

# Développement des systèmes d'IA : les recommandations de la CNIL pour respecter le RGPD

08 avril 2024

---

*La CNIL a publié ses premières recommandations sur l'application du RGPD au développement des systèmes d'**intelligence artificielle** pour aider les professionnels à concilier innovation et respect des droits des personnes. Voici ce qu'il faut en retenir.*

Les concepteurs et développeurs de systèmes d'**intelligence artificielle** font souvent remonter à la CNIL que l'application du RGPD leur pose des difficultés, notamment pour l'entraînement des modèles.

L'idée reçue selon laquelle le RGPD empêcherait l'innovation en intelligence artificielle en Europe est fausse. En revanche, il faut avoir conscience que les bases d'entraînement comprennent parfois des « données personnelles », des informations sur des personnes réelles. L'utilisation de ces données fait courir des risques aux personnes, qu'il faut prendre en compte, afin de développer des systèmes d'IA dans des conditions qui respectent les droits et libertés des personnes, et notamment leur droit à la vie privée.

## Périmètre des recommandations

Quels sont les systèmes d'IA concernés ?

Ces recommandations concernent le développement de **systèmes d'IA impliquant un traitement de données personnelles** (pour plus d'informations sur le cadre juridique, voir la [fiche n°1](#)). En effet, l'entraînement des systèmes d'IA nécessitent régulièrement l'utilisation d'importants volumes d'informations sur des personnes physiques, qu'on nomme « données personnelles ».

Sont concernés :

- Les systèmes fondés sur l'**apprentissage automatique** (*machine learning*) ;
- Les systèmes dont l'usage opérationnel est défini dès la phase de développement et les systèmes à usage général qui pourront être utilisés pour nourrir différentes applications (« *general purpose AI* »).
- Les systèmes dont l'apprentissage est réalisé « une fois pour toutes » ou de façon continue, par exemple en utilisant des données d'utilisation pour son amélioration.

## Quelles sont les étapes concernées ?

Ces recommandations **concernent la phase de développement de systèmes d'IA, et non celle de déploiement.**

La phase de développement comprend toutes les étapes préalables au déploiement du système d'IA à savoir : la conception du système, la constitution de la base de données et l'apprentissage

## Comment ces recommandations s'articulent-elles avec le règlement européen sur l'IA ?

Les recommandations formulées prennent en considération le nouveau règlement européen sur l'intelligence artificielle. En effet, **lorsque des données personnelles sont utilisées** pour le développement d'un système d'IA, **le RGPD et le règlement sur l'IA s'appliquent tous les deux.** Les recommandations de la CNIL ont donc été élaborées pour compléter ces dernières de manière cohérente sur le volet relatif à la protection des données.

► Pour plus d'informations, voir la [fiche n° 0](#)

## 1ère étape : Définir un objectif (finalité) pour le système d'IA

### Le principe

Un système d'IA reposant sur l'exploitation de données personnelles doit être développé avec une « finalité », c'est-à-dire un objectif bien défini.

Cela permet de cadrer et de limiter les données personnelles que l'on va pouvoir utiliser pour l'entraînement, afin de ne pas stocker et traiter des données inutiles.

Cet objectif doit être déterminé, soit établi dès la définition du projet. Il doit également être explicite, autrement dit connu et compréhensible. Il doit enfin être légitime, c'est-à-dire compatible avec les missions de l'organisme.

Il est parfois objecté que l'exigence de définir une finalité est incompatible avec l'entraînement d'IA, qui peut développer des caractéristiques non anticipées. La CNIL estime qu'il n'en est rien et que l'exigence de définition d'une finalité doit être adaptée au contexte de l'IA, sans disparaître pour autant, comme le montre les exemples qui suivent.

### En pratique

Il existe trois types de situations.

Vous savez clairement quel sera l'usage opérationnel de votre système d'IA

Dans ce cas, cet objectif sera la finalité de la phase de développement comme de la phase de déploiement et d'utilisation.

### Exemple :

Un organisme constitue une base de données composée de photos de rames de trains en service – c'est-à-dire avec des personnes présentes – afin d'entraîner un

**algorithme** pour mesurer l'affluence et la fréquentation des trains à quai dans les gares. La finalité en phase de développement est déterminée, explicite et légitime au regard de l'usage opérationnel identifié.

