CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Bonn, Bucarest, Dublin, Lisbonne, Madrid, Milan, Paris, La Haye, Vienne, Varsovie

# L'IA et les données personnelles
# Un guide pour les DPO
# « Foire aux questions »

## Groupe de travail du CEDPO sur l'IA
## 16 juin 2023

Informations de contact :
https://cedpo.eu
info@cedpo.eu

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

# À propos de ce guide

Ce guide a été préparé par le groupe de travail sur l'IA et les données de la Confédération des organisations européennes de protection des données (CEDPO). Il s'adresse aux délégués à la protection des données et répond, pour eux, aux questions fondamentales qui se poseront à mesure que leur travail croisera inévitablement et de plus en plus l'intelligence artificielle et les logiciels d'apprentissage automatique.

Les technologies d'intelligence artificielle et d'apprentissage automatique se développent rapidement et de manière exponentielle, et bien qu'elles n'impliquent pas toujours le traitement de données à caractère personnel, lorsqu'elles le font, c'est souvent à une vaste échelle et à un niveau de complexité élevé.

Cela introduit de nouveaux risques pour les personnes concernées ainsi que de nouveaux défis pour le DPO qui n'a pas nécessairement une formation en informatique, mais qui devra néanmoins analyser et comprendre les rouages et les implications de ces technologies. Les DPO doivent relever un double défi : ils sont confrontés à une courbe d'apprentissage abrupte, dans un domaine technologique dynamique qui évolue quotidiennement sous leurs yeux.

Bien qu'il incombe déjà aux DPO d'appliquer les principes de protection des données à l'intelligence artificielle, une tâche déjà complexe (et que ce guide explique), une nouvelle réglementation se profile également à l'horizon.

Le règlement européen sur l'intelligence artificielle fait son chemin dans l'appareil législatif de l'UE, avec une date d'entrée en vigueur prévue pour 2024. Une fois entré en vigueur, ce règlement fera double emploi avec le RGPD sur des points importants, ce qui entraînera des obligations supplémentaires pour les DPO. Les présentes orientations visent à mettre en évidence les points de jonction entre ces deux piliers majeurs et interdépendants du cadre réglementaire de l'UE.

Les entreprises et les organismes publics agissent rapidement pour comprendre et mettre en œuvre des solutions d'intelligence artificielle afin de réaliser toutes sortes de gains d'efficacité et d'opportunités de croissance des revenus. Le DPO n'a pas d'autre choix que de suivre le rythme ; la technologie n'attend pas. Les présentes orientations constituent donc un point de départ pour les DPO afin de commencer à naviguer dans le monde de plus en plus critique et complexe de l'intelligence artificielle.

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

# Table des matières

# 1. Le RGPD réglemente-t-il l'intelligence artificielle et l'apprentissage automatique ?

Oui, le RGPD réglemente l'IA et l'apprentissage automatique. Le RGPD réglemente toutes les formes de technologie qui traitent des données personnelles. En tant que règlement horizontal, basé sur les risques et, qui régit au niveau général plutôt que spécifique, le RGPD adopte de grands principes qui s'appliquent quel que soit le contexte particulier dans lequel les données à caractère personnel sont traitées. Cela contraste avec une réglementation verticale, fondée sur des règles, qui légifère spécifiquement pour des technologies ou des secteurs définis.

Il en résulte que le RGPD est explicitement neutre sur le plan technologique. Les mots « IA » ou « apprentissage automatique » n'apparaissent nulle part dans le texte du RGPD, mais il n'y a pas non plus de références à la blockchain, à l'Internet des objets, aux jetons non fongibles (NFT), à la réalité virtuelle, ni à aucune autre technologie émergente. L'absence de ces références est intentionnelle et non accidentelle. La logique des législateurs était que si des technologies spécifiques étaient mentionnées, cela pourrait permettre à des technologies futures encore inconnues d'échapper au champ d'application du règlement. Comme l'indique le considérant 15 : « Afin d'éviter de créer un risque grave de contournement, la protection des personnes physiques devrait être neutre sur le plan technologique et ne devrait pas dépendre des techniques utilisées ».

