Fiches pratiques sur le développement des systèmes d'intelligence artificielle

MARIE-AGNÈS NICOLET,

Présidente du Comité Magazine et du Comité d'Orientation du Centre des Professions Financières,
Présidente de Regulation Partners

Le Club des Marchés Financiers, présidé par Marie-Agnès NICOLET, a organisé un groupe de travail pour répondre à une consultation de la CNIL en août 2024 sur ses fiches pratiques sur le développement des systèmes d'intelligence artificielle.

Vous trouverez ci-après la réponse envoyée à la CNIL, résultat des réflexions et travaux du groupe de travail.

Fiches pratiques sur le développement des systèmes d'intelligence artificielle

Mobiliser la base légale de l'intérêt légitime pour développer un système d'IA
Commentaires et suggestions : Le groupe de travail propose d'abord de vérifier systématiquement que le traitement est nécessaire et la réelle incidence sur les personnes dont on a décidé de collecter les données. Par exemple, un système d'IA développé pour contrôler automatiquement des pièces d'identité des clients d'une institution financière nous paraît remplir la base légale de l'intérêt légitime, l'institution financière étant obligée de réaliser ce contrôle réglementaire.

Le groupe de travail suggère en complément la pseudonymisation **lorsque c'est possible** avant d'envoyer les données personnelles au modèle d'IA et tout au long de la phase de développement du modèle. Il paraît néanmoins nécessaire de différencier l'intérêt légitime selon le niveau de risque du SIA (tel que défini par le règlement européen sur l'IA). Par ailleurs, certains développements ne peuvent pas être réalisés avec des données pseudonymisées. (exemple d'un système de contrôle automatique de documents d'identité cité plus haut).

De surcroît, la durée de conservation doit être strictement limitée à ce qui est nécessaire pour accomplir la finalité spécifiée. Les données doivent être supprimées ou anonymisées une fois que cette finalité est atteinte.

Enfin, le chiffrement des données devrait être implémenté dès les premières étapes de la collecte pour renforcer la sécurité et la confidentialité des informations traitées. Ce processus devrait être maintenu tout au long du cycle de vie des données au sein du modèle d'IA.

Intérêt légitime : focus sur la diffusion des modèles en source ouverte (*open source*)
Commentaires et suggestions : Le fait d'avoir diffusé un modèle en open source permet en effet de le faire tester plus facilement par de nombreux acteurs. En revanche, il faut s'assurer que le modèle en open source ne contient pas les données personnelles qui ont servi à le développer ou ne permet pas de remonter à ces données personnelles.

Intérêt légitime : focus sur le moissonnage (*web scraping*)
Commentaires et suggestions : Le groupe de travail propose d'étudier les risques liés au web scraping de sources non publiques. Si le web scraping est réalisé sur des réseaux sociaux où les utilisateurs s'attendent à un certain degré de confidentialité, les risques pour les données personnelles nous paraissent significatifs.

Ces pratiques peuvent facilement entrer en conflit avec les droits à la vie privée des individus et nécessitent une analyse rigoureuse de la proportionnalité et de la nécessité du traitement envisagé.

Le groupe de travail souligne l'importance de préciser les modalités d'utilisation des données en la limitant dans le temps ou en formalisant un dispositif d'information des personnes concernées.

De plus, il apparait nécessaire de préciser la base légitime sur laquelle s'appuie l'utilisation des données, et imposer l'anonymisation de ces données avant transfert.

Informer les personnes
Commentaires et suggestions : Le groupe de travail recommande d'établir un protocole clair de notification pour les clients lorsque les finalités du traitement évoluent. Cette information doit être directe et accessible, potentiellement avec une interaction humaine pour en assurer la clarté. En revanche, lorsque les finalités du traitement restent les mêmes (par exemple pour un contrôle réglementaire qui désormais serait automatisé à l'aide d'un algorithme d'IA), une information au client ne paraît pas nécessaire car il a déjà été informé de la finalité de contrôle réglementaire du traitement.

Le groupe de travail rappelle la nécessité, pour tout développeur/utilisateur d'une IA, de garantir l'explicabilité des décisions prises par ce système.

De plus, en cas de contestation d'une décision prise par un système d'IA (ex : modèle de système de risque de crédit), le groupe de travail propose d'ajouter l'obligation pour les utilisateurs et concepteurs de fournir des informations permettant à la personne concernée d'expliquer la décision prise.

Respecter et faciliter l'exercice des droits des personnes concernées
Commentaires et suggestions : Le groupe de travail précise que l'obligation de respecter les droits des personnes concernées devrait être imposée **au concepteur du modèle IA qui a utilisé les données personnelles lors du développement, et non à l'utilisateur final qui ne se servirait pas** de données personnelles mais uniquement du modèle déjà développé, sous réserve que ce dernier ne procède lui-même à aucun nouveau développement.

Annoter les données
Commentaires et suggestions : Les procédures proposées dans la consultation pour annoter les données semblent trop lourdes et risquent de freiner l'innovation et le développement de modèles d'IA. Le groupe de travail suggère de permettre aux développements de l'IA de se poursuivre librement et d'intervenir réglementairement uniquement en cas de déviations ou d'abus.
Il s'agirait a minima de faire une distinction claire entre les systèmes d'IA à haut risque et les autres (selon la définition du règlement européen), afin d'appliquer des normes différenciées et de limiter les dispositifs proposés par la CNIL aux SIA à haut risque.

Garantir la sécurité du développement d'un système d'IA
Commentaires et suggestions : Le groupe de travail recommande d'adopter une stratégie de sécurité exhaustive qui inclut le chiffrement des données et des méthodes adéquates de gestion des accès, assurant ainsi la protection des données à chaque étape de leur traitement.

Les mesures de sécurité devraient être adaptées en fonction des objectifs et des niveaux de risque associés aux différents systèmes d'IA.

La mise en place de contrôles réguliers pour assurer la cohérence des résultats fournis par les systèmes d'IA ainsi que l'incorporation des SIA dans les audits de cybersécurité sont les solutions préconisées.

Ces mesures de sécurité, bien que nécessaires, doivent être proportionnelles afin de ne pas entraver l'innovation technologique. De même, les stratégies de gouvernance pour être efficaces doivent être adaptées aux risques réels.

Le groupe de travail rappelle la nécessité de procéder à l'évaluation des risques liés aux éventuels changements de propriétaires des systèmes d'IA afin de formaliser le dispositif de maîtrise des risques.

De plus, le groupe de travail propose l'intégration d'une obligation de réajustement régulier des modèles avec une information claire sur les évolutions.

Enfin, le groupe de travail souligne le nécessaire encadrement des systèmes d'IA les plus sensibles pour valider et contrôler les résultats du système. ■