**

L’essor de l’IA générative – enjeux de protection des données

Réutilisation des données utilisateurs

« à des fins d’amélioration et de développement de services »

« Please don’t provide sensitive information »

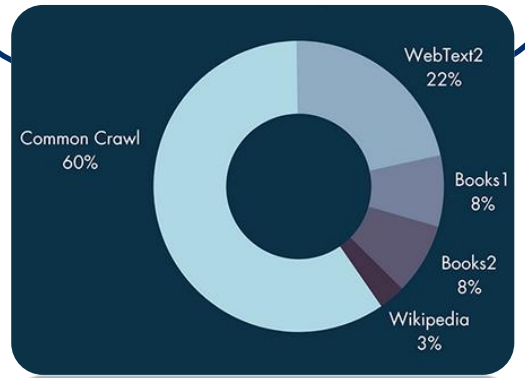
Enjeux RGPD : confidentialité et sécurité

L’essor de l’IA générative – enjeux de protection des données

Collecte de données en sources ouvertes

Collectées par API ou *scraping*.

Enjeux RGPD : licéité de la collecte, base légale, transparence, exercice des droits.

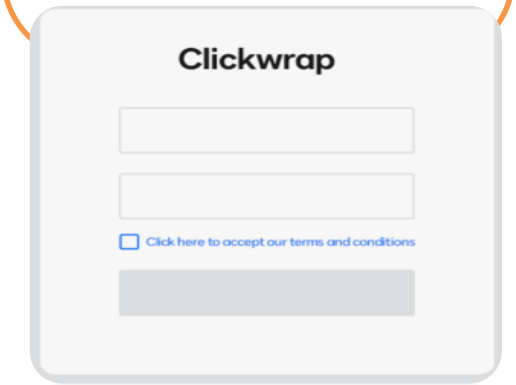


Réutilisation des données utilisateurs

« à des fins d’amélioration et de développement de services »

« Please don’t provide sensitive information »

Enjeux RGPD : confidentialité et sécurité

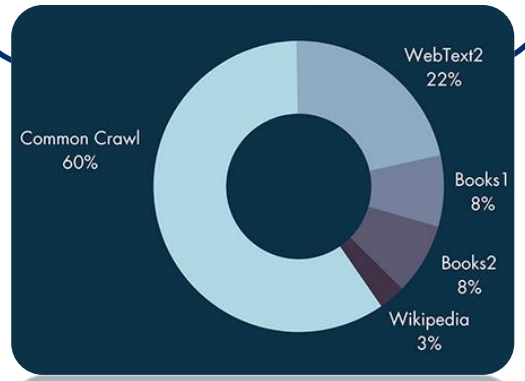


L'essor de l'IA générative – enjeux de protection des données

Collecte de données en sources ouvertes

Collectées par API ou *scraping*.

Enjeux RGPD : licéité de la collecte, base légale, transparence, exercice des droits.



Enrichissement et synthèse

Ex. : annotation de données d'entrée ou de sorties

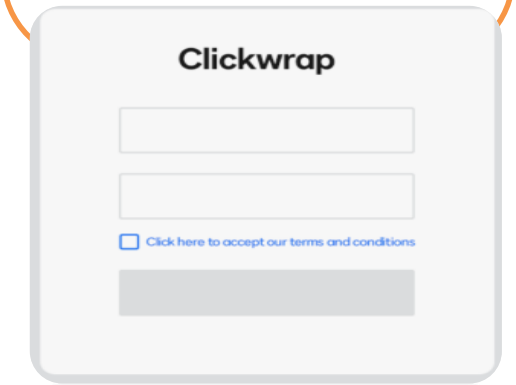
Enjeux RGPD : pertinence des données, risques de biais, conservation

Réutilisation des données utilisateurs

« à des fins d'amélioration et de développement de services »

« Please don't provide sensitive information »