Le principe susmentionné de la neutralité technologique du RGPD a également été examiné et confirmé par la Cour de Justice de l'Union Européenne dans l'affaire C-25/17 *Tietosuojavaltuutettu et Jehovan todistajat - uskonnollinen yhdyskunta*. La grande chambre de la Cour a considéré que « la protection des personnes doit s'appliquer aussi bien au traitement de données automatisé qu'au traitement manuel ; que le champ de cette protection ne doit pas en effet dépendre des techniques utilisées, sauf à créer de graves risques de détournement ».[1]

Le RGPD est donc à l'épreuve du temps en fournissant des principes de haut niveau qui peuvent être adaptés à toute technologie émergente ou, de fait, à toute finalité de traitement des données imprévue. Par exemple, la réponse à la pandémie de Covid-19 en 2020 a montré comment les principes généraux existants du RGPD pouvaient être appliqués avec succès à une situation d'urgence inattendue qui a conduit à la création rapide de nouvelles technologies potentiellement intrusives pour la vie privée, telles que les applications de suivi et de traçage du Covid-19.

[1] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:62017CJ0025

Indépendamment, donc, du mode, de l'apparence, de la technique, du contexte ou de l'utilisation, si une technologie d'IA ou d'apprentissage automatique traite des données à caractère personnel, le RGPD s'applique. Par exemple, l'évolution actuelle des grands modèles de langage puissants, tels que ChatGPT, n'a pas été spécifiquement anticipée ou envisagée lorsque le RGPD est entré en application en 2018, mais il est clair que cette évolution et d'autres développements de ce type sont soumis au champ d'application du RGPD et doivent se conformer à ses principes.

## 2. Le traitement automatisé implique-t-il nécessairement l'IA ou l'apprentissage automatique ?

Non, il existe de nombreux cas où le traitement automatisé n'implique pas l'IA ou l'apprentissage automatique. Le considérant (15) du RGPD confirme que le traitement automatisé fait référence au traitement par des moyens automatisés, par opposition au traitement qui est effectué manuellement. Les opérations de traitement des données seront fréquemment « automatisées » sans qu'aucune composante d'IA ou d'apprentissage automatique ne soit impliquée. Par exemple, les outils de gestion de la relation client (CRM) impliqueront un traitement automatisé des données à caractère personnel (par le biais de systèmes informatiques), sans nécessairement faire intervenir l'IA ou l'apprentissage automatique.

Le même raisonnement s'applique aux deux concepts fondamentaux décrits dans les orientations du Comité Européen de la Protection des Données (CEPD) sur la prise de décision individuelle automatisée et le profilage aux fins du règlement 2016/679 :[2] Bien que l'on puisse s'attendre à ce que l'IA et l'apprentissage automatique deviennent de plus en plus importants, la prise de décision automatisée et le profilage ont été et peuvent encore être appliqués sans utiliser l'IA.

Le profilage est défini à l'art. 4 du RGPD comme « 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 ». Toutefois, comme indiqué, le profilage n'implique pas toujours l'IA ou l'apprentissage automatique, ce que confirment de nombreux cas d'utilisation.

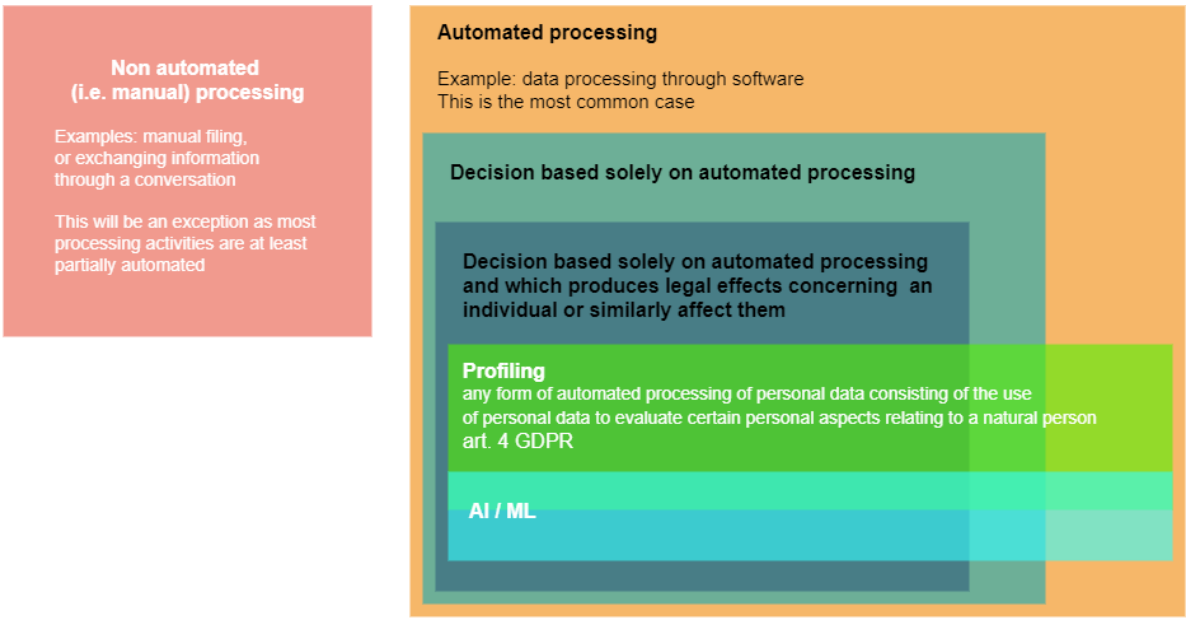
[2] https://ec.europa.eu/newsroom/article29/items/612053/en

