



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

Charte pour des usages éthiques de l'intelligence artificielle au Ministère de l'Intérieur

« Pour une intelligence artificielle responsable, transparente et au service de l'intérêt général »



PROPOS LIMINAIRES

L'intelligence artificielle (IA*) représente une avancée technologique majeure, susceptible de transformer en profondeur les modes d'action des administrations publiques. Par IA, on entend l'ensemble des systèmes informatiques capables de simuler certaines capacités cognitives humaines telles que l'apprentissage, le raisonnement, la planification ou encore la reconnaissance de formes en vue d'accomplir des tâches spécifiques, avec ou sans supervision humaine.

Dans un contexte de numérisation croissante des services publics, l'IA offre des opportunités considérables : amélioration de l'efficacité administrative, aide à la décision, personnalisation des services aux usagers, traitement de grands volumes de données, etc. Ses potentialités sont nombreuses, tant pour les agents que pour les usagers du service public.

Si les technologies intégrant de l'IA peuvent susciter des questionnements éthiques et soulever des défis sociétaux, en raison de leurs spécificités et des craintes qu'elles inspirent, son intégration dans les missions de service public nécessite un cadre éthique fort et partagé.

L'usage de l'IA par le Ministère de l'Intérieur engage des principes fondamentaux : respect des droits et libertés des citoyens, transparence de l'action publique, redevabilité des décisions, lutte contre les biais et discriminations, protection des données à caractère personnel, sécurité des systèmes, et préservation de l'autonomie humaine dans les choix décisionnels.

C'est dans cet esprit que cette Charte des usages éthiques de l'intelligence artificielle a été élaborée.

Elle vise à poser les repères éthiques indispensables à une mise en œuvre responsable et maîtrisée de l'IA au Ministère de l'Intérieur dans le respect du cadre légal, de la déontologie et de nos valeurs, au service de l'intérêt général.

La finalité première de cette charte est de définir les bonnes pratiques et les règles de fonctionnement, une référence collective sur les comportements et attitudes attendues, de favoriser le respect mutuel et la protection des intérêts communs, d'ancrer une culture commune de vigilance, de responsabilité et de transparence autour des outils d'intelligence artificielle.

Cette charte s'adresse à l'ensemble des agents titulaires et contractuels du MI, aux agents d'autres institutions publiques mis à disposition, à tous les personnels au service occasionnel ou permanent du MI, aux alternants, stagiaires et élèves, aux partenaires et prestataires intervenant dans la conception, le développement, l'acquisition, le déploiement ou l'usage de systèmes d'IA dont la finalité et les règles sont définies par le Ministère de l'Intérieur et relèvent de sa responsabilité (sauf dispositions réglementaires ou législatives liés à des traitements spécifiques).

Elle s'inscrit dans la continuité des engagements pris par la France au niveau national et international, notamment dans le cadre de la Déclaration de l'UNESCO sur l'éthique de l'intelligence artificielle (2021) et le règlement européen 2024/1689 du 13 juin 2024 relatif à l'IA digne de confiance. **(RIA – voir règles fondamentales** - synthèse en annexe 1).**

Résultant d'un travail collaboratif et consultatif, la présente charte est un socle fondateur. Elle présente des engagements qui, pris dans leur ensemble, permettent de garantir un cadre de confiance, pour minimiser les risques liés au déploiement de ces technologies, mais également dans le contexte global du Ministère de l'Intérieur conformément à ses engagements en matière de service public écoresponsable.

**** Objectifs fixés par le RIA pour une administration**

=> Garantir que l'IA utilisée respecte les droits fondamentaux, la sécurité, la non-discrimination et la protection des citoyens.

=> Prévenir les usages abusifs (surveillance de masse, évaluation sociale, manipulation des usagers).

=> Renforcer la confiance dans l'usage de l'IA dans les services publics

Cadre d'emploi des services d'IA générative

au ministère de l'Intérieur

1 – Solutions internes : le portail d'outils d'IA générative MlrAI

Afin de garantir un usage conforme aux exigences de sécurité et de confidentialité propres à un ministère régalien, la DTNUM a développé le portail interne **MlrAI** (<https://mirai.interieur.gouv.fr/>).