Cela est toutefois plus complexe lorsque vous développez **un système d'IA à usage général** qui pourra être utilisé dans divers contextes et applications ou lorsque **votre système est développé à des fins de recherche scientifique**.

Pour les systèmes d'IA à usage général

### Exemple :

Un organisme peut constituer une base de données pour l'entraînement d'un modèle de classification d'images (personnes, véhicules, aliments, etc.) et le rendre publiquement accessible, sans qu'aucun usage opérationnel spécifique ne soit prévu lors du développement du modèle.

Vous ne pouvez pas définir la finalité de manière trop générale comme, par exemple, « le développement et amélioration d'un système d'IA ». Il vous faudra être plus précis et faire référence :

- **au « type » de système développé**, comme, par exemple, le développement d'un **modèle de langage** de grande taille, d'un système de vision par ordinateur (*computer vision*) ou encore d'un système d'IA générative d'images, de vidéos, de sons, de code informatique, etc.
- **aux fonctionnalités et capacités techniquement envisageables**.

### Bonne pratique :

Vous pouvez donner encore plus de précisions quant à l'objectif poursuivi, par exemple en déterminant :

- les capacités prévisibles les plus à risque ;
- les fonctionnalités exclues par conception ;
- les conditions d'utilisation du système d'IA : les cas d'usage connus de la solution ou encore les modalités d'utilisation (diffusion du modèle en *open source*, commercialisation, mise à disposition en **SaaS** ou par API, etc.).

Pour les systèmes d'IA développés à des fins de recherche scientifique

### Exemple :

Pourrait être considéré comme poursuivant des fins de recherche scientifique le développement d'un système d'IA pour une preuve de concept destinée à démontrer la robustesse d'un **apprentissage automatique** nécessitant moins de données d'entraînement, dans une démarche scientifique documentée ayant vocation à faire l'objet d'une publication.

Vous pouvez définir un objectif moins détaillé, compte tenu des difficultés à le définir précisément dès le début de vos travaux. Vous pouvez alors fournir des informations complémentaires pour préciser cet objectif à mesure que votre projet progresse.

- Pour plus d'informations, voir la [fiche n° 2](#)

## 2e étape : Déterminer vos responsabilités

### Le principe

Si vous utilisez des données personnelles pour le développement de systèmes d'IA, vous devez déterminer votre responsabilité au sens du RGPD. Vous pouvez être :

- **responsable de traitement (RT)** : vous déterminez les objectifs et les moyens, c'est-à-dire lorsque vous décidez du « pourquoi » et du « comment » de l'utilisation de données personnelles. Si un ou plusieurs autres organismes décident avec vous de ces éléments, vous serez responsables conjoints du traitement et devrez définir vos obligations respectives (par exemple, par le biais d'un contrat).
- **sous-traitant (ST)** : vous traitez des données pour le compte d'un donneur d'ordre qui est le « responsable du traitement ». Dans ce cas, ce dernier doit s'assurer que vous respectez le RGPD et que vous ne traitez les données que sur ses instructions : la loi prévoit alors la conclusion d'un [contrat de sous-traitance](#).

### En pratique

Le règlement européen sur l'IA définit plusieurs rôles :

- le **fournisseur de système d'IA** qui développe ou fait développer un système et qui le met sur le marché ou le met en service sous son propre nom ou sa propre marque, à titre payant ou gratuit ;
- les **importateurs, distributeurs et les utilisateurs (également appelés dépoyeurs)** de ces systèmes.