Par exemple, les entreprises de commerce électronique ont utilisé le profilage pour comprendre les intérêts et les préférences des individus, puis suggérer des produits pertinents, bien avant que l'IA ou l'apprentissage automatique ne se développent.

La personne concernée qui fait l'objet d'une décision « sur le seul fondement d'un traitement automatisé et qui produit des effets juridiques la concernant ou qui, de façon similaire, l'affecte de manière significative » est couverte par le RGPD en particulier dans le considérant (71) et l'article 22. Le considérant (71) fournit deux illustrations : « le rejet automatique d'une demande de crédit en ligne » ou l'utilisation de « pratiques de recrutement en ligne sans aucune intervention humaine ». Il est clair que de telles décisions ne font pas toujours appel à l'IA ou à l'apprentissage automatique.

Par exemple, et comme indiqué dans les orientations du CEPD sur la prise de décision individuelle automatisée et le profilage, le rejet automatique d'une demande de crédit en ligne peut être mis en œuvre à l'aide d'un algorithme qui évalue une demande en fonction d'un ensemble de critères, tels que les informations fournies dans le formulaire de demande, ou les informations sur le comportement antérieur liées au compte, y compris les arriérés de paiement. Ces algorithmes peuvent être mis en œuvre sans recourir à l'intelligence artificielle ou à l'apprentissage automatique.

Le schéma suivant montre comment les concepts de traitement automatisé, d'IA et d'apprentissage automatique convergent et divergent :



## 3. L'IA et l'apprentissage automatique impliquent-ils toujours le traitement de données à caractère personnel ?

Non, les systèmes d'IA et d'apprentissage automatique n'impliquent pas toujours le traitement de données à caractère personnel. Ils peuvent être utilisés à diverses fins, qui peuvent n'avoir aucun lien avec les données à caractère personnel, telles que les prévisions météorologiques, où les données d'entrée sont des mesures atmosphériques provenant de capteurs, ou l'agriculture de précision pour optimiser l'utilisation des pesticides et des nutriments. Il existe donc de nombreux cas où les systèmes d'IA et d'apprentissage automatique traitent des données non personnelles.

Toutefois, les ensembles de données traités par les systèmes d'IA devraient être examinés plus en détail, même lorsque ces systèmes n'impliquent a priori pas de données à caractère personnel. Il est important de noter que les données non personnelles peuvent être de deux types : les données qui, à l'origine, ne se rapportaient pas à une personne physique identifiée ou identifiable et les données qui, à l'origine, étaient personnelles mais qui ont été anonymisées par la suite. Les données anonymes ne peuvent pas être attribuées à une personne spécifique, même en utilisant des données supplémentaires. Toutefois, si des données non personnelles peuvent être reliées à une personne de quelque manière que ce soit, la rendant directement ou indirectement identifiable, ces données doivent être considérées comme des données personnelles. Plusieurs exemples de réidentification d'ensembles de données prétendument anonymes ont montré qu'il faut être particulièrement prudent lors de l'anonymisation d'ensembles de données.

Il convient également de prendre en considération le cas des ensembles de données mixtes, qui sont constitués d'une combinaison de données à caractère personnel et non personnel. La frontière entre les données personnelles et non personnelles est donc parfois floue et, dans un ensemble de données mixtes, les données personnelles et non personnelles peuvent même être inextricablement liées. Ce type d'ensemble de données est particulièrement courant avec les technologiques émergentes tels que l'internet des objets, mais aussi l'IA et les systèmes d'apprentissage automatique. Dans ce cas, le RGPD s'applique.

