INTELLIGENCE ARTIFICIELLE

COMMENT CONCILIER PERFORMANCE ET PROTECTION DES DONNÉES PERSONNELLES ?

Juin 2024

Aurexia Institute

L'essor de l'Intelligence Artificielle

L'essor de l'IA demande de s'adapter à des changements bouleversants dans nos organisations et dans nos pratiques.

On distingue principalement deux types d'IA.

- Le premier type est l'IA forte, ce concept pour l'instant très théorique viserait à reproduire l'intelligence humaine dans son ensemble. Bien qu'il n'existe pas d'exemples clairs d'IA forte, le domaine de l'IA innove rapidement.
- Le second type d'IA est l'IA faible ou spécialisée conçue pour effectuer une tâche spécifique comme une requête sur *ChatGPT* ou une recommandation de contenu sur un réseau social. L'IA faible comprend de nombreuses sous-catégories d'IA comme l'IA générative et l'IA prédictive, ces types d'IA très populaires semblent déjà avoir des applications dans tous les domaines d'activités.

L'IA générative a la capacité de créer du texte, des images ou différents types de contenus tandis que l'IA prédictive identifie des modèles pour prévoir des événements futurs. Ces IA s'appuient principalement sur des modèles de ***Machine Learning*** qui permettent aux algorithmes d'apprendre de manière autonome à partir de bases de données puis d'améliorer leurs performances au fil du temps.

On voit déjà dans le secteur financier que ce soit en banque privée (Front ou middle office), en gestion des sinistres, dans la gestion de la relation client … de multiples applications de l'IA.

Sur le sujet de la sécurité financière par exemple, on y voit déjà de nombreux cas d'usages (KYC, LCB-FT) déjà exposés dans l'article «Intelligence Artificielle en Sécurité Financière» paru dans la Regwatch d'Aurexia de février 2024.

Pour faire face à l'augmentation des réglementations mais aussi pour maintenir sa position face à la concurrence accrue du secteur depuis DSP2, il devient indispensable de gagner en efficacité opérationnelle et de renforcer ses systèmes d'information.

Ce sont là les deux enjeux majeurs de l'intégration de l'IA pour les acteurs bancaires et assurantiels. Qui doivent aussi composer avec d'autres règlementations spécifiques. La question qui se pose alors est de savoir comment concilier ces enjeux avec ceux de la protection des données personnelles, garantie par le Règlement général sur la Protection des Données (« RGPD ») ?

Le développement de l'IA et les risques associés

L'impact du développement de l'IA sur les données personnelles

Pour développer l'IA, il est nécessaire d'entraîner les algorithmes en les nourrissant de quantités innombrables de données … notamment personnelles, par exemple par le biais de *web scraping* (aussi appelé « moissonnage de données »).

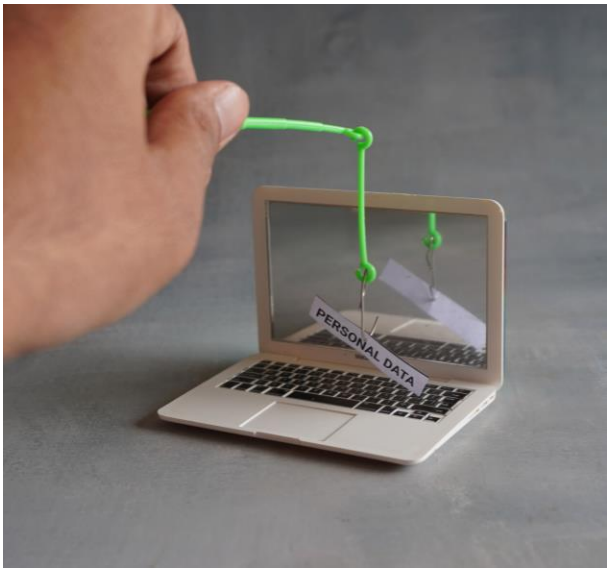
Tout en tenant compte de ce besoin, comment trouver un **équilibre entre l'amélioration des systèmes d'IA** et **la protection des données personnelles ?**

Les risques de l'IA sur les données personnelles

L'utilisation de l'IA soulève plusieurs difficultés pour la protection des données personnelles :

- Accès et analyse par des algorithmes d'IA d'une quantité exceptionnelle de données personnelles **sans le consentement des personnes concernées.**
- **Collecte de données sensibles** et de **traitements potentiellement illégaux, combinés à des croisements de données**
- **Manque de transparence** vis-à-vis des personnes concernées
- Difficultés liées à la **définition et l'implémentation de durées de conservations adaptées**
- **Mise en œuvre non effective des droits** tels que le **droit à l'effacement** qui pourrait impacter l'algorithme
- Violation de données en cas de **cyberattaques** ou de **fuite de données**
- **Discriminations** fondées sur des données sensibles, des biais de sélection ou biais d'attribution
- Prévalence entre les **analyses de risques de l'IA** et les **analyses d'impact du RGPD**

C'est dans ce contexte que les projets d'IA nécessitent d'être gérés **en conformité avec des règlementations de plus en plus strictes, techniques et parfois contradictoires.**



L'IA règlementée: focus sur l'IA Act

Les réglementations imposées à l'IA

Les réglementations actuelles peinent à établir des normes pouvant s'adapter assez rapidement à l'essor rapide de l'IA.

En effet le nouveau règlement **IA Act** visant à réglementer l'usage de l'IA dans l'UE et approuvé le 21 mai dernier **s'appliquera deux ans après son entrée en vigueur, avec plusieurs exceptions pour des dispositions spécifiques**.

