(Version française - Avril 2026)

Autorité de protection des données

L'impact de l'intelligence artificielle sur la vie privée

Table des matières

L'impact de l'intelligence artificielle sur la vie privée 6
1. Système d'IA 6
1.1. Notion et caractéristiques 6
1.2. Système d'IA et modèle d'IA 6
1.3. Domaines d'application des systèmes d'IA 7
1.4. Cycle de vie des systèmes d'IA et activités de traitement de données y afférentes 8
2. Risques en termes de vie privée 10
3. Protéger ses données à caractère personnel 11
3.1. Principaux points d'attention 11
3.2. Droits des personnes concernées 13
3.3. Exercer ses droits en tant que personne concernée 16
Sources: 18

Objectif de la présente brochure d'information

L'Autorité de protection des données (APD) surveille continuellement les développements sociaux, économiques et technologiques qui ont un impact sur la protection des données à caractère personnel.

Parmi ces tendances en pleine évolution, l'utilisation de systèmes d'intelligence artificielle (IA) s'est étendue au-delà de l'industrie et du monde universitaire pour s'intégrer dans la vie quotidienne des citoyens. D'outils d'assistance virtuels au diagnostic médical assisté par l'IA, les citoyens interagissent de plus en plus avec des systèmes d'IA. Certains de ces systèmes sont entraînés sur des données à caractère personnel[1] collectées dans différentes sources, dont les contenus des réseaux sociaux, les recherches Internet, les contributions dans les chatbots (agents conversationnels) ou les achats en ligne. Toutefois, la complexité et l'opacité des systèmes d'IA permettent difficilement de comprendre quelles sont les données à caractère personnel qui sont collectées, les finalités du traitement[2] ou le processus décisionnel. Ces caractéristiques affectent les citoyens dans l'exercice de leur droit à la protection des données, entraînant une perte de contrôle de leurs données à caractère personnel et une limitation de leur capacité à contester des résultats injustes.

Le droit à la vie privée et le droit à la protection des données, consacrés dans la Charte des droits fondamentaux de l'Union européenne et dans le Règlement général sur la protection des données (RGPD), prévoient des droits objectifs destinés à garantir le contrôle des citoyens sur leurs données à caractère personnel. Par ailleurs, l'Artificial Intelligence Act (AI Act, règlement sur l'IA) élabore un cadre réglementaire pour le développement et le déploiement de systèmes d'IA, destiné à favoriser un environnement innovant tout en respectant la sécurité, la santé et les droits fondamentaux des citoyens.

Dans ce contexte, la présente brochure d'information a été conçue pour aider les citoyens à comprendre comment les systèmes d'IA peuvent affecter leur vie privée et la protection de leurs données à caractère personnel. Cette brochure contient également des recommandations pratiques pour aider les citoyens à garder le contrôle de leurs données dans un environnement de plus en plus impacté par l'IA.

---

[1] Article 4.1) du RGPD : " *'données à caractère personnel', toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée 'personne concernée') ; est réputée être une 'personne physique identifiable' une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;*"
Remarque : Une protection plus stricte s'applique au traitement de catégories particulières de données (par ex. données relatives à la santé, à la race, à la religion), en vertu de l'article 9 du RGPD.

[2] Article 4.2) du RGPD : " *'traitement', toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;*"

S'inspirant du contenu de la brochure "Les systèmes d'intelligence artificielle et le RGPD sous l'angle de la protection des données" de décembre 2024, le Secrétariat Général entend explorer des thèmes spécifiques pour sensibiliser les citoyens, augmenter la maîtrise de l'IA et donner des conseils pratiques au monde de l'industrie à travers une série de publications sur l'IA et la protection des données. La série est disponible dans son intégralité **ici**.

Public cible de la présente brochure d'information

La présente brochure d'information s'adresse aux citoyens qui utilisent ou interagissent avec des systèmes d'IA dans leur vie quotidienne – que ce soit via des plateformes en ligne, des applications mobiles, des appareils connectés ou d'autres services numériques.

Elle est destinée aux lecteurs qui souhaitent comprendre comment les systèmes d'IA utilisent leurs données à caractère personnel et de quelle manière cela peut affecter leur vie privée, sans avoir besoin de connaissances techniques ou légales.

Au moyen d'explications claires et d'exemples concrets, la brochure offre un aperçu concis de ce que sont les systèmes d'IA, de la manière dont ils fonctionnent, des types de données à caractère personnel qu'ils collectent et traitent, des risques potentiels engendrés en termes de vie privée et des droits dont disposent les citoyens en vertu de la législation en matière de protection des données – en reprenant des démarches simples pour exercer ces droits.

L'impact de l'intelligence artificielle sur la vie privée

1. Système d'IA

1.1. Notion et caractéristiques

L'AI Act définit un système d'IA comme suit : "*un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites*[3]*, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels*"[4].