**Votre degré de responsabilité dépend d'une analyse au cas par cas.** Par exemple :

- Si vous êtes un fournisseur à l'initiative du développement d'un système d'IA et que vous constituez la base de données d'apprentissage à partir de données que vous avez sélectionnées pour votre propre compte, **vous pouvez être qualifié de responsable de traitement.**
- Si vous constituez la base de données d'apprentissage d'un système d'IA avec d'autres responsables de traitement pour un objectif que vous avez défini ensemble, **vous pouvez être qualifiés de responsables conjoints du traitement.**
- Si vous êtes un fournisseur de système d'IA, **vous pouvez être sous-traitant si vous développez un système pour le compte d'un de vos clients.** Le client sera responsable de traitement s'il détermine l'objectif mais aussi les moyens, les techniques à utiliser. S'il ne vous donne qu'un objectif à atteindre et que c'est vous qui concevez le système d'IA, vous êtes **responsable de traitement.**
- Si vous êtes un fournisseur de système d'IA vous pouvez faire appel à un prestataire pour collecter et traiter les données selon vos instructions. **Le prestataire sera votre sous-traitant.** C'est le cas par exemple du prestataire qui doit constituer une base de données d'apprentissage pour un fournisseur de système d'IA qui lui indique précisément comment elle doit être élaborée.

► Pour plus d'informations, voir la [fiche n°3](#)

#### Pour la suite :

- Si vous êtes responsable de traitement, toutes les étapes suivantes vous concernent directement, c'est vous qui êtes tenus d'en assurer le respect.
- Si vous êtes sous-traitant, vos principales obligations sont les suivantes :

- Vous assurer qu'un contrat de sous-traitance de données personnelles a été conclu et qu'il est conforme à la réglementation ;
  - Respecter strictement les instructions du responsable de traitement et ne pas utiliser les données personnelles pour autre chose ;
  - Assurer rigoureusement la sécurité des données que vous traitez ;
  - Évaluer à votre niveau le respect du RGPD (cf. les étapes suivantes) et alerter le responsable de traitement s'il vous semble qu'il y a un problème.
- 

## 3e étape : Définir la « base légale » qui vous autorise à traiter des données personnelles

### Le principe

Le développement de systèmes d'IA contenant des données personnelles devra disposer d'une [base légale](#) qui vous autorise à traiter ces données. Le RGPD liste 6 bases légales possibles : le consentement, le respect d'une obligation légale, l'exécution d'un contrat, l'exécution d'une mission d'intérêt public, la sauvegarde des intérêts vitaux, la poursuite d'un intérêt légitime.

Selon la **base légale** retenue, vos obligations et les droits des personnes pourront varier, c'est pour cela qu'il est important de la déterminer en amont et de l'indiquer dans la politique de confidentialité des données.

### En pratique

Vous devez vous interroger sur **la base légale la plus adaptée à votre situation**.

Si vous collectez les données directement auprès des personnes et qu'elles sont libres d'accepter ou de refuser sans subir de préjudice (tel que le fait de renoncer au service), le consentement est souvent la base légale la plus appropriée. Selon la loi, il doit **être libre, spécifique, éclairé et univoque**.

Recueillir le consentement est cependant souvent impossible en pratique. Par exemple, lorsque vous collectez des données accessibles en ligne ou réutilisez une base de données ouverte (*open source*), sans contact direct avec les personnes concernées, d'autres bases légales seront, généralement, plus adaptées :

- **Les acteurs privés** devront analyser s'ils respectent les conditions pour se fonder sur l'intérêt légitime. Ils doivent pour cela justifier de trois conditions :
  - **L'intérêt poursuivi est légitime** c'est-à-dire légal, défini de manière précise et réel ;
  - il faut pouvoir établir que les données personnelles sont vraiment nécessaires à l'entraînement du système, parce qu'il n'est pas possible de n'utiliser que des données ne se rapportant pas à des personnes physiques ou des données anonymisées. ;
  - l'utilisation de ces données personnelles ne doit pas porter une « atteinte disproportionnée » à la vie privée des personnes. Cela s'apprécie au cas par cas, en fonction de ce que révèlent les données utilisées, qui peut être plus ou moins privé ou sensible, et de ce qui est fait des données. ;

*À noter : une fiche pratique spécifique à la base légale de l'intérêt légitime sera prochainement publiée.*

- **Les acteurs publics** doivent vérifier si le traitement s'inscrit dans leur mission d'intérêt public telle que prévue par un texte (par exemple une loi, un décret, etc.) et s'il y contribue de manière pertinente

et appropriée.

**Exemple :** le pôle d'expertise de la régulation numérique (PEReN) est autorisé sur ce fondement à réutiliser des données publiquement accessibles pour réaliser des expérimentations ayant notamment pour objet de concevoir des outils techniques destinés à la régulation des opérateurs de plateformes en ligne.