Une fois que la question de savoir si les données contenues dans les ensembles de données sont personnelles ou non est examinée, une autre question doit être abordée.

Il convient de noter que la mise en œuvre d'un système d'IA se déroule (généralement) en deux phases, la phase d'apprentissage et la phase de production. Dans la phase d'apprentissage, le système d'IA apprend à partir d'un ensemble de données, créant un modèle capable de faire des prédictions ou de prendre des décisions. Dans la phase de production, le modèle formé est

appliqué à de nouvelles données pour générer des résultats, tels que des prédictions, des recommandations ou des décisions. Ces deux étapes n'ont pas le même objectif et doivent donc être séparées.

Il est donc possible qu'un système d'IA implique le traitement de données à caractère personnel à la fois dans sa phase d'apprentissage et dans sa phase de production, mais aussi dans une seule de ces deux phases. À cet égard, il est nécessaire d'étudier toutes les étapes du processus de mise en œuvre d'un système d'IA.

En outre, comme nous l'avons déjà mentionné à propos de la déduction de données à caractère personnel à partir de données non personnelles, il est important de souligner que même si les systèmes d'IA ne reçoivent pas explicitement des données à caractère personnel au cours de ces étapes, ils peuvent toujours déduire des informations à caractère personnel à partir de données non personnelles. Les données d'entrée et les données de sortie peuvent toutes deux comporter des informations à caractère personnel et l'une n'implique pas l'autre.

Compte tenu de tous ces aspects, nous pouvons dire que les systèmes d'IA et d'apprentissage automatique ne traitent pas toujours des données à caractère personnel, mais il est essentiel de veiller à ce que les données utilisées et générées soient véritablement non personnelles, lorsque c'est l'objectif recherché.

Une dernière remarque s'impose. Bien que les activités de traitement de base d'un système d'IA ne concernent pas les données à caractère personnel, il est toujours possible qu'il traite des données à caractère personnel liées à l'utilisateur humain réel de l'outil. Ces données peuvent être liées au compte nécessaire à l'utilisation du système d'IA ainsi qu'aux « données d'utilisation » qui peuvent directement ou indirectement identifier une personne réelle. Certaines données à caractère personnel peuvent même être déduites d'un tel cas d'utilisation, de l'utilisateur final ou d'une tierce personne, en particulier avec l'IA générative.

## 4. Certains articles et considérants du RGPD s'appliquent-ils spécifiquement à l'IA et à l'apprentissage automatique ?

Le RGPD s'applique à tous les traitements de données à caractère personnel, par conséquent, dans son sens le plus fondamental, chaque fois qu'un système d'IA ou d'apprentissage automatique est engagé dans le traitement de données à caractère personnel, alors le RGPD s'applique. Il est important de noter que ces obligations s'appliquent dès maintenant et un DPO ne doit pas attendre la réglementation officielle de l'IA par la Commission européenne par le biais de la proposition de règlement IA pour s'assurer que l'utilisation de l'IA par son responsable de

traitement est conforme à ses obligations en matière de protection des données en vertu du RGPD. Le RGPD est technologiquement agnostique et ne contient pas de références spécifiques à l'IA ou au traitement basé sur l'apprentissage automatique en tant que tel.

Néanmoins, certaines nuances doivent être prises en compte. En premier lieu, tous les systèmes d'IA ou d'apprentissage automatique n'impliquent pas le traitement de données à caractère personnel, de sorte que le RGPD ne s'applique pas systématiquement. En outre, l'article 2, paragraphe 2, du RGPD prévoit diverses exceptions, et l'utilisation d'un système d'IA ou d'apprentissage automatique dans ces circonstances serait également exclue au titre de ces exceptions (qu'il s'agisse ou non de traiter des données à caractère personnel).

Les systèmes d'IA et d'apprentissage automatique peuvent impliquer des données à caractère personnel de plusieurs manières, notamment :

- Elles peuvent faire partie de l'ensemble de données utilisé pour « entrainer » le système d'IA.
- Elles peuvent faire l'objet d'une recherche, à partir d'Internet, par exemple, dans le cadre d'une requête (en ce qui concerne le RGPD, le fait que les données soient publiques n'a pas d'importance).
- Elles peuvent être fourni par l'utilisateur final dans le cadre d'une requête ou d'une autre entrée dans le système d'IA.
- Elles peuvent être générée par le système d'IA, par inférence, ou par association via la recherche de motifs, etc.
- Le système d'IA peut, compte tenu des limites inhérentes au modèle génératif, se contenter d'inventer des choses, c'est-à-dire de générer du contenu plausible ou d'« halluciner » y compris des données personnelles.