Exploitée sur des infrastructures maîtrisées par le ministère, cette solution met notamment à disposition :

- * un agent conversationnel (synthèse de documents, traduction, reconnaissance de caractères dans des documents scannés) ;
- * un outil de transcription et de synthèse de réunions (en présentiel ou en distanciel).

Conçu spécifiquement pour accompagner les agents dans leurs activités quotidiennes, **MlrAI** doit être privilégié par rapport à toute autre solution d'IA générative, en particulier vis-à-vis des services commerciaux ou grand public.

2 – Solutions commerciales ou grand public

L'utilisation de services externes depuis un poste professionnel est strictement encadrée. Elle est soumise à la règle selon laquelle aucune donnée personnelle (d'agent ou d'usager) ou sensible ne peut être transmise. En pratique, ces solutions ne peuvent être utilisées que si :

=> Le contenu transmis (prompt, fichier, image, etc.) ne contient aucune information sensible (confidentielle, à caractère personnel ou relative à un projet non public) ;

=> Le service propose des conditions générales d'utilisation (CGU) et licences claires et accessibles.

NB : À titre de bonne pratique, privilégier des modèles entraînés sur des corpus incluant des données françaises (ex. Mistral).

☐ **Cas Autorisé :** générer une offre d'emploi publique à partir d'une description de poste à l'aide d'un service IA grand public

✗ Exemples de cas interdits :

- * *Demander à un service IA grand public de résumer les notes d'une réunion contenant des dossiers d'usagers (données personnelles) ;*
- * *Procéder à la traduction d'échanges avec des usagers (explicitement interdit par la CNIL au MI) ;*
- * *Évaluer l'éligibilité à l'allocation/au retrait d'un droit (titre d'identité, titre de séjour...);*
- * *Analyser des preuves judiciaires ou réaliser des analyses juridiques ;*
- * *Concourir à l'exécution de missions de services répressifs.*

Donnée interne = IA interne // Donnée publique = IA grand public

3 – Solutions d’IA « métier » déployées par les services

Lorsqu’un service du ministère met en place un outil d’IA spécifique à ses besoins, les agents doivent se référer aux conditions générales d’usage définies par le service porteur et aux directives d’utilisation auxquelles ils pourront accéder et à des parcours de formation adaptés.

En cas de traitement de données à caractère personnel/sensibles, le service pilote du déploiement doit :

- => Démontrer sa conformité aux règlements (RGPD, règlement européen sur l’IA...) et lois (loi Informatique et Libertés) applicables ;
- => Offrir les garanties nécessaires quant au traitement des données ;
- => Réaliser (dans la plupart des cas) une analyse d’impact sur la protection des données et/ou une analyse d’impact sur la protection des droits fondamentaux (qui sont deux documents différents répondant à deux obligations légales différentes).

Principes éthiques, engagements et cas d’usage interdits

L’intelligence artificielle constitue une opportunité historique pour l’administration française, et plus particulièrement pour le Ministère de l’Intérieur, où elle peut contribuer à améliorer la sécurité, la gestion des crises, la simplification des démarches des citoyens et l’efficacité des services publics.

Les opportunités offertes par l’IA :

- * **Améliorer le service aux usagers et aux agents** : démarches simplifiées, délais réduits, meilleure accessibilité ;
- * **Renforcer l’efficacité interne** : automatisation des tâches répétitives et meilleure répartition des ressources (humaines, budgétaires, bâtimentaires, matérielles) ;
- * **Aider à la décision publique** : analyse prédictive pour l’anticipation des besoins de sécurité et de gestion des flux ;
- * **Lutter contre la fraude et renforcer la sécurité** : détection des fraudes documentaires et protection des infrastructures critiques ;
- * **Innover au service du bien commun** : services publics numériques modernes, inclusifs et durables.