**Les bases légales du contrat et de l'obligation légale peuvent être plus exceptionnellement mobilisées**, si vous démontrez en quoi votre traitement est nécessaire pour répondre à l'exécution du contrat ou de mesures précontractuelles ou à une obligation légale (suffisamment précise) à laquelle vous êtes soumis.

► Pour plus d'informations, voir la [fiche n° 4](#).

---

## 4e étape : Vérifier si je peux réutiliser certaines données personnelles

### Le principe

Si vous envisagez de réutiliser une base de données à caractère personnel, il faut s'assurer que c'est légal. Cela dépend des modalités de collecte et de la source des données en cause. **Vous devez, en tant que responsable de traitement (voir la partie « déterminer vos responsabilités »), effectuer certaines vérifications complémentaires afin de garantir que cette utilisation est légale.**

### En pratique

Les règles vont dépendre des situations.

Le fournisseur réutilise des données qu'il a lui-même déjà collectées

Vous pouvez vouloir réutiliser les données que vous avez initialement collectées pour un autre objectif. Dans ce cas, si vous n'aviez pas prévu et informé les personnes concernées de cette réutilisation, vous devez vérifier que ce nouvel usage est **compatible** avec l'objectif initial, sauf si vous êtes autorisé par les personnes concernées (elles ont consenti) ou par un texte (par exemple une loi, un décret etc.).

Vous devez effectuer ce qu'on appelle un « test de compatibilité », qui doit prendre en compte :

- l'existence d'un lien entre l'objectif initial et celui de constitution de base de données pour l'apprentissage d'un système d'IA ;
- le contexte dans lequel les données personnelles ont été collectées ;
- le type et la nature des données ;
- les éventuelles conséquences pour les personnes concernées ;
- l'existence de garanties appropriées (par exemple, la pseudonymisation des données).

À noter : **si vous souhaitez réutiliser des données dans un objectif de production de statistiques ou de recherche scientifique**, le traitement est présumé compatible avec l'objectif initial. **Aucun test de compatibilité n'est donc nécessaire dans ce cas.**

Le fournisseur réutilise des données publiquement accessibles (*open source*)

Dans ce cas, vous devez vous assurer que vous n'êtes pas en train de réutiliser une base de données dont la constitution était manifestement illicite (par exemple, provenant d'une fuite de données). **Une analyse au cas par cas doit être effectuée.**

La CNIL recommande aux réutilisateurs de vérifier et de documenter (par exemple, dans l'analyse d'impact sur la protection des données) les éléments suivants :

- la description de la base de données mentionne leur source ;
- la constitution ou la diffusion de la base de données **ne résulte pas manifestement d'un crime ou d'un délit ou a fait l'objet d'une condamnation ou d'une sanction publique** de la part d'une autorité compétente qui a impliqué une suppression ou une interdiction d'exploitation ;
- **il n'y a pas de doutes flagrants sur le fait que la base de données est licite** en s'assurant en particulier que les conditions de collecte des données soient suffisamment documentées ;
- la base de données ne contient **pas de données sensibles** (données de santé ou révélant des opinions politiques par exemple) **ou de données d'infraction** ou, si elle en contient, il est recommandé de mener des vérifications supplémentaires pour s'assurer que ce traitement est licite.

L'organisme qui a mis en ligne la base de données est censé s'être assuré que cette publication respectait le RGPD, et en est responsable. En revanche, vous n'avez pas à vérifier que les organismes qui ont constitué et diffusé la base de données aient respecté toutes les obligations prévues par le RGPD : la CNIL estime que les quatre vérifications mentionnées ci-dessus suffisent généralement à permettre la réutilisation de la base pour l'entraînement d'un système d'IA, à condition de respecter les autres recommandations de la CNIL. Si vous recevez des informations, notamment de personnes dont les données sont contenues dans la base, qui mettent en lumière des problèmes de licéité de la base de données utilisées, vous devrez investiguez davantage.

Le fournisseur réutilise des données acquises auprès d'un tiers (courtiers en données ou *data brokers*, etc.)

Pour le tiers qui partage des données personnelles, parfois contre rémunération, il existe deux types de situations.