Cette définition adopte une perspective fondée sur le cycle de vie en distinguant la phase de développement de systèmes d'IA de leur déploiement. À cet égard, la définition admet que leurs caractéristiques puissent apparaître dans une phase sans être transférées à l'autre.[i]

Dans l'absolu, les systèmes d'IA sont des systèmes informatiques qui peuvent prendre des décisions en analysant des données et en identifiant des modèles. Leur autonomie permet l'apprentissage au départ desdites données pour adapter et améliorer les performances de manière à générer des résultats plus précis et plus nuancés, parfois en déduisant un comportement futur.[ii]

1.2. Système d'IA et modèle d'IA

Ce qui distingue les systèmes d'IA des systèmes d'automatisation traditionnels – comme la segmentation client prédéfinie (des utilisateurs regroupés sur la base de caractéristiques prédéfinies) ou des outils de masquage de données à règles fixes (remplacer des noms ou des identifiants par des pseudonymes en utilisant des modèles établis) –, c'est leur capacité d'inférence à partir de données ou de connaissances.[iii] Les systèmes d'IA incorporent des techniques de traitement de données avancées[5] pour inférer à partir de données et, dans certains cas, pour apprendre ou adapter.[iv]

Ces techniques de traitement de données sont appliquées par un ou plusieurs modèle(s) d'IA contenu(s) dans un système d'IA. Un modèle d'IA est un algorithme entraîné à l'aide d'une base de données afin de réaliser un ensemble de tâches prédéfinies ou apprises par le biais d'un entraînement. Les systèmes d'IA intègrent un (des) modèle(s) d'IA à d'autres

[3] Les objectifs explicites sont ceux qui ont été délibérément encodés dans le système par son développeur (par ex. minimiser les erreurs, maximiser le taux de clics, prédire le risque de maladie). Les objectifs implicites sont déduits à partir du comportement du système ou d'hypothèses sous-jacentes (par ex. favoriser les publications provoquant des émotions, amplifier le contenu polarisant ou prioriser le contenu d'utilisateurs très actifs peut indiquer un but caché qui est d'accroître l'engagement).
[4] Article 3.1) de l'AI Act.
[5] On peut distinguer deux approches principales pour traiter des données. D'une part, avec une approche d'apprentissage automatique, le système d'IA apprend à partir des données la manière d'atteindre un ensemble spécifique d'objectifs. D'autre part, avec les approches fondées sur la logique et les connaissances, les systèmes d'IA sont capables de faire des inférences à partir des connaissances encodées ou de la représentation symbolique de la tâche en question.

composants du système (outils de contrôle, interfaces de programmation d'applications (API), etc.).[v]

L'analogie culinaire peut aider à comprendre la différence. Entraîner un modèle d'IA revient à créer une recette de gâteau, tandis que le système d'IA cuit le gâteau. Le gâteau confectionné (la sortie ou l'*output*) dépend de la qualité des ingrédients (les données), de la fiabilité de la recette (l'architecture du modèle d'IA) et des étapes à suivre (l'algorithme). L'intégration de ce modèle dans le système d'IA permet au gâteau d'être confectionné en suivant la recette, avec les bons ingrédients, en réalisant les étapes dans l'ordre et en utilisant le four, le moule à gâteau, les bols mélangeurs, etc. (l'infrastructure, les API, les interfaces, etc.) pour achever le processus.

1.3. Domaines d'application des systèmes d'IA

Les systèmes d'IA peuvent être utilisés dans de nombreux cas[6]. Dès lors, en fonction de leur objectif, les systèmes d'IA peuvent être classés dans une ou plusieurs des catégories ci-après. Le but poursuivi par l'utilisation d'un système d'IA contribuera aussi à identifier les catégories de données nécessaires à son entraînement et à son déploiement.

Les systèmes experts simulent la capacité décisionnelle d'un expert humain dans des domaines spécifiques (par ex. fournir des commentaires diagnostiques cliniques automatisés sur des rapports médicaux). Ils requièrent souvent des données à caractère personnel structurées telles que des dossiers de santé, des antécédents médico-légaux ou des informations diagnostiques.

Les systèmes autonomes peuvent fonctionner de manière indépendante dans des environnements dynamiques (par ex. les voitures autonomes, les drones). Ils peuvent traiter des données de localisation, des données de capteurs ou des identifiants biométriques.

L'informatique cognitive imite les processus de pensée humaine pour interpréter des données non structurées et soutenir la prise de décision (par ex. des systèmes utilisés pour analyser des informations de patients). Ces systèmes utilisent souvent diverses données à caractère personnel telles que des e-mails, des enregistrements vocaux, des documents et des historiques de conversations.

La vision par ordinateur interprète des entrées visuelles (*visual inputs*), comme des images ou des vidéos, pour des tâches de reconnaissance, de suivi ou d'analyse (par ex. les systèmes utilisés pour surveiller les mouvements de patients). Un tel système peut traiter des images faciales, des schémas de marche et des séquences vidéo.

Les robots assistés par l'IA sont des machines qui exécutent des tâches complexes en interaction avec leur environnement (par ex. les aspirateurs robots autonomes). Selon leur application, ils peuvent utiliser des données audiovisuelles et des données de localisation.

