Travaux sur la constitution de bases de données pour l'intelligence artificielle

Appel à contributions

Publié le 27/07/2023

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Introduction

Pour alimenter ses travaux, et afin de bénéficier de l'expertise pratique et opérationnelle des acteurs de l'IA, la CNIL souhaite recueillir les contributions de tous les acteurs concernés sur plusieurs points structurants de son analyse.

Comment contribuer ?

La CNIL vous invite à rédiger des réponses **sous forme d'exemples concrets** mis en place, qui seront particulièrement utiles pour étayer ses futures recommandations.

Les contributions peuvent être transmises à l'adresse **ia@cnil.fr**.

Il n'est pas nécessaire de répondre à l'ensemble des questions soulevées dans le questionnaire. Il est même recommandé de fournir des contributions ciblées sur les questionnements recensés ci-dessous sur lesquels vous disposez d'une expertise juridique, technique ou opérationnelle spécifique.

Quelles informations seront collectées ?

Les contributeurs sont invités à se présenter pour contextualiser leurs contributions (nom et catégorie de l'organisme : chercheur, association représentative de la société civile, administration publique, entreprise privée, développeur ou utilisateur de systèmes d'IA, etc.).

La CNIL traite les données ainsi recueillies afin d'analyser les observations des contributeurs en vue d'adopter une position sur les sujets concernés. Les données sont également collectées pour réaliser des statistiques relatives aux contributions et, si nécessaire, pour contacter les contributeurs afin d'approfondir les échanges ou les tenir informés des suites de la consultation.

Vous pouvez :

- accéder à vos données ;
- vous opposer à leur traitement ;
- demander leur rectification ou leur effacement.
- exercer votre droit à la limitation du traitement de vos données.

En savoir plus sur la gestion de vos données et vos droits.

Attention : dans votre contribution, signalez tout élément protégé par des droits de propriété littéraire ou artistique (précisez, dans ce cas, si vous en permettez ou non la communication), ou par le secret des affaires.

En effet, toutes les contributions reçues par la CNIL peuvent faire l'objet d'une demande d'accès en tant que documents administratifs (code des relations entre le public et l'administration). Toutefois, la CNIL n'est pas tenue de suivre votre évaluation sur ce qui est protégé ou non.

Information sur votre organisme

Nom de l'organisme :

Catégorie de l'organisme (chercheur, association représentative de la société civile, administration publique, entreprise privée, développeur ou utilisateur de systèmes d'IA, etc.) :

Assurer le caractère déterminé, explicite et légitime de la finalité

Tout traitement de données personnelles doit poursuivre une finalité (ou objectif) déterminée, explicite et légitime, portée à la connaissance des personnes concernées. Le cas des IA à usage général et des modèles de fondation interroge sur la finalité de ces systèmes génériques.

La CNIL souhaite recevoir des contributions sur ces questions :

- Comment définir la finalité d'un traitement visant à entraîner un modèle d'IA lorsque l'usage opérationnel prévu n'est pas unique et précisément identifié (par exemple en cas de développement d'IA générative ou de système d'IA à usage général) ?
    - Vous semble-t-il pertinent à cette fin de faire référence à la capacité ou la tâche du modèle (par exemple reconnaissance faciale, détection et classification d'objets, segmentation/partitionnement ou « *clusterisation* » en anglais) ?
    - Vous semble-t-il pertinent à cette fin de faire référence aux modes de réutilisations envisagées ou envisageables du modèle (par exemple, exploitation commerciale, recherche scientifique, diffusion en source ouverte ou fermée) ?
    - Vous semble-t-il pertinent à cette fin de faire référence aux cas d'usage connus ou envisageables du système d'IA (diagnostic médical, conduite autonome, etc.) ?
- Dans quel cas la conception du système d'IA vous semble-t-elle poursuivre une finalité de recherche scientifique ? Si le système d'IA développé à des fins scientifiques est également commercialisé, comment distinguer en droit et en pratique la finalité de recherche de la finalité commerciale ?
- Dans quel cas et à quelles conditions la conception du système d'IA vous semble-t-elle poursuivre une finalité statistique ?

Sélection et minimisation des données

Tout traitement de données personnelles doit respecter le principe de minimisation des données. Par ailleurs, la constitution de bases de données pour l'IA passe toujours par des étapes de sélection et de filtrage des données, pour garantir la performance des modèles entraînés (par ex. : dédoublonnage) ou pour éviter le traitement de données particulièrement porteuses de risques (par ex. : numéros de carte bancaire).

La CNIL souhaite recevoir des contributions sur les pratiques à l'état de l'art et les mesures de minimisation mobilisées :

- Pour un exemple donné, quelles sont les méthodes de sélection des données mises en place :
    - En amont de la collecte (périmètre, filtres, etc.) ?
    - Au moment de la collecte (via l'exclusion de données non pertinentes par exemple) ? ;
    - En aval de la collecte (par des mesures d'anonymisation et de pseudonymisation notamment) ?
- Quelles sont les contraintes pesant sur cette phase de collecte et quels sont les risques identifiés ?
- Quelles sont les mesures relevant, d'après vous, de bonnes pratiques à mettre en œuvre concernant :
    - La vérification et l'amélioration de la qualité des données (revue aléatoire des données et de leur annotation, procédures de validation croisée des annotation, procédés techniques automatisés, etc.) ?