Enjeux RGPD : confidentialité et sécurité



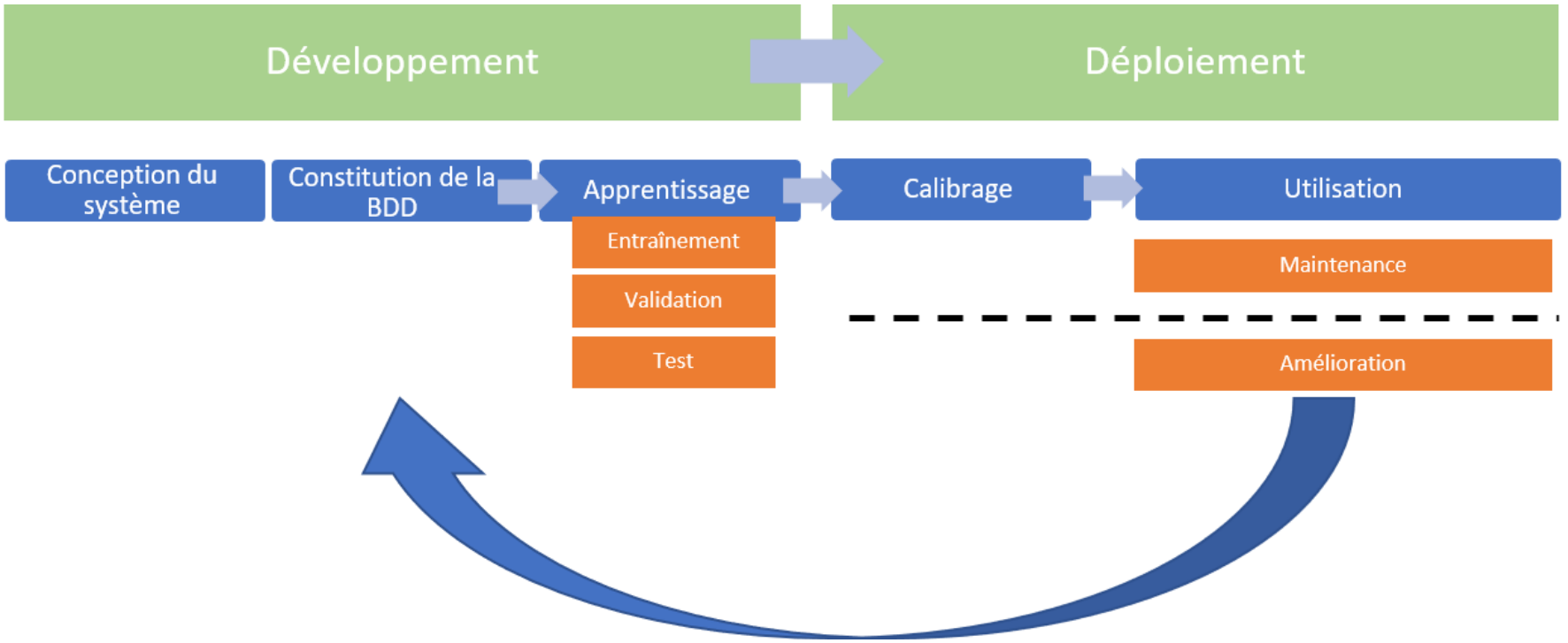
CNIL.

Bref aperçu du travail de fond de la CNIL

RECOMMANDATIONS POUR LE DÉVELOPPEMENT D'UN SYSTÈME D'IA

FOCUS SUR LES FICHES IA DE LA CNIL

* Découpage du cycle de vie des systèmes d'IA:



FOCUS SUR LES FICHES IA DE LA CNIL

Introduction

QUEL EST LE PÉRIMÈTRE DES FICHES PRATIQUES SUR L'IA ?

La CNIL apporte des réponses concrètes pour la constitution de bases de données utilisées pour l'apprentissage des systèmes d'intelligence artificielle (IA), qui impliquent des données personnelles.

> En savoir plus

Fiche 1

DÉTERMINER LE RÉGIME JURIDIQUE APPLICABLE

La CNIL vous aide à déterminer le régime juridique applicable aux traitements de données personnelles en phase de développement.

> En savoir plus

Fiche 2

DÉFINIR UNE FINALITÉ

La CNIL vous aide à définir la ou les finalités en tenant compte des spécificités du développement de systèmes d'IA.