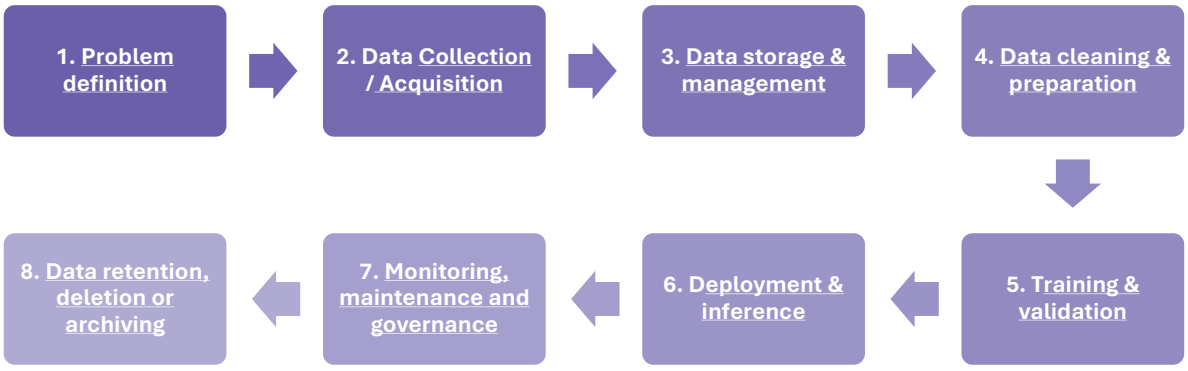
Les systèmes de traitement automatique du langage naturel par l'IA sont conçus pour comprendre, interpréter et générer du langage humain sous la forme de texte ou de

[6] Voir la brochure 'Les systèmes d'intelligence artificielle et le RGPD sous l'angle de la protection des données', pages 6-7, publiée par l'APD.

paroles (par ex. les chatbots). Ces systèmes traitent souvent des historiques de conversations, des commandes vocales.

1.4. Cycle de vie des systèmes d'IA et activités de traitement de données y afférentes

Indépendamment de leur objectif, les systèmes d'IA suivent généralement des activités similaires de traitement de données durant leur cycle de vie. Le schéma ci-dessous montre les activités de traitement de données habituellement effectuées lors d'un cycle de vie d'un système d'IA.



vi

1. Définition du problème : La première étape consiste à identifier le but du système d'IA. Ce but doit être clairement défini et inclut généralement des objectifs, des critères de réussite et des obligations réglementaires.

2. Collecte/acquisition des données : La deuxième étape consiste à collecter ou à acquérir des données brutes, y compris des données à caractère personnel, provenant de différentes sources. De telles sources incluent notamment :

- Les activités sur les réseaux sociaux : publications en ligne, 'likes', commentaires, connexions, etc.
- Des bases de données de clients : noms, e-mails, numéros de téléphone, historique d'achats, etc.
- Des relevés de transactions : paiements par carte de crédit, factures, données de cartes de fidélité, etc.
- L'historique de navigation : sites Internet visités, demandes de recherche, habitudes de clics, etc.
- Des documents publics : registres du commerce, titres de propriété, messages d'un forum, etc.
- Des dispositifs intelligents : commandes vocales, localisation GPS, mesures du capteur d'activité physique, etc.

3. Stockage et gestion des données : La troisième étape vise à stocker et à gérer en toute sécurité les données collectées ou acquises lors de l'étape précédente. Ceci inclut

l'application de conditions de stockage appropriées et des mesures de sécurité telles que le cryptage, des contrôles d'accès et des mécanismes de protection de la vie privée.

4. Nettoyage et préparation des données : Au cours de la quatrième étape, les données brutes sont prétraitées afin d'améliorer la qualité et la cohérence tout en garantissant le respect de la vie privée. Ces activités de prétraitement peuvent impliquer la correction d'erreurs dans les données (par ex. surreprésentation ou sous-représentation de certaines tranches de la population), la standardisation des données (par ex. toutes les dates sont enregistrées sous le format suivant : JJ/MM/AAAA ; toutes les données de genre sont enregistrées sous le format suivant : Masculin/Féminin), et dans la mesure du possible, la pseudonymisation ou l'anonymisation des données à caractère personnel. Une fois nettoyées, les données sont généralement réparties en trois bases de données différentes qui serviront chacun leur propre objectif lors de la cinquième étape (base de données d'entraînement, base de données de validation et base de données de test).

5. Entraînement et validation : Lors de cette étape, les bases de données sont utilisées pour entraîner, valider et tester un système d'IA afin de garantir le bon fonctionnement du système d'IA. Les données de validation permettent d'adapter le système lors de l'entraînement alors que les données de test sont utilisées pour évaluer des indicateurs de performance clés tels que la précision, l'équité et la généralisabilité. Les données d'entraînement sont utilisées pour entraîner le système d'IA avant son déploiement.

6. Déploiement et inférence : Après une validation réussie, un système d'IA entraîné est déployé et commence à recevoir des données d'entrée (*input data*) (par ex. des prompts de l'utilisateur ou des demandes générées par le système) et à générer des sorties (*outputs*). Des mécanismes de filtrage peuvent être appliqués afin d'éviter des entrées non désirées ou des sorties interdites.

7. Contrôle, maintenance et gouvernance : Après le déploiement, un système d'IA est surveillé afin de garantir la performance attendue. Les données de rétroaction et du système peuvent être utilisées pour un affinage ou un réentraînement du modèle. Des processus de gouvernance assurent la conformité, l'auditabilité et la responsabilité tout au long du cycle de vie de l'AI.