Seront concernés par cette législation tous **fournisseurs**, **importateurs** ou **utilisateurs de l'IA** dans l'UE.

Les **principaux objectifs de l'IA Act** sont les suivants :

- Harmoniser les règles applicables à l'IA dans le but de favoriser le développement d'un marché unique en UE
- Assurer la sécurité, la conformité et l'alignement avec la Charte des Droits Fondamentaux de l'UE des systèmes d'IA
- Compléter le RGPD et la directive "Police-Justice" de 2016 concernant les traitements de données personnelles par les systèmes d'IA
- Garantir la sécurité légale des systèmes d'IA pour faciliter l'investissement et l'innovation
- Compléter la loi européenne sur la non-discrimination algorithmique (design, qualité et test de la donnée et obligations de gestion des risques)

Autant de principes que l'on retrouve dans la règlementation européenne sur la protection des données.

En réponse à une inquiétude grandissante du secteur de l'IA, la **CNIL** a publié le 8 avril 2024 ses **Recommandations sur l'application du RGPD au développement des systèmes d'IA**, qui se veulent complémentaires à l'IA Act.

Recommandations pour la mise en conformité de l'IA

Ces recommandations impliquent pour commencer l'adoption des pratiques de protection de données **dès la conception des projets d'IA (privacy-by-design), avant même leur déploiement.**

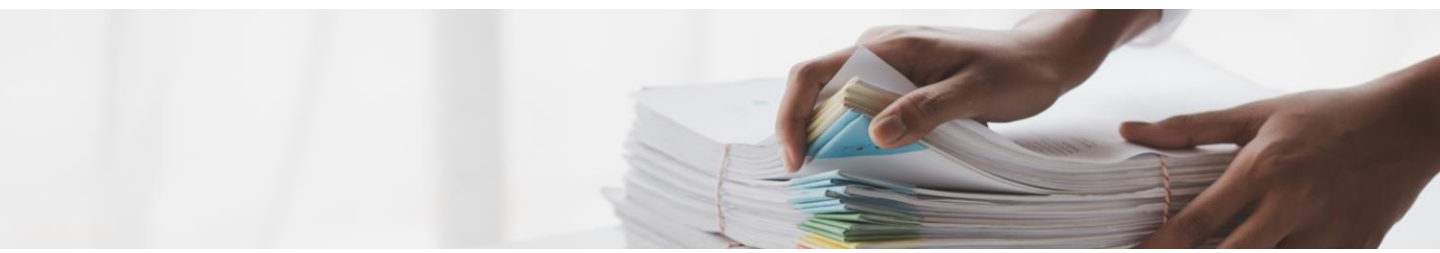
En synthèse, les pratiques à mettre en place d'après la CNIL sont - logiquement - les suivantes :

- La détermination d'un **objectif bien défini** ;
- La détermination des **responsabilités au sens du RGPD** ;
- Définir le **fondement juridique ou « base légale »** encadrant ce traitement de données personnelles ;
- Vérifier son **droit à réutiliser des données personnelles** ;
- Appliquer le **principe de minimisation des données personnelles** ;
- Définir **des durées de conservation** ;
- Réaliser une ou plusieurs **analyses d'impact sur la protection des données (AIPD)**

Ces recommandations sont une première étape afin d'aider les concepteurs d'IA à se mettre en conformité au RGPD et de ne pas subir les risques de non-conformité au RGPD dont les amendes qui peuvent atteindre jusqu'à 4% du chiffre d'affaires mondial de la société.

De plus, la CNIL songe à créer **un registre (facultatif) des entreprises qui ont recours au scraping «à des fins de constitution de bases de données d'entraînement pour le développement de systèmes d'IA».** Cette inscription pourrait faciliter l'exercice des droits pour les personnes concernées et être prise en compte comme mesure additionnelle dans la balance lorsque le responsable de traitement souhaite mobiliser la base légale de l'intérêt légitime.

C'est dans ce contexte qu'il existe un réel défi de réussir à se conformer aux règlementations en vigueur, et aux réglementations à venir tout en assurant la performance du système dans des marchés hautement concurrentiels.



Comment Aurexia vous accompagne ?

Nos équipes Data assurent une ***veille régulière*** *sur ces sujets afin de* ***compléter l'expertise sectorielle du cabinet Aurexia*** *et* ***accompagner ses clients sur les sujets innovants et structurants,*** *tout en favorisant une approche par les risques.*

- Audit et mise en place des mesures de conformité à l'IA Act dont la **réalisation d'analyses de risques relatives à l'IA combinées aux analyses d'impact relatives à la protection des données**
- Audit des données (gestion, disponibilité, qualité, usages), définition de dictionnaires de données, mise en place d'un lineage, mise en place d'une gouvernance de données.
- Analyse de risque liée à l'utilisation de systèmes d'IA, mise en place de mesures de mitigation des risques (sélection des données, validation du modèle, explicabilité, monitoring du drifting de modèle).

Vos contacts

Sarah VELTÉ
Manager Data Regulation
Tel : + 33 (0) 6 75 66 74 98
sarah.velte@aurexia.com

Damien ISAI
Manager Data Technology
Tel : + 33 (0) 7 70 32 42 50
damien.isai@agilee.one

Frédéric ALCARAS
Partner Aurexia
Tel : + 33 (0) 6 47 58 27 39
frederic.alcaras@aurexia.com

Aurexia

Bringing value, together

© 2024 Aurexia - Tous droits réservés
Cette publication est la propriété d'Aurexia. Toute reproduction et /ou diffusion, en tout ou partie, par quelque moyen que ce soit est interdite sans autorisation préalable.