



Strasbourg, le 25 janvier 2019

T-PD(2019)01

**COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES  
PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES  
À CARACTÈRE PERSONNEL**

**(Convention 108)**

**LIGNES DIRECTRICES SUR  
L'INTELLIGENCE ARTIFICIELLE ET LA PROTECTION DES DONNEES**

Direction générale - Droits de l'Homme et État de droit

Les systèmes, logiciels et dispositifs<sup>1</sup> (appelés ci-après « applications ») basés sur l'intelligence artificielle (« IA ») procurent des solutions nouvelles et appréciables afin de répondre à des besoins et des défis voyant le jour dans de nombreux domaines, qu'il s'agisse notamment de maisons ou de villes connectées, du secteur industriel ou de celui de la santé et de la prévention des infractions. Les applications de l'IA peuvent constituer des outils utiles pour la prise de décisions, en particulier pour des politiques inclusives et basées sur des éléments probants. Comme cela peut être le cas avec d'autres innovations technologiques, ces applications peuvent avoir des conséquences défavorables pour les personnes et la société. Afin de prévenir cela, les Parties à la Convention 108 s'assureront et permettront que le développement et l'utilisation de l'intelligence artificielle respectent le droit à la vie privée et à la protection des données à caractère personnel (article 8 de la Convention européenne des droits de l'Homme), renforçant ainsi les droits de l'Homme et les libertés fondamentales.

Ces lignes directrices fournissent un ensemble de mesures de référence que les gouvernements, les développeurs en IA, les fabricants, les prestataires de services devraient appliquer pour garantir que les applications de l'IA ne nuisent à la dignité humaine, aux droits de l'Homme et aux libertés fondamentales de toute personne, notamment en ce qui concerne le droit à la protection des données à caractère personnel<sup>2</sup>.

Rien dans les présentes lignes directrices ne saurait être interprété comme excluant ou limitant les dispositions de la Convention européenne des droits de l'homme et de la Convention 108. Les présentes lignes directrices tiennent également compte des nouvelles garanties de la Convention 108 modernisée (communément appelée « Convention 108+ »)<sup>3</sup>.

## I. Orientations générales

1. La protection de la dignité humaine et la sauvegarde des droits de l'Homme et des libertés fondamentales, en particulier le droit à la protection des données à caractère personnel, sont essentiels au développement et à l'adoption d'applications basées sur l'IA qui sont susceptibles de produire des effets sur les personnes et la société. Ceci est particulièrement important lorsque l'IA est utilisée dans les processus décisionnels.
2. Un développement de l'IA reposant sur le traitement de données à caractère personnel devrait être fondé sur les principes figurant dans la Convention 108+. Les piliers de cette approche sont la licéité et la loyauté du traitement, la définition de la finalité, la proportionnalité du traitement, la prise en compte de la protection des données dès la conception (« *privacy by-design* ») et par défaut, la responsabilité et la démonstration de la conformité (« *accountability* »), la transparence, la sécurité des données et la gestion du risque.
3. Une approche centrée sur la prévention et la réduction des risques potentiels dus au traitement des données personnelles est un élément nécessaire à une innovation responsable dans le domaine de l'IA.
4. Conformément aux orientations sur l'évaluation des risques contenues dans les lignes directrices sur les mégadonnées (*Big Data*)<sup>4</sup> adoptées par le Comité de la Convention 108 en 2017, une vision plus large des éventuelles conséquences du traitement des données devrait être adoptée. Elle devrait examiner non seulement les droits de l'Homme et les libertés fondamentales, mais aussi le fonctionnement des démocraties et les valeurs éthiques et sociales.
5. Les applications de l'IA doivent, à tout moment, pleinement respecter les droits des personnes concernées, notamment conformément à l'article 9 de la Convention 108+.