8. Conservation, suppression ou archivage des données : Les données à caractère personnel ne doivent être conservées que le temps nécessaire. Une fois qu'elles ne sont plus nécessaires, les données doivent être supprimées, anonymisées ou archivées de manière sûre, conformément aux législations de protection des données et aux politiques organisationnelles en vigueur.

Il convient de noter que les septième et huitième étapes peuvent être effectuées simultanément et représentent un processus continu. Au cours du cycle de vie d'un système d'IA, une surveillance continue est nécessaire afin d'identifier des résultats injustes ou inexacts. Cette surveillance permet d'adapter le système d'IA pour améliorer la performance et corriger les inexactitudes – qu'elles proviennent des données d'entraînement ou de validation ou du code source sous-jacent.

2. Risques en termes de vie privée

Les systèmes d'IA introduisent de nouvelles dimensions en matière de risques pour la vie privée en raison de la collecte à grande échelle de données et des modes de traitement. Ces risques sont engendrés par la collecte, le traitement ou le partage illicite ou non autorisé(e) de données à caractère personnel. Toutefois, même des pratiques légales de gestion de données peuvent susciter des inquiétudes en matière de vie privée – particulièrement lorsqu'elles manquent de transparence, de loyauté ou de proportionnalité. À titre d'exemples, citons la surveillance excessive, le profilage ou des traitements ultérieurs imprévus de données.

Les systèmes d'IA peuvent amplifier les risques pour la vie privée – comme le risque d'une collecte excessive ou disproportionnée de données et des violations potentielles du principe de minimisation des données (article 5.1.c) du RGPD) – en raison de leur capacité à traiter de grandes quantités de données à caractère personnel souvent en temps réel. Les risques autrefois isolés – comme le profilage[7] manuel, la surveillance limitée ou la publicité ciblée – peuvent désormais se transformer en problèmes systémiques. Les systèmes d'IA peuvent être utilisés pour établir le profil de millions d'utilisateurs, appliquer la reconnaissance faciale dans des espaces publics et proposer des publicités hautement personnalisées et ciblées.[vii] La rapidité, l'ampleur et l'opacité de la prise de décision automatisée des systèmes d'IA compliquent la prévention des violations aux droits à la vie privée et à la protection des données.

L'automatisation gérée par l'IA pourrait supprimer ou réduire la surveillance humaine des décisions automatisées basées sur des données. De telles évaluations automatisées sont utilisées dans des scénarios du quotidien comme l'estimation de la solvabilité, les évaluations de risques de sécurité et les processus de recrutement ou de sélection. Cette caractéristique de la prise de décision automatisée soulève des inquiétudes concernant la transparence et l'implication humaine, ce qui peut nuire à l'équité des résultats et limiter la capacité des citoyens à demander réparation.[viii] Bien que l'article 22 du RGPD interdise des décisions fondées exclusivement sur un traitement automatisé produisant des effets significatifs (voir la section 3.2.h)), des exemptions sont prévues sous certaines conditions et moyennant certaines garanties.

La capacité de l'IA à déduire des données à caractère personnel sensibles peut donner lieu à des activités de traitement illégales ou à la catégorisation et au profilage des citoyens.[ix] En utilisant des techniques d'apprentissage automatique, les systèmes d'IA peuvent retrouver certains attributs comme l'orientation sexuelle, les convictions religieuses, l'état de santé ou l'état émotionnel à partir de sources indirectes comme l'historique de navigation, l'historique d'achats en ligne ou le ton de la voix – souvent à l'insu du citoyen ou sans son consentement. En outre, des déductions peuvent être inexactes ou

[7] Article 4.4) du RGPD : " *'profilage', toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ;*"

trompeuses en raison de leur caractéristique probabiliste[x] (des estimations statistiques plutôt que des faits vérifiés).

3. Protéger ses données à caractère personnel

Le RGPD a un large champ d'application et couvre des activités incluant le traitement de données à caractère personnel au sein de l'UE[8]. Les systèmes d'IA peuvent traiter des données à caractère personnel à différents stades de leur cycle de vie[xi], parfois sans que cela soit intentionnel. En fait, les systèmes d'IA destinés à ne pas traiter de données à caractère personnel doivent être entraînés à reconnaître de telles données. Dans ce cas, des données à caractère personnel seront incluses dans les bases de données d'entraînement, de validation et de test et seront traitées dans la phase de développement.

L'article 5 du RGPD énumère les principes que toute activité de traitement de données à caractère personnel doit respecter. Ces principes exigent que les données à caractère personnel soient : traitées de manière licite, loyale et transparente ; collectées pour des finalités déterminées, explicites et légitimes ; adéquates, pertinentes et limitées à ce qui est nécessaire pour atteindre ces finalités ; exactes et tenues à jour ; conservées pendant une durée n'excédant pas celle nécessaire au traitement ; et sécurisées de manière appropriée. En outre, les responsables du traitement[9] doivent être en mesure de démontrer le respect de ces principes.

En vertu du principe de transparence, les responsables du traitement sont tenus d'informer les citoyens à propos des activités de traitement de façon claire et accessible. Plus spécifiquement, et le cas échéant, les responsables du traitement peuvent être amenés à expliquer la logique qui sous-tend la prise de décisions automatisées, telles que celles prises par les systèmes d'IA.