Les enjeux :

Ils sont multiples et légitiment la rédaction de cette charte éthique pour

- * **Encadrer l’utilisation de l’IA** et permettre de définir clairement les règles et les limites d’utilisation des outils IA en assurant un cadre responsable et sécurisé ;
- * **Prévenir les risques éthiques** en identifiant les biais potentiels (discrimination).
- * **Garantir la protection et la confidentialité** des informations sensibles et des données à caractère personnel (les agents du ministère qui utilisent un système d’IA peuvent être amenés à traiter des données à caractère personnel qui concernent les agents du ministère, mais également des usagers (ex : un agent qui traite un dossier individuel en préfecture : naturalisation, titre de séjour, etc.). Les informations relatives à ces derniers peuvent être tout autant voire plus sensibles et doivent également être protégées ;

- * **Favoriser la confiance** des utilisateurs et partenaires comme des agents et des usagers par une transparence des usages (préservation du lien de confiance entre l'État et les citoyens) ;
- * **Promouvoir une culture éthique** en instaurant une culture ministérielle valorisant éthique et responsabilité dans l'utilisation des technologies émergentes ;
- * **Maintenir la responsabilité humaine** dans toute décision publique.

1 – Proportionnalité, dialogue et finalité d'intérêt général

Principes : Toute utilisation de l'IA dans le cadre ministériel doit viser la réalisation de missions d'intérêt général, au service des agents, des citoyens/usagers du service public et du bien commun.

Le développement de l'IA dans le service public doit être guidé par une démarche inclusive, associant les parties prenantes internes et externes.

Engagements :

- => Ne recourir à l'IA que lorsqu'elle apporte une valeur ajoutée claire à l'action publique ;
- => Évaluer systématiquement la pertinence de l'usage de l'IA par rapport à des alternatives humaines ou techniques existantes ;
- => Assurer que l'IA ne remplace pas indûment la relation humaine dans les situations sensibles ;
- => Associer les agents, experts métiers, ainsi que le correspondant local du délégué ministériel à la protection des données si des données personnelles sont traitées, dès les phases de conception des projets IA. Les représentants du personnel, au niveau local comme national, seront informés de la démarche et de sa progression. Ils seront consultés lorsque la mise en œuvre d'une IA impacte l'organisation du travail.
- => Favoriser les échanges interservices pour développer une culture partagée de l'éthique de l'IA ;
- => Promouvoir des démarches d'expérimentation et de retour d'expérience sur les usages de l'IA en associant les représentants du personnel.

L'IA doit être adaptée aux besoins et concertée. Elle préserve le lien humain.

✗ Exemples de cas interdits :

- * *Utiliser la reconnaissance faciale hors du cadre légal autorisé ;*
- * *Déployer une IA sans en avertir les agents et/ou les usagers qui pourraient y être exposés.*

2 – Transparence et explicabilité*

Principe : Les décisions ou recommandations produites par un système d'IA doivent être compréhensibles par les agents et les usagers concernés.

Engagements :

- => Documenter de manière claire les objectifs, les sources de données, les modalités de fonctionnement et les limites des systèmes d'IA ;
- => Mettre à la disposition des agents les outils et formations nécessaires pour utiliser les applications ;
- => Offrir aux agents et usagers des voies de recours et des explications accessibles lorsque l'IA intervient dans une décision les concernant.

Le ministère s'engage à faciliter l'explicabilité de ses systèmes IA par la documentation de leur fonctionnement, la présentation de leur rôle dans les processus décisionnels et la désignation en tant que tel de tout système en partie automatisé, ainsi qu'à faciliter la mise en œuvre effective des droits des personnes, conformément aux règles applicables en matière de protection des données à caractère personnel*.

La transparence s'exercera également dans le cadre du dialogue social par une communication nourrie à l'attention des représentants du personnel, locaux et nationaux, et concernant l'ensemble des informations nécessaires à la connaissance de tout nouvel applicatif basé sur l'IA.

Ils seront en outre avisés des incidents survenus et disposeront du bilan du déploiement des outils IA.

Toute utilisation de l'IA doit être compréhensible, explicite et justifiée

✗ Exemple de cas interdit :

** Présenter une décision comme purement humaine alors qu'elle a été partiellement ou totalement automatisée.*

3 – Équité et non-discrimination

Principe : Le développement et l'usage de l'IA doivent garantir le respect des droits et libertés fondamentaux, en particulier la vie privée, la non-discrimination, et la liberté d'expression.