**Soit le tiers a collecté les données dans l'objectif de constituer une base de données pour l'apprentissage de système d'IA.** Il doit s'assurer de la conformité du traitement de transmission des données au regard du RGPD (définition d'un objectif explicite et légitime, exigence d'une **base légale**, information des personnes et gestion de l'exercice de leurs droits, etc.).

**Soit le tiers n'a pas initialement collecté les données pour cet objectif.** Il doit alors s'assurer que la transmission de ces données poursuit un objectif compatible avec celui ayant justifié leur collecte. **Il devra donc réaliser le « test de compatibilité » présenté plus haut.**

Le réutilisateur des données a, quant à lui, plusieurs obligations :

- Il doit s'assurer qu'il n'est pas en train de réutiliser une base de données manifestement illicite en faisant les mêmes vérifications que celles énoncées dans la partie ci-dessus. La conclusion d'un accord entre le détenteur initial des données et le réutilisateur est recommandée afin de faciliter ces vérifications.
- En plus de ces vérifications, il doit s'assurer de sa propre conformité au RGPD dans le traitement de ces données.

► Pour plus d'informations, voir la [fiche n° 4](#).



## 5e étape : minimiser les données personnelles que j'utilise

### Le principe

Les données personnelles collectées et utilisées doivent être **adéquates, pertinentes et limitées à ce qui est nécessaire** au regard de l'objectif défini : c'est le principe de [minimisation des données](#). Vous devez respecter ce principe et l'appliquer de manière rigoureuse lorsque les données traitées sont sensibles (données concernant la santé, données relatives à la vie sexuelle aux opinions religieuses ou politiques, etc.).

### En pratique

#### La méthode à employer

Vous devez privilégier la technique permettant d'atteindre le résultat recherché (ou du même ordre) **en utilisant le moins de données personnelles possible**. En particulier, le recours à l'apprentissage profond ne doit donc pas être systématique.

Le choix du protocole d'apprentissage utilisé peut, par exemple, permettre de limiter l'accès aux données aux seules personnes habilitées, ou encore de ne donner accès qu'à des données chiffrées.

#### La sélection des données strictement nécessaires

Le principe de **minimisation** n'interdit pas d'entraîner un **algorithme** avec des volumes très importants de données, mais implique :

- d'avoir une réflexion en amont afin de recourir aux seules données personnelles utiles au développement du système ; et
- à mettre, par la suite, en œuvre les moyens techniques pour ne collecter que celles-ci.

#### La validité des choix de conception

Afin de valider les choix de conception, il est recommandé à titre de bonne pratique de :

- **mener une étude pilote**, c'est-à-dire réaliser une expérimentation à petite échelle. Des données fictives, synthétiques, anonymisées peuvent être utilisées à cette fin ;
- **interroger un comité éthique** (ou un « référent éthique »). Ce comité doit garantir que les enjeux en matière d'éthique et de protection des droits et libertés des personnes sont bien pris en compte. Il peut ainsi formuler des avis sur tout ou partie des projets, outils, produits, etc. de l'organisme susceptibles de poser des problématiques éthiques.

#### L'organisation de la collecte

Vous devez vous assurer que les données collectées sont pertinentes compte tenu des objectifs poursuivis. Plusieurs étapes sont fortement recommandées :

- **Le nettoyage des données** : cette étape vous permet de constituer une base d'apprentissage de qualité et ainsi renforcer l'intégrité et la pertinence des données en réduisant les incohérences, et ainsi



que le coût de l'apprentissage.

- **L'identification des données pertinentes** : cette étape vise à optimiser les performances du système tout en évitant les sous- et sur-apprentissage. En pratique, elle vous permet de vous assurer que certaines classes ou catégories inutiles pour la tâche visée ne sont pas représentées, que les proportions entre les différentes classes d'intérêt sont bien équilibrées, etc. Cette procédure vise également à identifier les données non pertinentes pour l'apprentissage (qui devront alors être supprimées de la base).
- La mise en œuvre de **mesures pour intégrer dès leur conception les principes de protection des données personnelles** : cette étape vous permet d'appliquer des transformations sur les données (telles que des mesures de généralisation et/ou de randomisation, anonymisation des données, etc.) pour limiter l'impact pour les personnes.
- **Le suivi et la mise à jour des données** : les mesures de minimisation pourraient devenir obsolètes au cours du temps. En effet, les données collectées pourraient perdre leurs caractères exact, pertinent, adéquat et limité, en raison d'une possible **dérive des données**, d'une mise à jour de celles-ci ou de l'évolution des techniques. Vous devrez donc conduire une analyse régulière pour assurer le suivi de la base de données constituée.
- **La documentation des données** utilisées pour le développement d'un système d'IA : celle-ci vous permet de garantir la traçabilité des jeux de données utilisés que la grande taille peut rendre difficile. Vous devez tenir cette documentation à jour en fonction des modifications apportées à la base de données. La CNIL fournit [ici](#) un modèle de documentation.