Les sections suivantes abordent les principaux aspects auxquels nous recommandons aux citoyens de prêter attention lorsqu'ils sont actifs en ligne. Ces recommandations ont pour but de les aider à prendre conscience des opérations de traitement qui sont effectuées et des moyens d'exercer leurs droits.

3.1. Principaux points d'attention

3.1.1. Vérifier les politiques de confidentialité, les conditions générales d'utilisation et les paramètres de confidentialité par défaut

Adhérer aux politiques de confidentialité permet aux responsables du traitement de traiter les données à caractère personnel qui y sont détaillées. Les citoyens ont le droit de ne pas approuver les politiques de confidentialité sans que cette action les empêche

[8] Articles 2 et 3 du RGPD.

[9] Article 4.7) du RGPD : " *'responsable du traitement' , la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.*"

d'accéder à des sites Internet, des services, etc. sauf s'il existe une raison légitime (par ex. des cookies nécessaires au fonctionnement du site Internet). Retirer son consentement devrait être aussi simple que de le donner.

Lire et vérifier les politiques de confidentialité ainsi que les conditions générales d'utilisation permet aux personnes concernées de comprendre comment leurs données à caractère personnel sont collectées, traitées et partagées. Ceci favorise la prise de décisions éclairées et facilite l'exercice effectif des droits à la protection des données.

Il est conseillé de vérifier les paramètres de confidentialité par défaut tels que ceux liés à l'historique des conversations, l'historique des recherches, l'entraînement de l'IA, la publicité personnalisée, le partage d'analyses et les sauvegardes automatiques dans le cloud. Ces paramètres sont souvent activés par défaut et peuvent être réglés en fonction des préférences personnelles.

En outre, pour les citoyens qui utilisent des appareils intelligents dans la sphère privée, il est recommandé de changer les mots de passe par défaut et de vérifier la manière dont ces appareils traitent leurs données à caractère personnel. Ces appareils intelligents collectent des informations liées aux activités domestiques des citoyens, pouvant inclure des données sensibles ou comportementales. Comprendre comment ces appareils collectent, traitent et partagent des informations permet d'identifier et d'atténuer des risques potentiels, ce qui contribue à réduire le partage superflu ou excessif de données dans la sphère privée.

3.1.2. Faire preuve de prudence lors du partage de données à caractère personnel

Avant de saisir des informations sensibles - telles que des informations médicales, des données financières ou des photos privées - dans des chatbots, des applications ou des plateformes en ligne, les personnes concernées devraient faire preuve de prudence. Dans la mesure du possible, l'utilisation de pseudonymes ou le masquage d'informations permettant d'identifier une personne (par ex. les noms, les adresses ou l'âge) peut contribuer à protéger l'identité d'une personne.

Limiter la diffusion d'informations personnelles réduit le risque d'abus, de profilage ou d'accès non autorisé, ce qui renforce le contrôle des données à caractère personnel.

Avant d'interagir avec des systèmes d'IA, les citoyens sont encouragés à réfléchir à la sensibilité des informations qu'ils fournissent. Une question utile pour orienter cette réflexion pourrait être la suivante : "Si j'étais à table avec des inconnus, me sentirais-je à l'aise de partager ces informations sur moi-même ou sur quelqu'un d'autre ?"

3.1.3. Garder ses logiciels et ses appareils à jour

La mise à jour régulière des logiciels et des micrologiciels contribue à atténuer les risques en matière de sécurité, réduisant ainsi le risque d'une violation de données ou d'un accès non autorisé à des données à caractère personnel.

3.1.4. Gérer les autorisations des applications et des appareils

Il est recommandé de vérifier régulièrement les applications ayant accès au micro, à la caméra, aux données de localisation, aux contacts et aux fichiers des appareils.

Lorsque certaines autorisations ne sont pas essentielles, la personne concernée peut choisir de les désactiver ou de les activer uniquement lorsque c'est nécessaire - par ex., en limitant l'accès aux photos ou en les partageant ponctuellement avec des applications spécifiques. Régler les autorisations de cette façon permet de limiter les accès superflus à des données à caractère personnel et de s'assurer que seules les informations essentielles sont traitées.

3.2. Droits des personnes concernées

Suivre les recommandations formulées dans les sections précédentes devrait déjà permettre aux citoyens de comprendre le type de données à caractère personnel que les responsables du traitement détiennent et utilisent. En outre, le RGPD confère aux citoyens des droits qui peuvent être exercés en contactant lesdits responsables du traitement. En cas de demande d'exercice de ces droits, les responsables du traitement doivent y répondre dans un délai d'un mois. Ce délai peut être prolongé de deux mois supplémentaires, si cela se justifie.

3.2.1. Droit à l'information

Les articles 13 et 14 du RGPD prévoient un droit à l'information qui impose aux responsables du traitement l'obligation d'informer les citoyens sur les activités de traitement effectuées. Ces informations devraient permettre aux citoyens de prendre des décisions en connaissance de cause et d'exercer leurs droits en matière de protection des données. Ces informations doivent être fournies dans un langage clair et accessible et se trouvent généralement dans la politique de confidentialité.