Engagements :

=> Intégrer une analyse d'impact sur les droits fondamentaux (AIDF) dès la conception des projets IA quand les conditions de déclenchement sont remplies ; (Cette obligation est prévue par l'art 27 du RIA et concerne les SIA à haut risque).

=> Prévenir et corriger les biais* algorithmiques susceptibles de produire des discriminations directes ou indirectes ;

L'un des risques connus des systèmes d'intelligence artificielle est de reproduire ou de générer des discriminations. C'est pourquoi il est essentiel de mettre en œuvre des mesures visant à garantir l'équité, l'absence de discriminations et la fiabilité des solutions proposées.

Le ministère veille à ce que les productions obtenues par l'IA soient alignées sur le principe irréfragable d'égalité de traitement. Cette préoccupation se traduit également par un effort maintenu en faveur de l'accessibilité des systèmes IA déployés.

Les algorithmes doivent éviter tout biais

✗ Exemples de cas interdits :

** Exploiter des systèmes d'IA conduisant à des discriminations de toute nature ;*

** Introduire volontairement des variables sensibles dans les modèles (origine, religion, opinions, etc.). sauf si la finalité de l'IA le nécessite ex : élections*

4 – Protection des données

Principes : Minimisation des données en ne collectant que les données strictement nécessaires au fonctionnement de l'IA et transparence de l'information pour les utilisateurs et usagers.

Engagements :

=> Garantir la protection des données à caractère personnel conformément au RGPD*, à la loi informatique et libertés (LIL)*, aux recommandations de la CNIL et à la politique ministérielle de conformité des données, avec réalisation d'études d'impact soumises au délégué ministériel (DMPD) ;

=> Assurer la traçabilité des usages des données dans un SIA ;

=> Garantir l'exercice des droits (accès, rectification, portabilité, opposition ou effacement) pour les usagers et les agents.

Le ministère fait de la protection des données, y compris à caractère personnel, et du respect de la vie privée des valeurs **intangibles**. Cette volonté se traduit par des mesures rigoureuses de protection de l'intégrité des données et de contrôle strict des protocoles d'accès pour toutes les données et en particulier celles de ses agents. (Strict respect de la politique ministérielle de conformité des données personnelles (PCDP-MI) et de la note du délégué ministériel à la protection des données relative à l'IA).

Le respect du RGPD et des règles de cyber sécurité doit être strict et absolu

✗ Exemples de cas interdits :

** Utiliser un outil grand public pour traiter des informations classifiées, métier, confidentielles, à caractère personnel ou sensibles ;*

** Recourir à des systèmes non sécurisés (stocker, exporter des données etc) ;*

** Utiliser des données dans un cadre non prévu ou non conforme à l'éthique ;*

** Entraîner une IA avec des données collectées pour une autre finalité, sans s'assurer auprès du DMPD de la légalité de cette nouvelle finalité ;*

** Recourir à une IA pour un traitement de données à caractère personnel autorisé par un acte réglementaire, sans s'assurer auprès du DMPD de la légalité de cet usage ;*

**** Sont notamment répertoriés par le règlement européen sur l'intelligence artificielle comme « système d'IA à haut risque » les systèmes utilisés dans les domaines de la biométrie¹, de la répression², ou encore de la migration, de l'asile et de la gestion des contrôles aux frontières³. Ces systèmes d'IA doivent être autorisés par des dispositions législatives ou réglementaires nationales spécifiques et doivent faire l'objet de garanties renforcées (étude d'impact).**

1 SIA d'identification biométrique à distance, SIA destinés à être utilisés à des fins de catégorisation biométrique, SIA destinés à être utilisés pour la reconnaissance des émotions.

2 SIA destinés à être utilisés pour évaluer le risque qu'une personne physique devienne la victime d'infractions pénales, SIA destinés à être utilisés en tant que polygraphes ou outils similaires, SIA destinés à être utilisés pour évaluer la fiabilité des preuves au cours d'enquêtes ou de poursuites pénales, SIA destinés à être utilisés pour évaluer le risque qu'une personne physique commette une infraction ou récidive, SIA destinés à être utilisés pour le profilage de personnes physiques.