► Pour plus d'informations, voir les fiches [n° 6](#) et [n° 7](#)

---

## 6e étape : Définir une durée de conservation

### Le principe

Les données personnelles ne peuvent être conservées indéfiniment. Le RGPD vous impose de définir une durée au bout de laquelle les données doivent être supprimées ou, dans certains cas, archivées. **Vous devez déterminer cette durée de conservation en fonction de l'objectif** ayant conduit au traitement de ces données.

### En pratique

Vous devez fixer une durée de conservation des données utilisées pour le développement du système d'IA :

- **Pour la phase de développement** : la conservation des données doit faire l'objet d'une planification en amont et d'un suivi dans le temps. Les personnes concernées doivent être informées de la durée de conservation des données (par exemple dans les [mentions d'information](#)) ;
- **Pour la maintenance ou l'amélioration du produit** : lorsque les données n'ont plus à être accessibles pour les tâches quotidiennes des personnes en charge du développement du système d'IA, elles doivent en principe être supprimées. Elles peuvent toutefois être conservées pour la maintenance du produit ou son amélioration si des garanties sont mises en œuvre (support cloisonné, restriction des accès aux seules personnes habilitées, etc.).

**À noter : la conservation des données d'apprentissage peut permettre d'effectuer des audits et faciliter la mesure de certains biais.** Dans ces cas, une conservation prolongée des données peut être justifiée, sauf si la conservation d'informations générales sur les données suffit (par exemple, la

documentation réalisée sur le modèle proposé dans la section [Documentation](#), ou encore des informations sur la distribution statistique des données). Cette conservation doit être limitée aux données nécessaires, et s'accompagner de mesures de sécurité renforcées.

► Pour plus d'informations, voir la [fiche n° 7](#)

---

## 7e étape : Réaliser une analyse d'impact sur la protection des données (AIPD)

### Le principe

L'analyse d'impact sur la protection des données (AIPD) est une démarche qui vous permet de cartographier et d'évaluer les risques d'un traitement sur la protection des données personnelles et d'établir un plan d'action pour les réduire à un niveau acceptable. Elle va notamment vous conduire à définir les mesures de sécurité pour protéger les données.

### En pratique

La réalisation d'une AIPD pour le développement de systèmes d'IA

**Il est fortement recommandé de réaliser une AIPD pour le développement de votre système d'IA** notamment lorsque deux des critères suivants sont remplis :

- des données sensibles sont collectées ;
- des données personnelles sont collectées à large échelle ;
- des données de personnes vulnérables (personnes mineures, en situation de handicap, etc.) sont collectées ;
- des ensembles de données sont croisés ou combinés ;
- de nouvelles solutions technologiques sont mises en œuvre ou une utilisation innovante est faite.

Par ailleurs, si des risques importants existent (par exemple : de mésusage des données, de **violation de données**, ou de discrimination), une AIPD doit être réalisée même si deux des critères précédents ne sont pas remplis.

Pour aider à réaliser une AIPD, [la CNIL met à disposition le logiciel open source PIA dédié](#).

Les critères de risque introduits par le règlement européen sur l'IA

La CNIL considère que, pour le développement des systèmes à haut risque visés par le règlement européen sur l'IA et impliquant des données personnelles, la réalisation d'une AIPD est en principe nécessaire.

À noter : la réalisation de l'AIPD pourra reposer sur la documentation exigée par le règlement sur l'IA sous réserve de comporter les éléments prévus par le RGPD (article 35 du RGPD).