Le RGPD distingue les situations où les données à caractère personnel sont collectées directement auprès de la personne concernée (formulaires de consentement, abonnements à un site Internet, etc.) et celles où ces données sont collectées indirectement (*web scraping* (ou moissonnage), contrats de licence, etc.). Lorsque des données à caractère personnel sont collectées indirectement, l'article 14 du RGPD impose aux responsables du traitement d'informer les personnes concernées dans un délai d'un mois à partir de la collecte.

Les responsables du traitement doivent communiquer les informations suivantes : l'identité et les coordonnées du responsable du traitement ; la (les) finalité(s) et la (les) base(s) juridique(s) de l'opération de traitement ; les délais de conservation ; les droits des personnes concernées ; les informations relatives aux transferts de données ainsi que des informations relatives à la prise de décision automatisée. En vertu de l'article 14 du RGPD, les responsables du traitement sont également tenus de communiquer les sources des données et les catégories de données à caractère personnel collectées.

3.2.2. Droit d'accès

En vertu de l'article 15 du RGPD, les personnes concernées ont le droit d'obtenir la confirmation que leurs données à caractère personnel sont ou ne sont pas traitées. Lorsque ce droit est exercé, les responsables du traitement doivent donner accès aux informations telles que les finalités du traitement et les catégories de données traitées ; les destinataires des données s'il en existe ; la durée de conservation ; les droits en matière de protection des données ; le droit d'introduire une plainte auprès d'une autorité de

contrôle ; la source des données lorsque celles-ci ne sont pas collectées directement auprès de la personne concernée ainsi que l'existence de toute prise de décision automatisée, y compris un profilage, avec des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

En outre, les personnes concernées ont le droit d'obtenir une copie des données à caractère personnel faisant l'objet du traitement, sans frais, si cette copie est nécessaire à la compréhension du contexte dans lequel l'activité de traitement de données est effectuée[10].

3.2.3. Droit à l'effacement

En vertu de l'article 17 du RGPD, les personnes concernées peuvent demander l'effacement de leurs données à caractère personnel dans les meilleurs délais lorsque certaines conditions s'appliquent :

- lorsque les données à caractère personnel ne sont plus nécessaires pour la finalité initiale ;
- lorsque la personne concernée retire son consentement et qu'il n'existe pas d'autre fondement juridique pour le traitement ;
- lorsque la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et qu'il n'existe pas de motif légitime impérieux ;
- lorsque les données à caractère personnel ont fait l'objet d'un traitement illicite ;
- lorsque les données à caractère personnel doivent être effacées pour respecter une obligation légale ; ou
- lorsque les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information.

Dans les situations où le responsable du traitement a communiqué les données à caractère personnel à des destinataires tiers ou les a rendues publiques, il doit prendre des mesures appropriées pour garantir l'effacement de ces données à caractère personnel[11].

3.2.4. Droit d'opposition

L'article 21 du RGPD confère aux personnes concernées le droit de s'opposer au traitement de leurs données à caractère personnel. En cas d'opposition, le responsable du

[10] D'après la CJUE, dans l'affaire C-487/21 (*Österreichische Datenschutzbehörde* et CRIF), une "copie" peut inclure des passages de documents originaux ou des documents entiers, si cela est nécessaire pour assurer l'effectivité du droit d'accès, tout en respectant également les droits et libertés d'autrui. Le format doit permettre à la personne concernée de conserver et de consulter les données et, dans certains cas (par ex. notes manuscrites ou enregistrements vocaux), le format lui-même peut faire partie intégrante des données à caractère personnel.

[11] Article 19 du RGPD : "*Le responsable du traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement effectué conformément à l'article 16, à l'article 17, paragraphe 1 et à l'article 18, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement fournit à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande.*"

traitement doit mettre fin au traitement, à moins qu'il ne puisse démontrer l'existence de motifs légitimes impérieux.

Dans le cas d'un traitement à des fins de marketing direct, le droit d'opposition est absolu et ne nécessite aucune justification.

Par ailleurs, l'APD et l'autorité française de protection des données ont publié des lignes directrices décrivant les démarches que les citoyens peuvent entreprendre pour empêcher les entreprises de la tech (telles que Meta, TikTok, Microsoft, X) d'utiliser leurs données à caractère personnel pour entraîner leurs systèmes d'IA. Ces mesures peuvent être consultées ici et ici.

3.2.5. Droit à la limitation du traitement[11]

En vertu de l'article 18 du RGPD, les personnes concernées ont le droit de demander la limitation des activités de traitement lorsque :

- l'exactitude des données à caractère personnel est contestée par la personne concernée ;
- les données ont fait l'objet d'un traitement illicite ;
- le responsable du traitement n'a plus besoin des données pour leur finalité initiale mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;
- la personne concernée s'est opposée au traitement (article 21 du RGPD) pendant l'exercice de pondération entre les intérêts du responsable du traitement et ceux de la personne concernée.

Pendant une telle limitation, les données à caractère personnel ne peuvent être traitées (à l'exception de la conservation) qu'avec le consentement de la personne concernée ou pour des actions en justice, ou pour la protection des droits d'une autre personne (physique ou morale) ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre. La personne concernée doit être informée avant que la limitation ne soit levée.