3 SIA destinés à être utilisés en tant que polygraphes et outils similaires, SIA destinés à être utilisés pour évaluer un risque posé par une personne physique qui a l'intention d'entrer ou qui est entrée sur le territoire d'un État membre, SIA destinés à être utilisés pour aider les autorités publiques compétentes à procéder à l'examen des demandes d'asile, de visas et de titres de séjour et des plaintes connexes, SIA destinés à être utilisés aux fins de la détection, de la reconnaissance ou de l'identification des personnes physiques.

5 – Responsabilité humaine et redevabilité*

Principe : L'administration s'assure de la qualité et de la conformité des décisions prises avec l'appui de systèmes d'IA.

Engagements :

- => Identifier formellement les responsables de chaque système d'IA (conception, déploiement, supervision) ;
- => Ne jamais déléguer à un système d'IA la prise de décision finale sans supervision humaine appropriée ;
- => Mettre en place des mécanismes d'audit, de contrôle et de recours pour toutes les applications ;
- => Servir l'humain et les droits fondamentaux, sans restreindre ou dévoyer l'autonomie humaine ;
- => Servir les intérêts individuels légitimes des agents et usagers du Ministère de l'Intérieur, dans la stricte limite des missions de l'institution et de ses obligations en tant qu'employeur.

La décision finale appartient toujours à un agent public

✗ Exemples de cas interdits :

- * Laisser une IA délivrer automatiquement un titre, un refus ou un droit sans vérification humaine ;
- * Se décharger de toute responsabilité en invoquant la décision algorithmique.

Pour garantir une IA respectueuse de la liberté et de l'autonomie, les systèmes IA ne doivent être utilisés que pour éclairer la décision, non pour l'automatiser sans contrôle. Le ministère conçoit ses systèmes IA **pour garantir la primauté humaine**, fournir des outils d'interaction et de recours, et organiser les mécanismes de sécurité et de conformité légale utiles. Ainsi, aucune décision susceptible de produire des effets juridiques à l'égard des personnes ou les affectant de manière significative ne doit pouvoir être prise sur la seule base des systèmes d'IA.

6 – Sécurité et robustesse

Principe : Les systèmes d'IA doivent être techniquement fiables, résilients aux cyberattaques, et faire l'objet de vérifications régulières.

Engagements :

- => Appliquer les règles de cyber sécurité en vigueur dans l'administration pour tous les systèmes IA en production ;
- => Évaluer les risques de dysfonctionnement ou de détournement de l'IA dès la conception ;
- => Prévoir des dispositifs de supervision et de retrait en cas d'usage non conforme ou de dégradation des performances ;
- => Appliquer la procédure prévue dans la politique ministérielle PCDP-MI en cas de violation des données métiers ou à caractère personnel ;
- => Renforcer le contrôle des accès aux services proposés et limiter leurs usages dans le cadre des droits adaptés aux activités, besoins et obligations des personnes concernées.

La fiabilité et la résistance aux attaques des IA sont fondamentaux

✗ Exemples de cas interdits :

- * Utiliser une IA sans vérifier l'intégrité de son algorithme
- * Dissimuler une violation de données (ex : la destruction, la perte, l'altération ou la divulgation de données)

Le ministère fait de l'intégrité technique (sécurité et robustesse) de ses SIA le **prérequis de l'IA de confiance** qu'il entend déployer. Cela implique de concevoir des systèmes qui minimisent les risques, soient résilients et résistent aux cyberattaques. Ils seront en outre en capacité de reproduire des comportements prévisibles dans des conditions données pour garantir le respect de la vie privée des usagers tout au long du cycle de vie des solutions.

7 – Soutenabilité et sobriété numérique

Principe : L'usage de l'IA doit s'inscrire dans une démarche écoresponsable et respecter les objectifs de sobriété numérique de l'État.

Engagements :

- => Prendre en compte l'empreinte environnementale des SIA dans les choix techniques ;
- => Favoriser les modèles et solutions sobres en ressources, notamment en phase d'entraînement ;
- => Encourager la mutualisation des ressources numériques au sein du ministère et entre administrations.