Le périmètre de l'AIPD

Il existe deux types de situations pour le fournisseur d'un système d'IA, selon l'objectif du système d'IA (voir « [définir un objectif \(finalité\) pour le système d'IA](#) »).

- **Vous savez clairement quel sera l'usage opérationnel de votre système d'IA**

Il est recommandé de réaliser une AIPD générale pour l'ensemble du cycle de vie, qui comprend les phases de développement et de déploiement. Attention, si vous n'êtes pas l'utilisateur/déploieur du système d'IA, c'est ce dernier qui aura la responsabilité de réaliser l'AIPD pour la phase de déploiement (même s'il pourra s'appuyer sur le modèle d'AIPD que vous aurez proposé).

- **Si vous développez un système d'IA à usage général**

Vous ne pourrez réaliser une AIPD que sur la phase de développement. Cette AIPD doit être fournie aux utilisateurs de votre IA pour leur permettre de conduire leur propre analyse.

## Les risques liés à l'IA à prendre en compte dans une AIPD

Les traitements de données personnelles reposant sur des systèmes d'IA présentent des risques spécifiques que vous devez prendre en compte :

- les risques liés à la confidentialité des données susceptibles d'être extraites depuis le système d'IA ;
- les risques pour les personnes concernées liés à des mésusages des données contenues dans la base d'apprentissage (par vos employés qui y ont accès ou en cas de violation de données) ;
- le risque d'une discrimination automatisée causée par un biais du système d'IA introduit lors du développement ;
- le risque de produire du contenu fictif erroné sur une personne réelle, notamment dans le cas des systèmes d'IA génératives ;
- le risque de prise de décision automatisée quand l'agent utilisant le système n'est pas en capacité de vérifier sa performance en conditions réelles ou de prendre une décision contraire à la sortie du système sans que cela ne lui porte préjudice (en raison d'une pression hiérarchique par exemple) ;
- le risque d'une perte de contrôle des utilisateurs sur leurs données publiées et librement accessibles en ligne ;
- les risques liés aux attaques connues spécifiques aux systèmes d'IA (par exemple, les attaques par empoisonnement des données) ;
- les risques éthiques systémiques et graves liés au déploiement du système.

## Les mesures à prendre en fonction des résultats de l'AIPD

Une fois le niveau de risque déterminé, votre AIPD doit prévoir un ensemble de mesures visant à le réduire et à le maintenir à un niveau acceptable, par exemple :

- des mesures de sécurité (par exemple, le [chiffrement homomorphe](#) ou l'utilisation d'un environnement d'exécution sécurisé) ;
- des mesures de **minimisation**, (par exemple le recours à des données synthétiques) ;
- des mesures d'anonymisation ou de pseudonymisation (par exemple la confidentialité différentielle) ;
- des mesures de protection des données dès le développement (par exemple l'**apprentissage fédéré**) ;
- des mesures facilitant l'exercice des droits ou les recours pour les personnes (par exemple techniques de **désapprentissage machine**, mesures d'explicabilité et de traçabilité des sorties des systèmes d'IA, etc.) ;
- des mesures d'audit et de validation (par exemple des attaques fictives).

D'autres mesures, plus génériques, pourront également être appliquées : mesures organisationnelles (encadrement et limitation de l'accès aux bases de données d'apprentissage et pouvant permettre une modification du système d'IA, etc.), mesures de gouvernance (mise en place d'un comité éthique, etc.), mesures de traçabilité des actions ou documentation interne (charte information, etc.).

► Pour plus d'informations, voir la [fiche n°5](#)

---

## À suivre... La CNIL continue ses travaux pour aider les concepteurs de systèmes d'IA

Elle publiera prochainement de nouvelles fiches permettant d'expliquer comment concevoir et entraîner des modèles dans le respect du RGPD : récupération de données sur internet ; comment mobiliser l'intérêt légitime comme **base légale**, exercice des droits d'accès, de rectification et d'effacement ; recours ou non à des licences ouvertes...

Ces fiches seront soumises à consultation publique.

## Pour approfondir

- [La recommandation complète de la CNIL sur le déploiement des systèmes d'IA](#)
  - [Tous les contenus de la CNIL sur l'intelligence artificielle](#)
-