

Déclaration commune sur la mise en place de cadres de gouvernance des données fiables pour favoriser une intelligence artificielle innovante et protectrice de la vie privée

Le 11 février 2025

1. L'intelligence artificielle (IA) offre d'immenses possibilités au profit de l'humanité, de l'innovation scientifique, de l'économie et de la société dans son ensemble. L'IA présente également des risques importants en ce qui concerne la protection des droits fondamentaux comme la protection des données et de la vie privée, mais elle présente aussi des risques en matière de discrimination, de désinformation et d'hallucination qui sont souvent causés par le traitement inapproprié des données.
2. Nous reconnaissons la nécessité de cultiver pleinement la confiance du public et de tirer parti des avantages transformateurs que l'IA pourrait apporter. Nous rappelons que l'IA doit être développée et déployée conformément aux règles relatives à la protection des données et de la vie privée et à d'autres normes. Cela comprend l'intégration des principes de protection des données dès la conception dans les systèmes d'IA à partir de l'étape de planification initiale et la mise en œuvre de cadres de gouvernance des données internes robustes. Ces cadres devraient intégrer des mesures de protection techniques et procédurales pour une gestion et une atténuation efficaces des risques tout au long du cycle de vie d'un système d'IA.
3. De plus, nous reconnaissons que, dans l'environnement actuel relatif au développement et au déploiement de l'IA, le traitement des données est devenu extrêmement complexe. En effet :
 - a. L'IA est développée et déployée dans de nombreux secteurs différents, notamment la santé, les services publics, la sécurité publique, les ressources humaines et l'éducation.
 - b. Elle met en cause un grand nombre de parties prenantes de partout dans le monde et des chaînes de valeur complexes, y compris des créateurs d'ensembles de données, des fournisseurs de modèles, des plateformes d'hébergement d'ensembles de données et de modèles, des intégrateurs, des annotateurs, des déployeurs de systèmes et des utilisateurs finaux.
 - c. L'IA fonctionne à grande échelle avec des technologies nécessitant de grandes quantités de données qui sont au cœur de ces systèmes.
 - d. Elle met en cause un traitement des données complexe qui pose des défis importants en lien avec son contrôle et qui fait augmenter les besoins de transparence afin de favoriser la protection de la vie privée et d'autres droits fondamentaux.
 - e. L'IA évolue à un rythme très rapide, et des avancées scientifiques et technologiques majeures sont enregistrées quotidiennement.

4. Il est donc de plus en plus urgent pour les citoyennes et citoyens et les entreprises d'obtenir des réponses et une certitude juridique afin de permettre le développement de l'IA dans des cadres de gouvernance des données fiables. Parallèlement, l'application des règles devrait offrir un degré de souplesse suffisant pour permettre la mise en œuvre de diverses initiatives novatrices conformément aux dispositions relatives à la protection de la vie privée et des données personnelles. Nous reconnaissons donc l'importance de soutenir les acteurs de l'écosystème de l'IA dans leurs efforts visant à se conformer aux règles de protection des données et de la vie privée et de les aider à concilier innovation et respect des droits des individus.

Soulignant le rôle de premier plan des autorités de protection des données dans l'élaboration de la gouvernance des données afin de relever les défis en constante évolution liés à l'IA, nous nous engageons à faire ce qui suit :

5. Favoriser notre compréhension commune des motifs légitimes de traitement des données dans le contexte de l'entraînement de l'IA dans nos juridictions respectives. Des normes et des exigences claires doivent être élaborées pour garantir que les données utilisées pour l'entraînement de l'IA sont traitées de manière licite, que ce soit en fonction du consentement, de la nécessité contractuelle, de l'intérêt légitime ou d'autres justifications juridiques. Ce faisant, il convient de prêter attention à divers facteurs pertinents, notamment les fins précises du développement de l'IA, les caractéristiques des données requises, les attentes raisonnables des individus concernés et les stratégies d'atténuation des risques connexes.
6. Échanger de l'information et établir une compréhension commune des mesures de sécurité proportionnées basées sur des évaluations scientifiques rigoureuses et fondées sur des données probantes et adaptées à divers cas d'utilisation. La pertinence de ces mesures devrait être régulièrement mise à jour afin de suivre le rythme de l'évolution des technologies et des pratiques de traitement des données de l'IA.
7. Surveiller en permanence les répercussions aussi bien techniques que sociétales de l'IA et tirer parti, dans la mesure du possible, de l'expertise et de l'expérience des autorités de protection des données et d'autres entités pertinentes, notamment les organisations non gouvernementales, les autorités publiques, le milieu universitaire et les entreprises, dans le cadre des politiques relatives à l'IA.
8. Réduire les incertitudes juridiques et créer un espace propice à l'innovation lorsque le traitement des données est essentiel au développement et au déploiement de l'IA. Cela peut inclure des mesures institutionnelles, comme des bacs à sable réglementaires, ainsi que des outils permettant de mettre en commun les pratiques exemplaires. Ces mesures et outils devraient reposer sur la confiance du public et être conformes aux principes de protection de la vie privée et des données.
9. Renforcer nos interactions avec les autorités compétentes, entre autres avec celles chargées de la concurrence, de la protection des consommateurs et de la propriété intellectuelle, afin de faciliter la cohérence et de favoriser les synergies entre les différents cadres réglementaires applicables aux systèmes, outils et applications d'IA. Il conviendrait également d'encourager le dialogue entre les différents acteurs de l'écosystème de l'IA.

Haksoo Ko
Président

Marie-Laure Denis
Présidente

Commission de protection des
renseignements personnels
Corée

John Edwards

Commissaire
Commissariat à l'information
Royaume-Uni

Carly Kind

Commissaire à la protection de la vie
privée
Commissariat à l'information de l'Australie
Australie

Borislav Bozhinov

Комисия за защита на личните данни
Président
Bulgarie

Zdravko Vukić

Agencija za zaštitu osobnih podataka
Directeur
Croatie

Andreas Hartl

Bundesbeauftragter für den Datenschutz
und die Informationsfreiheit
Sous-commissaire
Allemagne

Ginevra Cerrina Feroni

Garante per la protezione dei dati
personali
Vice-présidente
Italie

Michael Webster

Commissariat à la protection de la vie
privée
Commissaire à la protection de la vie
privée
Nouvelle-Zélande

Ken Chongwei YANG

Bureau de protection des données
personnelles

Commission nationale de l'informatique et
des libertés
France

Dale Sunderland

Commissaire à la protection des données
Irlande

Hielke Hijmans

Autorité de protection des données
Commissaire
Belgique

Philippe Dufresne

Commissariat à la protection de la vie
privée
Commissaire à la protection de la vie
privée
Canada

Helja-Tuulia Pihamaa

Tietosuojavaltuutetun toimisto
Sous-commissaire
Finlande

Ada CHUNG Lai-ling

Commissariat à la protection des données
personnelles
Hong Kong

Aleid Wolfsen

Autoriteit Persoonsgegevens
Président
Pays-Bas

Alain Herrmann

Commission nationale pour la protection
des données
Présidente
Luxembourg

Lorenzo Cotino Hueso

Agencia Española de Protección de Datos
Président

Directeur
Région administrative spéciale de Macao,
Chine

Mirosław Wróblewski
Urząd Ochrony Danych Osobowych
Président
Pologne

Espagne

Eric Leijonram
Integritetsskyddsmyndigheten
Directeur général
Suède