Le droit à la limitation du traitement diffère du droit d'opposition car il entraîne une interruption de toutes les opérations de traitement plutôt qu'uniquement de celles visant des finalités spécifiques.

3.2.6. Droit de rectification

L'article 16 du RGPD confère aux personnes concernées le droit de demander que les données à caractère personnel inexactes soient rectifiées et que les données incomplètes soient complétées (y compris en fournissant une déclaration complémentaire).

Si les données ont été communiquées à des tiers, le responsable du traitement doit les informer de la rectification, à moins que cela se révèle impossible ou exige des efforts disproportionnés.

3.2.7. Droit à la portabilité des données

Conformément à l'article 20 du RGPD, les personnes concernées ont le droit de recevoir leurs données à caractère personnel dans un format structuré, couramment utilisé et

lisible par machine. Elles ont également le droit de transmettre ces données à un autre responsable du traitement lorsque le traitement est fondé sur le consentement de la personne concernée, est nécessaire à l'exécution d'un contrat ou est effectué à l'aide de procédés automatisés. Lorsque cela est techniquement possible, les données doivent être transmises directement au nouveau responsable du traitement.

3.2.8. Droit de ne pas faire l'objet d'une décision automatisée

L'article 22 du RGPD confère aux personnes concernées le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques les concernant ou les affectant de manière significative de façon similaire[12].

Une opération de traitement n'est pas entièrement automatisée lorsqu'elle implique une intervention humaine significative. Cela suppose l'intervention d'une personne ayant l'autorité suffisante pour modifier le résultat de l'activité de traitement.[xii]

La prise d'une décision automatisée est autorisée lorsqu'elle est nécessaire à l'exécution d'un contrat, avec le consentement explicite de la personne concernée ou si la loi l'autorise. Dans ces cas, les responsables du traitement doivent veiller à ce que les personnes concernées aient le droit : d'obtenir une intervention humaine[13] de la part du responsable du traitement ; d'exprimer leur point de vue et de contester la décision.

En outre, conformément à l'article 15.1.h) du RGPD, les personnes concernées ont le droit d'obtenir des informations sur le fonctionnement du mécanisme sous-jacent de la prise de décision automatisée[14,15]. Ceci implique la communication claire des procédures et des principes appliqué(e)s pour comprendre comment les données à caractère personnel ont été utilisées dans la prise de décision automatisée[16].

3.3. Exercer ses droits en tant que personne concernée

Lorsqu'un responsable du traitement est soupçonné d'utiliser abusivement des données à caractère personnel ou lorsqu'il devient nécessaire de vérifier quelles données sont traitées, les personnes concernées peuvent exercer leurs droits à la protection des données.

---

[12] Conformément aux Lignes directrices du Groupe de travail Article 29 relatives à la prise de décision individuelle automatisée et au profilage (2018), une décision peut être considérée comme ayant des effets significatifs similaires si la décision est de nature à : affecter de manière significative la situation, le comportement ou les choix des personnes concernées ; avoir un impact prolongé ou permanent sur la personne concernée ; ou entraîner l'exclusion ou la discrimination des personnes.

[13] En ce qui concerne les systèmes d'IA à haut risque (Chapitre III de l'AI Act), les déployeurs confient le contrôle humain à des personnes physiques qui disposent des compétences, de la formation et de l'autorité nécessaires ainsi que du soutien nécessaire (article 26, paragraphe 2 de l'AI Act). L'article 14 de l'AI Act définit les exigences et les finalités du contrôle humain dans les systèmes d'IA à haut risque.

[14] *Dun & Bradstreet*, § 57.

[15] De plus, de manière générale, l'article 86 de l'AI Act prévoit que les citoyens ont le droit de recevoir des explications claires sur le rôle du système d'IA à haut risque dans la procédure décisionnelle si la décision affecte significativement leur santé, leur sécurité ou leurs droits fondamentaux.

[16] *Dun & Bradstreet*, § 61.

3.3.1. Contacter directement le responsable du traitement

Les personnes concernées peuvent exercer leurs droits en s'adressant au responsable du traitement.

- Utilisation d'une lettre type : L'APD a élaboré des lettres types sur mesure **ici**. Elles utilisent des formats standardisés pour aider à formuler de telles demandes. La lettre doit exposer clairement la nature de la demande ainsi que la base juridique sur laquelle elle est fondée.
- Identifier les coordonnées du responsable du traitement : S'il y en a un, la demande doit être adressée au délégué à la protection des données (DPO) désigné, dont les coordonnées sont fournies dans la politique de confidentialité. Si aucun DPO n'est spécifié, la demande peut être envoyée à l'adresse de contact générale du responsable du traitement.
- Conserver des preuves : La personne concernée devrait toujours conserver une copie de la demande. Cela servira de preuve au cas où des mesures supplémentaires, y compris une intervention réglementaire, deviendraient nécessaires.
- Accorder un délai de réponse : En vertu de la législation relative à la protection des données, les responsables du traitement sont tenus de répondre dans un délai d'un mois à compter de la réception de la demande. Dans des cas exceptionnels, ce délai peut être prolongé de deux mois supplémentaires, moyennant une motivation.