> En savoir plus

Fiche 3

DÉTERMINER LA QUALIFICATION JURIDIQUE DES FOURNISSEURS DE SYSTÈMES D'IA

Responsable de traitement, responsable conjoint ou sous-traitant : la CNIL aide les fournisseurs de systèmes d'IA à déterminer leur qualification.

> En savoir plus

Fiche 4 (1/2)

ASSURER QUE LE TRAITEMENT EST LICITE - DÉFINIR UNE BASE LÉGALE

La CNIL vous aide à déterminer vos obligations en fonction de votre responsabilité et des modalités de collecte ou de réutilisation des données.

> En savoir plus

Fiche 4 (2/2)

ASSURER QUE LE TRAITEMENT EST LICITE - EN CAS DE RÉUTILISATION DES DONNÉES

La CNIL vous aide à déterminer vos obligations en fonction de votre responsabilité et des modalités de collecte ou de réutilisation des données.

> En savoir plus

Fiche 5

RÉALISER UNE ANALYSE D'IMPACT SI NÉCESSAIRE

La CNIL vous explique comment et dans quels cas réaliser une analyse d'impact sur la protection des données (AIPD) en tenant compte des risques spécifiques au développement de modèles d'IA.

> En savoir plus

Fiche 6

TENIR COMPTE DE LA PROTECTION DES DONNÉES DANS LA CONCEPTION DU SYSTÈME

Pour assurer le développement d'un système d'IA respectueux de la protection des données, il est nécessaire de mener une réflexion préalable lors de la conception du système. La CNIL en détaille les étapes.

> En savoir plus

Fiche 7

TENIR COMPTE DE LA PROTECTION DES DONNÉES DANS LA COLLECTE ET LA GESTION DES DONNÉES

La CNIL donne les bonnes pratiques pour sélectionner les données et limiter leur traitement afin d'entraîner un modèle performant dans le respect des principes de protection des données dès la conception et par défaut.

> En savoir plus

Fiche 8
SOUS CONSULTATION

MOBILISER LA BASE LÉGALE DE L'INTÉRÊT LÉGITIME POUR DÉVELOPPER UN SYSTÈME D'IA

La base légale de l'intérêt légitime sera la plus couramment utilisée pour le développement de systèmes d'IA. Cette base légale ne peut toutefois pas être mobilisée sans en respecter les conditions et mettre en œuvre des garanties suffisantes.

> En savoir plus

Fiche 8 (1/2)
SOUS CONSULTATION

LA BASE LÉGALE DE L'INTÉRÊT LÉGITIME : FICHE FOCUS SUR LA DIFFUSION DES MODÈLES EN SOURCE OUVERTE (OPEN SOURCE)

Compte tenu des bénéfices qu'elles peuvent présenter, les pratiques d'ouverture sont à prendre en compte dans l'évaluation de l'intérêt légitime d'un fournisseur de système d'IA. Il est toutefois nécessaire d'adopter des garanties permettant de limiter les atteintes qu'elles peuvent porter aux personnes.

> En savoir plus

Fiche 8 (2/2)
SOUS CONSULTATION

LA BASE LÉGALE DE L'INTÉRÊT LÉGITIME : FICHE FOCUS SUR LES MESURES À PRENDRE EN CAS DE COLLECTE DES DONNÉES PAR MOISSONNAGE (WEB SCRAPING)

La collecte des données accessibles en ligne par moissonnage (*web scraping*) doit être accompagnée de mesures visant à garantir les droits des personnes concernées.

> En savoir plus

Fiche 9
SOUS CONSULTATION

INFORMER LES PERSONNES CONCERNÉES

Les organismes qui traitent des données personnelles pour développer des modèles ou des systèmes d'IA doivent informer les personnes concernées. La CNIL précise les obligations en la matière.

> En savoir plus

Fiche 10
SOUS CONSULTATION

RESPECTER ET FACILITER L'EXERCICE DES DROITS DES PERSONNES CONCERNÉES

Les personnes dont les données sont collectées, utilisées ou réutilisées pour développer un système d'IA disposent de droits sur leurs données qui leur permettent d'en conserver la maîtrise. Il appartient aux responsables des traitements de les respecter et d'en faciliter l'exercice.