Les IA utilisées au MI doivent être respectueuses de leur environnement

Le ministère s'engage dans une approche maîtrisée du développement de l'IA, attentive à son impact sur les parties prenantes. Conscient des enjeux sociaux et environnementaux du numérique, le Ministère de l'Intérieur a adopté une démarche globale pour un numérique responsable et durable pour atteindre ses objectifs en matière de réduction des émissions carbone.

Dispositions diverses

Diffusion de la charte

La diffusion de la charte sera organisée pour assurer sa portée et sa connaissance effective :

- * Communication directe (envoi à chaque agent, réunion d'information, support numérique, affichage) ;
- * Annexion au kit d'accueil pour tous les nouveaux arrivants.

Amélioration continue

Les outils comportant de l'IA doivent être audités et corrigés régulièrement.

✗ Exemples de cas interdits :

- * Continuer à utiliser un algorithme malgré des résultats faussés signalés ;
- * Ignorer des audits révélant des biais ou des failles.

Clause de révision de la charte

Le Ministère de l'Intérieur s'engage à réviser cette charte **au minimum tous les ans** afin de tenir compte :

- Des évolutions sociétales ;
- Des évolutions juridiques à l'échelle européenne et nationale ;
- Des évolutions technologiques rapides dans le domaine de l'intelligence artificielle ;
- Des retours d'expérience liés à l'usage des outils dans l'administration ;
- Des résultats des audits et des mécanismes de correction mis en place.

Cette révision sera conduite, sur la base d'éléments de bilan sur le déploiement, l'utilisation et l'impact de l'IA au sein du Ministère sur les différents enjeux abordés dans cette charte, en concertation avec :

- Les représentants des personnels ;
- Les autorités compétentes en matière d'éthique, de protection des données, RH et de sécurité numérique ;
- Les experts techniques et juridiques.

Chaque nouvelle version de la charte sera communiquée à l'ensemble des agents et fera l'objet d'une formation adaptée, afin d'expliquer les évolutions et de maintenir une compréhension partagée et une application uniforme des règles établies.

Formation et accompagnement

Les agents doivent être sensibilisés, formés (formation initiale et continue) et accompagnés dans un environnement utilisant l'IA ou pour faire usage directement d'un outil doté d'intelligence artificielle.

Les encadrants seront vigilants sur la formation des agents et particulièrement à la prise de poste si ce dernier requiert l'utilisation de l'IA.

✗ Exemples de cas interdits :

- * *Imposer un outil d'IA dans un environnement de travail sans informer les agents ;*
- * *Détourner un outil d'IA de son usage prévu.*

Usage des IA génératives

Seuls les outils développés, validés et sécurisés par l'administration peuvent être utilisés dans le cadre d'un processus métier.

L'accès aux solutions commerciales ou grand public depuis un terminal professionnel est notamment conditionné par l'évaluation de leur conformité aux standards requis par le Centre de cyber sécurité du ministère de l'Intérieur (C2MI) du SHFD. Il est limité aux usages ne mettant pas en œuvre des informations sensibles ou des données à caractère personnel (par exemple : génération d'une image d'illustration pour un document de communication).

✗ Exemples de cas interdits :

- * *Utiliser une IA générative grand public pour traiter des dossiers, des informations à caractère personnel ou tout travail administratif ;*
- * *Saisir dans un outil externe des informations relatives à la sécurité, aux usagers, aux fonctionnaires ou aux infrastructures publiques.*

Responsabilité de l'administration vis-à-vis de ses agents

Le Ministère de l'Intérieur s'engage à :

- Viser la **souveraineté numérique** en privilégiant autant que possible des solutions internes, souveraines ou validées au niveau national ;

- Veiller à alimenter le dialogue social sur l'IA au niveau local comme national ;
- Diffuser largement la charte et informer les agents sur la charte et sa portée ;
- Offrir une formation adaptée tant initiale que continue à ses agents sur l'IA et ces applications ;
- Promouvoir le développement et l'exploitation d'une IA « de confiance » qui minimise tout risque de dérive d'un système partiellement automatisé.