- La mesure et l'amélioration de la représentativité des données (sur la diversité de situations, personnes, conditions d'utilisation du système d'IA telles que des outils statistiques, des outils permettant de constituer des sous-ensembles de données représentatifs pour l'apprentissage, etc.) ?
- La validation de la méthode la plus adaptée pour la tâche visée (comparaison entre des systèmes basés sur de l'apprentissage ou non, un développement internalisé ou externalisé tel que l'utilisation de modèles pré-entraînés, intégrant une mise en balance avec le coût d'une collecte de données et la mise en conformité, etc.) ?
- La sélection des catégories et du volume de données nécessaires pour l'apprentissage (comparaison de la performance obtenue en retirant certaines variables ou en réduisant le volume de données utilisées, analyse en composantes principales (*principal component analysis*), etc.) ?
- Les techniques permettant de collecter les données (par moissonnage, ou *scraping*, via l'utilisation d'une API, par le téléchargement d'un fichier, etc.) ?

Adopter une démarche respectueuse du principe de protection des données dès la conception et par défaut

La CNIL souhaite identifier les ressources techniques, contractuelles ou organisationnelles permettant de mettre en place le traitement dans le respect du principe de protection des données dès la conception et par défaut.

À ce stade, la CNIL a identifié les techniques et mesures suivantes :

- Données synthétiques.
- Apprentissage fédéré.
- Calcul multipartite sécurisé.
- Anonymisation ou pseudonymisation (grâce à la confidentialité différentielle, par exemple).
- Recours à un intermédiaire de données ou à un tiers de confiance pour la mise en œuvre de mesures protectrices comme l'anonymisation ou l'exercice des droits.
- Licences pour la réutilisation des jeux de données et modèles d'IA.
- Environnements d'exécution sécurisé.
- Certaines techniques de désapprentissage machine.
- Chiffrement homomorphe pour l'apprentissage.
- Mise en place d'un comité d'éthique.

La CNIL souhaite recevoir des contributions sur des mises en œuvre opérationnelles de mesure de ce type sur des exemples concrets :

- Pour quelles applications et sur quels types de données ces techniques ont-t-elles été appliquées ?
- Quelles sont les conditions de réussite de l'intégration de ces techniques (environnement technique, gouvernance, etc.) ?

L'intérêt légitime : assurer l'équilibre entre les droits et intérêts en cause

Dans l'hypothèse où le traitement de constitution de la base de données pour l'IA ou celui de configuration (« entraînement ») du modèle d'IA pourrait reposer sur l'intérêt légitime du responsable du traitement, il convient préalablement de s'assurer que le traitement ne heurte pas les droits et intérêts des personnes dont les données sont traitées.

La CNIL souhaite recevoir des contributions sur les différentes étapes permettant d'évaluer ce point :

- Quelles sont les conséquences que le traitement visant à la constitution d'une base de données pour l'IA et/ou l'entraînement du modèle peut avoir sur les personnes concernées ?
    - Ces traitements constituent-ils, selon vous, une intrusion dans la vie privée ? Dans quels cas ?
    - Ces traitements peuvent-ils avoir un impact, selon vous, sur les autres droits fondamentaux (liberté d'expression, liberté d'information, liberté de conscience, etc.) ?
    - Ces traitements peuvent-ils avoir, selon vous, d'autres impacts concrets (services accessibles à l'utilisateur, exclusion de certains droits), notamment du fait de l'automatisation et de l'ampleur de la collecte des informations ?
- Selon vous, quelles sont les attentes raisonnables des personnes concernées vis-à-vis de ces traitements et des données qui servent à les entraîner ?
    - Dans quels cas et pour quelles catégories de données vous semble-t-il possible de considérer que la constitution et l'usage de la base de données pour l'entraînement d'IA entrent dans les attentes raisonnables des personnes (notamment pour les bases de données composées de données librement accessibles) ?
    - Quelles sont les limitations des finalités de l'IA qui pourraient correspondre aux attentes raisonnables des personnes (par exemple, le fait que l'IA est uniquement destinée à la recherche) ?
- Quelles sont les mesures compensatoires ou additionnelles pertinentes qui pourraient limiter les impacts du traitement sur les personnes concernées ?
    - En matière d'information des personnes (mécanismes de traçabilité des données en cas de réutilisation de jeux de données préconstitués par exemple) ?
    - En matière d'exercice des droits (centralisation ou transmission des demandes d'exercice de droit en cas de pluralité d'acteurs, mécanismes permettant de faciliter l'exercice d'un droit d'accès, par exemple au moyen d'un moteur de recherche, etc.) ?
    - En matière de gestion des données (filtre, sélection, anonymisation, etc.) ?
    - En matière de design de service (ajout de modules visant à contrôler les entrées et/ou les sorties du modèle par exemple) ?
- La publication du modèle d'IA en source ouverte vous semble-t-elle contribuer à un meilleur équilibre entre les droits et intérêts en cause ? ? Si oui, dans quelle mesure et dans quels cas ?
- Selon vous, dans quels cas l'exercice du droit des personnes pourrait être exclu (en particulier du droit d'opposition, mais aussi s'agissant plus largement du droit à la modification, à l'effacement, au droit d'accès, etc.) ? »
- Auriez-vous des exemples de jeux de données publiquement accessibles :
    - Sur lesquels vous souhaitez attirer l'attention de la CNIL dans le cadre de l'établissement de sa doctrine en raison des difficultés de conformité qu'ils semblent présenter ?
    - Ou à l'inverse qui illustrent des bonnes pratiques que vous souhaiteriez voir dans les recommandations de la CNIL ?