> En savoir plus

Fiche 11
SOUS CONSULTATION

ANNOTER LES DONNÉES

La phase d'annotation des données est cruciale pour garantir la qualité du modèle entraîné. Cet enjeu de performance peut être atteint au moyen d'une méthodologie rigoureuse garantissant le respect de la protection des données personnelles.

> En savoir plus

Fiche 12
SOUS CONSULTATION

GARANTIR LA SÉCURITÉ DU DÉVELOPPEMENT D'UN SYSTÈME D'IA

La sécurité des systèmes d'IA est une obligation afin de garantir la protection des données tant lors du développement du système que par anticipation de son déploiement. Cette fiche détaille les risques et mesures à prendre recommandées par la CNIL.

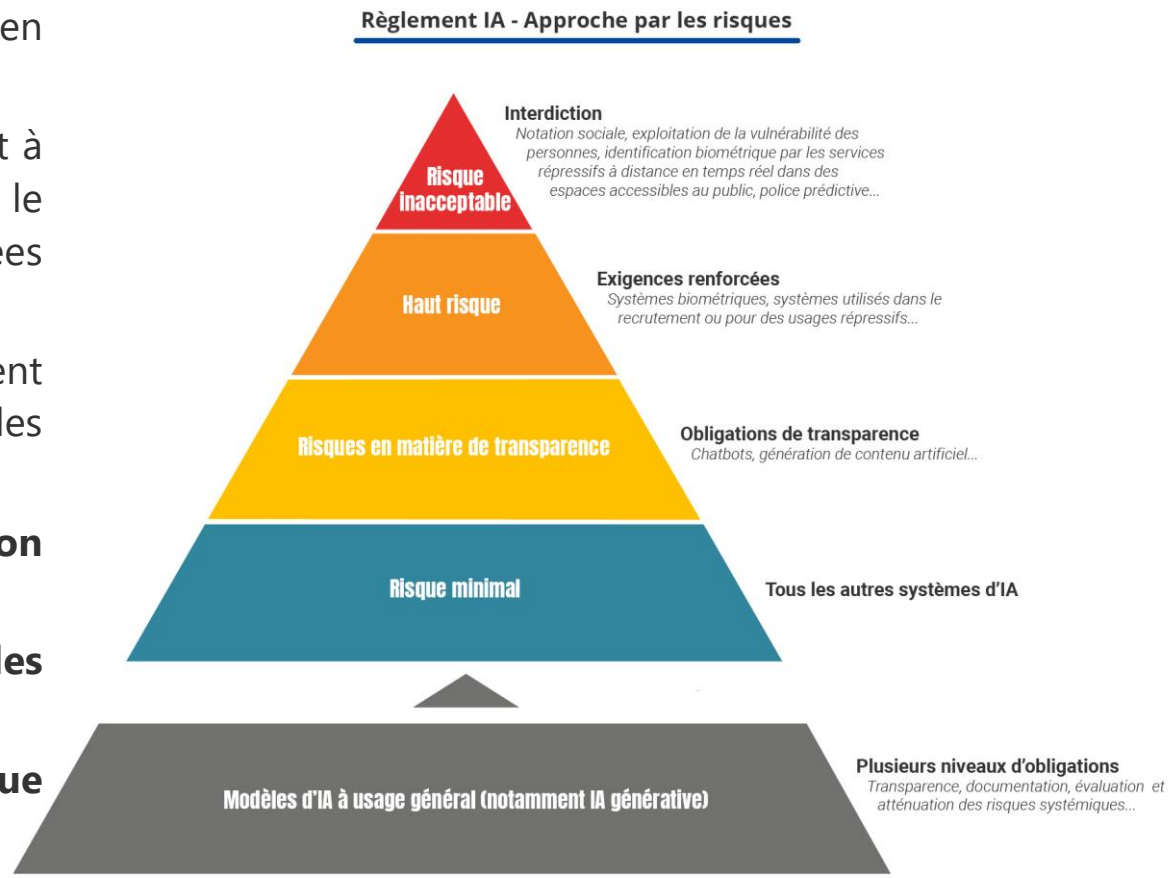
> En savoir plus

Et demain ?