Engagements des agents vis-à-vis de l'administration et des usagers

Les agents s'engagent à :

- Respecter la transparence envers les usagers ;
- Préserver le contrôle humain dans toutes les décisions ;
- Protéger les données confidentielles et en particulier les données nominatives ;
- Garantir l'équité et signaler tout biais détecté ;
- Assurer une vigilance active en cas d'anomalie ;
- Contribuer à l'amélioration continue ;
- Se former régulièrement ;
- Respecter l'intérêt général ;
- N'utiliser que les outils d'IA autorisés par le droit européen et national, ainsi que validés par le ministère pour leurs missions comportant des données à caractère personnel ou des informations sensibles.

Engagement final

Le ministère affirme sa volonté de faire de l'intelligence artificielle un outil au service de l'intérêt général, conforme aux valeurs de la République et aux principes fondamentaux du service public.

L'ensemble des agents, décideurs, partenaires et prestataires impliqués dans la conception, le développement, l'acquisition, le déploiement ou l'usage de systèmes d'intelligence artificielle s'engagent à respecter les principes énoncés dans ce document.

Cet engagement collectif vise à garantir une utilisation responsable, éthique, transparente et maîtrisée de l'IA, au bénéfice des citoyens et dans le respect des droits fondamentaux.

Cette charte a vocation à être régulièrement mise à jour, à la lumière des évolutions technologiques, des retours d'expérience et des débats publics sur les usages de l'intelligence artificielle.

L'intelligence artificielle est un outil puissant au service d'une administration plus moderne, plus proche et plus juste. Son usage éthique et responsable est une condition indispensable pour préserver la confiance entre l'État, ses agents et les citoyens.

Cette charte constitue un engagement réciproque : le Ministère de l'Intérieur protège ses agents et œuvre à la robustesse, la sécurité et la souveraineté des outils mis à leur disposition, tandis que les agents s'engagent à utiliser l'IA au service de l'intérêt général et dans le respect des règles établies et des droits des usagers.

Ressources internes : outils, procédures et contacts

=> Le portail d'outils IA « MIRA » : <https://mirai.interieur.gouv.fr/>

=> Forum « IAgora » (accessible librement par simple recherche sur Tchap) : espace communautaire dédié à l'intelligence artificielle au sein du ministère, administré par la DMIA ;

=> Note du délégué ministériel à la protection des données sur l'application à l'IA des règles sur les données personnelles ;

<http://sq.minint.fr/images/RGPD/Politique-ministerielle-v1-3-vf.pdf>

=> Politique de conformité des données personnelles du ministère de l'intérieur :

<http://sg.minint.fr/index.php/rgpd/pcdp-mi>

La direction de la Transformation numérique du ministère de l'Intérieur coordonne la mise en œuvre de la feuille de route ministérielle sur l'intelligence artificielle.

<http://dnum.minint.fr/index.php/actualites/4836-feuille-de-route-ministerielle-sur-l-intelligence-artificielle-retour-sur-la-visioconference-du-jeudi-03-juillet-2025>

Pour toute information complémentaire sur les actions et dispositifs prévus dans ce cadre, contactez la délégation ministérielle à l'intelligence artificielle (DMIA):

dmia@interieur.gouv.fr

Glossaire

- **IA (Intelligence artificielle)** : ensemble de techniques permettant à une machine de réaliser des tâches qui nécessitent normalement l'intelligence humaine (compréhension du langage, reconnaissance d'images, etc.).
- **Explicabilité** : capacité à rendre compréhensible pour les utilisateurs les mécanismes de fonctionnement, les décisions et les résultats produits par une IA. Ainsi l'IA donne un résultat et les raisons qui expliquent le résultat obtenu.
- **Algorithme** : suite d'instructions permettant de résoudre un problème ou d'effectuer une opération.
- **Apprentissage automatique (Machine Learning)** : méthode d'IA qui permet aux algorithmes d'apprendre et de s'améliorer automatiquement à partir de données.
- **Apprentissage profond (Deep Learning)** : sous-domaine du Machine Learning utilisant des réseaux de neurones complexes, souvent pour la reconnaissance d'images, de sons ou de textes.
- **Biais algorithmique** : distorsion ou discrimination introduite dans les résultats produits par un système automatisé en raison de données incomplètes, déséquilibrées ou biaisées.
- **Donnée à caractère personnel** : toute information relative à une personne physique identifiée ou identifiable (nom, adresse, biométrie, Numéro de sécurité sociale, etc.).
- **RGPD (Règlement général sur la protection des données)** : règlement européen fixant les règles de protection des données à caractère personnel.