3.3.2. Faire intervenir l'APD

Si le responsable du traitement ne répond pas ou si la réponse est jugée inadéquate, la personne concernée peut saisir l'autorité de contrôle compétente :

- **Demander une médiation** : La médiation est souvent la méthode la plus efficace pour régler des litiges. L'APD peut demander au responsable du traitement de traiter les droits de la personne concernée de manière appropriée.
- **Introduire une plainte** : Si la médiation n'aboutit pas à un règlement, une plainte formelle peut être introduite après de l'APD. Cette procédure peut mener à des mesures répressives, qui incluent, mais sans s'y limiter, un avertissement, une amende administrative ou une injonction immédiate de mettre fin à des activités de traitement spécifiques.

Sources:

- Andreas Krause, Jonas Hübotter. Probabilistic Artificial Intelligence (2025). Consultable via ce lien : https://arxiv.org/pdf/2502.05244.
- Bart Custers, Helena Vrabec. Tell me something new: data subject rights applied to inferred data and profiles, Computer Law & Security Review, Volume 52, 2024, 105956, ISSN 2212-473X, https://linkinghub.elsevier.com/retrieve/pii/S0267364924000232. (https://www.sciencedirect.com/science/Article/pii/S0267364924000232).
- Bygrave, dans Kuner, Bygrave, Docksey. The EU General Data Protection Regulation (GDPR): A Commentary, Article 22 GDPR, (Oxford University Press 2020) p. 533.
- Daniel J. Solove. Artificial Intelligence and Privacy, 77 Fla. L. Rev. 1 (2025). Consultable via ce lien : https://scholarship.law.ufl.edu/flr/vol77/iss1/1.
- Enrico Glerean. Fundamentals of Secure AI Systems with Personal Data (2024), EDPB.
- Commission européenne. Lignes directrices sur la définition d'un système d'intelligence artificielle au sens du règlement (UE) 2024/1689 (AI Act, règlement sur l'IA), consultable via ce lien : https://digital-strategy.ec.europa.eu/fr/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application.
- Comité européen de la protection des données (European Data Protection Board, EDPB). Respecter les droits des individus (Guide PME). Consultable via ce lien : https://www.edpb.europa.eu/sme-data-protection-guide/respect-individuals-rights_fr.
- Contrôleur européen de la protection des données (European Data Protection Supervisor, EDPS). Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions (2016) (uniquement disponibles en anglais). Consultable via ce lien : https://www.edps.europa.eu/sites/default/files/publication/16-11-07_guidelines_mobile_apps_en.pdf.
- Contrôleur européen de la protection des données (European Data Protection Supervisor, EDPS). Lignes directrices sur les droits des individus concernant le traitement des données à caractère personnel (2014). Consultable via ce lien : https://www.edps.europa.eu/sites/default/files/publication/14-02-25_gl_ds_rights_fr.pdf.
- Contrôleur européen de la protection des données (European Data Protection Supervisor, EDPS). Tech Dispatch #2/2023 - Explainable Artificial Intelligence (XAI) (uniquement disponible en anglais). Consultable via ce lien : https://www.edps.europa.eu/system/files/2023-11/23-11-16_techdispatch_xai_en.pdf.
- Marco Almada. Law & Compliance in AI Security & Data Protection (2024), EDPB.
- OCDE (2024). “Explanatory memorandum on the updated OECD definition of an AI system”, OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris,

consultable via ce lien : https://doi.org/10.1787/623da898-en (uniquement disponible en anglais).

- Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE.
- Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828.
- Groupe de travail Article 29, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, 17/FR, WP251rev.01, 6 février 2018.

---

[i] Lignes directrices de la Commission *sur la définition d'un système d'intelligence artificielle au sens du règlement (UE) 2024/1689 (règlement sur l'IA)*, p. 2.
[ii] De plus amples informations sont disponibles dans le considérant 12 de l'AI Act.
[iii] Lignes directrices de la Commission *sur la définition d'un système d'intelligence artificielle au sens du règlement (UE) 2024/1689 (règlement sur l'IA)*, p. 5.
[iv] Considérant 12 de l'AI Act.
[v] Marco Almada - *Law & Compliance in AI Security & Data Protection*, p. 22-24.
[vi] Enrico Glerean - *Fundamentals of Secure AI Systems with Personal Data*, p. 40-44.
[vii] Daniel J. Solove, *Artificial Intelligence and Privacy*, 77 Fla. L. Rev. 1 (2025). Consultable via le lien suivant : https://scholarship.law.ufl.edu/flr/vol77/iss1/1, p. 59-62.
[viii] Daniel J. Solove, *Artificial Intelligence and Privacy*, p. 6, 55-66.
[ix] Daniel J. Solove, *Artificial Intelligence and Privacy*, p. 16-18, 36-37, 39-40.
[x] Andreas Krause, Jonas Hübotter (2025) - *Probabilistic Artificial Intelligence*. Consultable via le lien suivant : https://arxiv.org/pdf/2502.05244, p. 1-2, 37-38.
[xi] Marco Almada - *Law & Compliance in AI Security & Data Protection*, p. 25-26.
[xii] Groupe de travail Article 29, Lignes directrices *relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679*, 17/FR, WP251rev.01, 6 février 2018, p. 23.
Bygrave, dans Kuner, Bygrave, Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary, Article 22 GDPR*, (Oxford University Press 2020) p. 533.