---

<sup>1</sup> La définition suivante de l'Intelligence artificielle est actuellement disponible sur le site web du Conseil de l'Europe : <https://www.coe.int/fr/web/human-rights-rule-of-law/artificial-intelligence/glossary> « Ensemble de sciences, théories et techniques dont le but est de reproduire par une machine des capacités cognitives d'un être humain. Les développements actuels visent, par exemple, à pouvoir confier à une machine des tâches complexes auparavant déléguées à un humain. »

<sup>2</sup> Ces lignes directrices sont à la fois tirées et basées sur le rapport sur l'Intelligence artificielle (« Intelligence artificielle et protection des données: défis et solutions possibles »), disponible à l'adresse suivante: <https://rm.coe.int/intelligence-artificielle-et-protection-des-donnees-enjeux-et-solution/168091f8a5>

<sup>3</sup> Protocole d'amendement (STCE n° 223) à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

<sup>4</sup> Lignes directrices sur les mégadonnées disponibles à l'adresse <https://rm.coe.int/CoERMPublicCommnSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a>.

6. Les applications de l'IA devraient permettre aux personnes concernées d'exercer un contrôle significatif sur le traitement des données et leurs effets connexes tant au niveau individuel que sur la société.

## II. Orientations à l'intention des développeurs, fabricants et prestataires de service

1. Les développeurs, fabricants et prestataires de service en IA devraient adopter une approche de conception des produits et services centrée sur les valeurs, conformément à la Convention 108+, notamment son article 10.2, et aux autres instruments pertinents du Conseil de l'Europe.
2. Les développeurs, fabricants et prestataires de service en IA devraient évaluer les éventuelles conséquences négatives des applications d'IA sur les droits de l'Homme et libertés fondamentales des personnes concernées et au regard de ces conséquences, adopter une approche de précaution basée sur des mesures de prévention et de réduction des risques appropriées.
3. Les développeurs, fabricants et prestataires de service en IA devraient, à tous les stades du traitement des données, y compris lors de la collecte, adopter une approche des droits de l'Homme dès la conception (*by-design*) et éviter tout biais potentiel, y compris les biais non intentionnels ou cachés, ainsi que les risques de discrimination ou d'autres effets négatifs sur les droits de l'Homme et libertés fondamentales des personnes concernées.
4. Les développeurs d'IA devraient évaluer de manière critique la qualité, la nature, l'origine et la quantité des données à caractère personnel utilisées, en réduisant les données inutiles, redondantes ou marginales lors des phases de conception et d'apprentissage, puis en vérifiant l'exactitude du modèle lorsqu'il est alimenté par de nouvelles données. Le recours à des données synthétiques<sup>5</sup> pourrait être considéré comme une solution possible pour minimiser la quantité de données personnelles traitées par des applications de l'IA.
5. Les risques d'impact négatif sur les personnes et la société inhérents aux données décontextualisées<sup>6</sup> et aux modèles algorithmiques décontextualisés<sup>7</sup> devraient être dûment pris en compte lors du développement et de l'utilisation d'applications de l'IA.
6. Les développeurs, fabricants et prestataires de service en IA sont encouragés à recourir à des comités d'experts issus de différents domaines ainsi qu'à des institutions universitaires indépendantes qui peuvent contribuer à concevoir des applications de l'IA fondées sur les droits de l'Homme et orientées de façon éthique et sociale, et à détecter des biais potentiels. Le rôle de ces comités peut être particulièrement important dans les domaines où la transparence et la mobilisation des parties prenantes peuvent être plus difficiles en raison d'intérêts et de droits concurrents, comme par exemple dans les domaines de la justice prédictive, de la prévention et de la détection des infractions.
7. Des démarches participatives d'évaluation des risques, reposant sur l'engagement actif des personnes et groupes potentiellement affectés par les applications de l'IA, devraient être encouragées.
8. Tous les produits et services de l'IA devraient être conçus de manière à garantir le droit des personnes à ne pas être soumises à des décisions qui les affectent de manière significative prises uniquement sur le fondement d'un traitement automatisé de données, sans que leur point de vue soit pris en compte.
9. Afin d'accroître la confiance des utilisateurs, les développeurs, fabricants et prestataires de service en IA sont encouragés à concevoir leurs produits et services de manière à préserver la liberté de choix de l'utilisateur concernant l'usage de l'IA en proposant des alternatives réalistes aux applications de l'IA.
10. Les développeurs, fabricants et prestataires de service en IA devraient adopter des formes de vigilance algorithmique qui fassent la promotion de la responsabilité de toutes les parties

---

<sup>5</sup> Les données synthétiques sont générées à partir d'un modèle construit sur des données réelles. Elles devraient être représentatives des données réelles originales. Voir la définition de données synthétiques de l'OCDE. Glossary of Statistical Terms' 2007. ("An approach to confidentiality where instead of disseminating real data, synthetic data that have been generated from one or more population models are released").