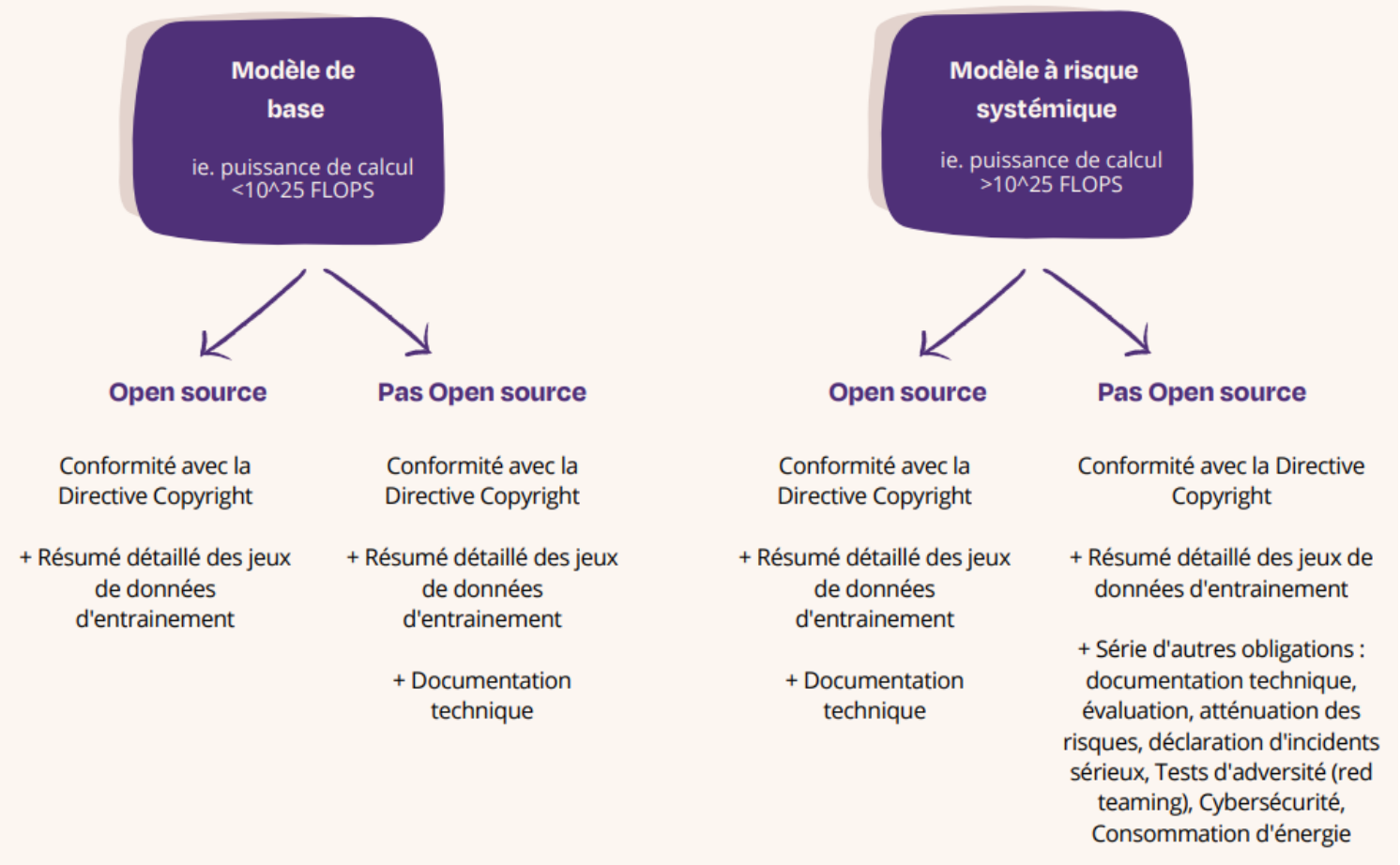
QUEL RÔLE POUR LA CNIL DANS LE RÈGLEMENT IA ?