- **Loi informatique et libertés (LIL)** : loi fixant les règles de protection des données à caractère personnel pour les traitements relevant du RGPD, de la directive police-justice et pour les traitements intéressant la sûreté de l'Etat et la défense.
- **RIA** : règlement européen sur l'intelligence artificielle.
- **Boîte noire algorithmique** : système dont le fonctionnement interne n'est pas compréhensible ou accessible pour l'utilisateur.
- **IA générative** : type d'IA capable de produire du contenu nouveau (texte, image, vidéo, code, etc.) à partir de données d'entraînement.
- **Souveraineté numérique** : capacité d'un État à garder le contrôle de ses infrastructures numériques, de ses données et de ses choix technologiques.
- **DMPD** : délégué ministériel à la protection des données, désigné pour conseiller les services et contrôler la conformité des traitements des données à caractère personnel avec la législation, notamment le RGPD et la loi informatique et libertés.
- **PCDP-MI** : politique de conformité des données personnelles du ministère de l'Intérieur
<http://sg.minint.fr/index.php/rgpd/pcdp-mi>
- **Redevabilité** : désigne l'obligation des concepteurs et utilisateurs de systèmes d'IA d'assumer la responsabilité de leurs choix, de leurs actions et des impacts de ces technologies sur l'individu, la société et l'environnement.

Synthèse du règlement européen sur l'intelligence artificielle du 13 juin 2024 (RIA)

☐ **Objectif pour les administrations**

- * Garantir que l'IA utilisée respecte les droits fondamentaux, la sécurité, la non-discrimination et la protection des citoyens.
- * Prévenir les usages abusifs (surveillance de masse, évaluation sociale, manipulation des usagers).
- * Renforcer la confiance dans l'usage de l'IA dans les services publics.

☐ **Ce que le RIA change pour une administration**

1. Usages interdits (à éviter absolument)

- * Reconnaissance biométrique en temps réel dans l'espace public (sauf exceptions limitées : terrorisme, recherche de victimes).
- * Évaluation social des individus par l'État ou des entreprises.
- * IA manipulatrice exploitant les vulnérabilités des personnes (mineurs, personnes âgées, handicap).

2. Usages "à haut risque"

Certaines applications dans le secteur public sont classées hauts risques :

- * Recrutement et gestion du personnel public.
- * Attribution de prestations sociales, aides, subventions.
- * Éducation et examens (concours, certifications).
- * Justice, sécurité, application de la loi.

☐ *Ces systèmes doivent respecter des obligations strictes :*

- * Analyse d'impact et gestion des risques.
- * Données d'entraînement fiables et non biaisées.
- * Documentation claire (traçabilité, justification des décisions).
- * Supervision humaine (décision finale par un agent).
- * Robustesse et cyber sécurité.

3. Usages à risque limité

Exemples : chabots pour renseigner le public, outils de rédaction automatique de documents.

- ☐ Obligation principale : informer clairement l'utilisateur qu'il interagit avec une IA ou lit un contenu généré par IA.

☐ **Gouvernance interne pour une administration**

- * Nommer un référent IA (ou s'appuyer sur l'autorité nationale compétente).
- * Mettre en place un registre interne des systèmes IA utilisés (cartographie des outils).
- * Intégrer des procédures de contrôle éthique et juridique avant tout déploiement.
- * Prévoir une formation des agents sur les risques, limites et obligations de transparence.
- * Suivre les évolutions réglementaires via l'Office européen de l'IA et les autorités nationales.

□ **Sanctions en cas de non-respect**

=> Amendes lourdes (jusqu'à 6 % du chiffre d'affaire mondial pour les entreprises ou plusieurs millions d'euros pour les administrations et organismes publics).

=> Perte de confiance et contentieux liés aux droits fondamentaux.

□ **En résumé :**

Pour une administration, le RIA impose prudence, transparence et supervision humaine. L'usage de l'IA doit être éthique, traçable et contrôlé, surtout lorsqu'il touche aux droits sociaux, à la justice, à l'éducation ou à la sécurité.