<sup>6</sup> A savoir le risque d'ignorer l'information contextuelle propre à la situation spécifique dans laquelle les solutions d'IA proposées devraient être appliquées.

<sup>7</sup> Ceci se produit en utilisant des modèles d'IA initialement conçus pour un autre contexte ou pour des finalités différentes.

prenantes et ce tout au long du cycle de vie des applications afin d'assurer leur conformité avec les principes et la législation relatifs à la protection des données personnelles et aux droits de l'Homme.

11. Les personnes concernées devraient être informées si elles interagissent avec des applications de l'IA et ont le droit de connaître du raisonnement qui sous-tend les opérations de traitement des données qui les concernent. Ceci devrait inclure les conséquences de ce raisonnement.
12. Le droit d'opposition devrait être garanti par rapport au traitement basé sur des technologies qui influencent les opinions et le développement personnel des individus.

### III. Orientations à l'intention des législateurs et décideurs

1. La confiance dans les produits et services de l'IA pourrait être renforcée grâce au respect du principe de la responsabilité des développeurs en IA, l'adoption de procédures d'évaluation des risques et la mise en œuvre d'autres mesures appropriées, tels que les codes de conduite et les mécanismes de certification.
2. Sous réserve des secrets protégés par la loi, les procédures de passation des marchés publics devraient imposer aux développeurs, fabricants et prestataires de service en IA des devoirs spécifiques de transparence et d'évaluation préalable de l'impact des traitements de données personnelles sur les droits de l'Homme et libertés fondamentales des systèmes d'IA, ainsi que de vigilance à l'égard des effets défavorables potentiels et des conséquences des applications d'IA (ci- après dénommée 'vigilance algorithmique »<sup>8</sup>).
3. Les autorités de contrôle devraient être dotées de ressources suffisantes pour encourager et contrôler les programmes de vigilance algorithmique des développeurs, fabricants et prestataires de service en IA.
4. Une dépendance excessive des solutions fournies par les applications de l'IA, de même que la crainte de contester des décisions suggérées par des applications de l'IA risquent d'altérer l'autonomie de l'intervention humaine dans la prise de décision. Le rôle de l'intervention humaine dans le processus décisionnel et la liberté des décideurs humains de ne pas suivre les résultats de recommandations fondées sur l'utilisation de l'IA devraient en conséquence être préservés.
5. Les développeurs, fabricants et prestataires de service en IA devraient consulter les autorités de contrôle dès lors que les applications de l'IA peuvent avoir un impact significatif sur les droits de l'Homme et les libertés fondamentales des personnes concernées.
6. La coopération devrait être encouragée entre autorités de contrôle de la protection des données et d'autres instances ayant des compétences liées à l'IA, telles que les autorités de régulation en matière de protection des consommateurs ; concurrence ; anti-discrimination ; médias et autorités sectorielles.
7. Des mécanismes appropriés visant à garantir l'indépendance des comités d'experts mentionnés à la section II.6 devraient être mis en place.
8. Les personnes, les groupes et les autres parties prenantes devraient être informés et impliqués de façon active dans le débat relatif au rôle que l'IA devrait jouer dans le modelage des dynamiques sociales, et dans les processus décisionnels les affectant.
9. Les décideurs devraient affecter des ressources à l'éducation au numérique afin de renforcer la sensibilisation des personnes concernées et la compréhension des applications de l'IA et de leurs effets. Ils devraient également encourager la formation professionnelle des développeurs en IA afin de les sensibiliser aux effets potentiels de l'IA sur les personnes et la société. Ils devraient soutenir la recherche en matière d'IA orientée vers les droits de l'Homme.

---

<sup>8</sup> S'agissant de la notion de vigilance algorithmique, telle que l'adoption de l'*accountability* et de pratiques en matière de sensibilisation et de gestion des risques liés à des effets négatifs et des conséquences tout au long des cycles de vie complets de ces applications, voir aussi la Déclaration sur l'éthique et la protection des données dans l'IA de la 40<sup>ème</sup> Conférence Internationale des Autorités de protection des données et Commissaires à la vie privée ; voir également le rapport sur l'IA (note de bas de page 2), section II.4.