Règlement sur l'intelligence artificielle - AIA

* **Proposition d'un cadre juridique sur l'IA** visant à proposer des règles harmonisées concernant la mise sur le marché, la mise en service et l'utilisation de systèmes d'IA dans l'UE (21 avril 2021).
* **Une définition de l'IA large** applicable aux acteurs à l'intérieur et à l'extérieur de l'UE, pour autant que le système d'IA soit mis sur le marché de l'UE ou que son utilisation affecte des personnes situées dans l'UE.
* **Des règles relatives à la surveillance du marché** qui s'appliquent aux fournisseurs et aux utilisateurs de systèmes d'IA dans les secteurs public et privé.
* Une approche basée sur la **classification des systèmes en fonction de leur niveau de risque.**
* **Systèmes d'identification biométrique à distance dans les espaces publics interdits** (sauf exceptions)
* Sinon, **systèmes d'identification et de catégorisation biométrique** identifiées comme à **haut risque**



Focus sur les modèles d'IA à usage général



Source : [Guide Conformite AI Act – France Digital – Gide Wavestone Fev 2024]

Règlement sur l'intelligence artificielle - AIA

* **Des obligations strictes pour les systèmes d'IA à haut risque :** systèmes d'évaluation et d'atténuation des risques, qualité élevée des données alimentant le système, traçabilité des résultats, documentation détaillée, informations claires à l'intention de l'utilisateur, contrôle humain, niveau élevé de robustesse et de sécurité et d'exactitude.
* **Des mécanismes de certification** (« marquage CE ») par des organismes notifiés.
* **La création d'un comité européen de l'IA (CEIA)** rassemblant la Commission, l'EDPS et les autorités nationales compétentes.
* **Un « bureau de l'IA » à Bruxelles** responsable de la supervision des modèles de fondation
* **Des sanctions pécuniaires** allant jusqu'à 30M€ / 6% du CA en plus des possibilités offertes par la surveillance du marché : actions correctrices, restriction, retrait, rappel, etc.
* **Des mesures visant à favoriser l'innovation** (bacs à sable réglementaires notamment).

Règlement sur l'intelligence artificielle - AIA

* Entrée en application de façon échelonnée :

* **Février 2025** (6 mois après l'entrée en vigueur) :
  * Interdictions relatives aux systèmes d'IA présentant des risques inacceptables.
* **Août 2025** (12 mois après l'entrée en vigueur) :
  * Application des règles pour les modèles d'IA à usage général.
  * Nomination des autorités compétentes au niveau des États membres.
* **Août 2026** (24 mois après l'entrée en vigueur) :
  * **Toutes les dispositions du règlement sur l'IA deviennent applicables,** en particulier l'application des règles relatives aux systèmes d'IA à haut risque de l'annexe III (systèmes d'IA dans les domaines de la biométrie, des infrastructures critiques, de l'éducation, de l'emploi, de l'accès aux services publics essentiels, de l'application de la loi, de l'immigration et de l'administration de la justice).
  * Mise en œuvre par les autorités des États membres d'au moins un bac à sable réglementaire.
* **Août 2027** (36 mois après l'entrée en vigueur)
  * Application des règles relatives aux systèmes d'IA à haut risque de l'annexe I (jouets, équipements radio, dispositifs médicaux de diagnostic in vitro, sécurité de l'aviation civile, véhicules agricoles, etc.).

* Par ailleurs, l'entrée en application s'appuiera sur des « **normes harmonisées** » au niveau européen:
  * Définissent précisément les exigences applicables aux systèmes d'IA concernés
  * Commande au CEN/CENELEC de dix normes actuellement en cours de rédaction
  * La CNIL participe à leur élaboration

CNIL.

Contact : ia@cnil.fr

RESSOURCES :

* **SITE CNIL :** HTTPS://WWW.CNIL.FR/FR/TECHNOLOGIES/INTELLIGENCE-ARTIFICIELLE-IA
* **SITE LINC :** HTTPS://LINC.CNIL.FR/DOSSIER-INTELLIGENCE-ARTIFICIELLE