Dès lors qu'un système d'IA ou d'apprentissage automatique traite des données à caractère personnel (quelle que soit la manière dont ces données sont entrées en sa possession), un certain nombre d'articles du RGPD s'appliquent directement. Il s'agit notamment de :

- Article 5 (principes) ; l'utilisation de l'IA ou du système d'apprentissage automatique, lorsqu'elle implique des données à caractère personnel, doit respecter tous les principes du RGPD. Comme pour tout système de traitement de données à caractère personnel, il convient de procéder à une évaluation des risques. Des préoccupations particulières peuvent exister en ce qui concerne, par exemple, la transparence, la minimisation et l'exactitude (voir la note sur l'« hallucination » ci-dessus) ; (voir aussi Considérant 39).

- Articles 4, 6 et 7 (licéité du traitement, consentement) ; dans la mesure où les systèmes d'IA et d'apprentissage automatique sont « entrainés » sur de grands ensembles de données, il doit y avoir une base juridique appropriée pour cela. Il se peut que dans de

nombreuses circonstances, le concept d'« intérêt légitime » soit invoqué, mais cela doit être clairement établi (considérant 47). Certaines circonstances (par exemple le traitement de catégories particulières) requièrent le consentement (article 7), alors que l'entrainement du système peut avoir été effectué à des fins de recherche scientifique, mais cette base devient caduque dès que l'utilisation du système passe dans le domaine commercial.

- Article 22 (prise de décision automatisée) : ce domaine fait l'objet d'une grande attention compte tenu des utilisations potentielles de l'IA et des systèmes d'apprentissage automatique. L'article 22 prévoit le droit pour les personnes concernées de s'opposer à un tel traitement, mais le droit correspondant prévu à l'article 14, paragraphe 2, point g), de recevoir des « informations utiles sur la logique mise en œuvre » est peut-être plus intéressant, ce qui constitue un défi compte tenu de la nature des systèmes concernés.

- Article 25 (Privacy by Design) ; l'article 25 exige que le responsable du traitement tienne compte de « l'état de la technique » afin de satisfaire aux exigences du règlement. Compte tenu de la complexité et des incertitudes qui entourent l'IA et les systèmes d'apprentissage automatique, des mesures supplémentaires peuvent être nécessaires pour garantir les droits des personnes concernées. Il convient de noter que le considérant 78 mentionne spécifiquement les « services ou produits qui traitent des données à caractère personnel pour remplir leurs fonctions » comme nécessitant l'application du privacy by design.

- Articles 35, 36 (Analyse d'impact relative à la protection des données) ; une grande partie de ce qui précède conduit à relever l'importance des AIPD dans ce domaine. Potentiellement, les systèmes d'IA et d'apprentissage automatique peuvent être davantage susceptibles de nécessiter la réalisation d'une AIPD que les systèmes de traitement plus traditionnels. Il y a ici une convergence avec le règlement IA lorsque les systèmes présentent un « risque élevé » (bien qu'il faille noter que la signification de « risque élevé » est différente dans chaque cas), dans ce cas, l'article 36, paragraphe 1, exige une consultation préalable avec les autorités de contrôle, ce qui implique que ces autorités disposent de capacités techniques appropriées dans ce domaine.

# 5. Si le RGPD réglemente déjà l'IA et l'apprentissage automatique, alors… pourquoi avons-nous également besoin du règlement IA ?

Si le RGPD et le règlement sur l'intelligence artificielle de l'UE (AI Act) présentent des similitudes, dans la mesure où ils envisagent tous deux des régimes de responsabilité, de gouvernance et de contrôle, il est important de reconnaître d'abord que, dans le seul contexte de l'IA et de l'apprentissage automatique, ils répondent à des objectifs réglementaires distincts. D'une part, le RGPD, qui concerne principalement la protection des données à caractère personnel, est technologiquement agnostique et ne fait pas explicitement référence à des applications technologiques spécifiques (y compris l'IA ou l'apprentissage automatique). D'autre part, le règlement IA représente une approche plus directe et concrète de la réglementation de l'IA et cherche à établir un cadre réglementaire complet pour promouvoir le développement et l'utilisation responsables de l'IA et des systèmes basés sur l'apprentissage automatique dans l'UE.

Le RGPD reconnaît que certaines opérations de traitement ont une incidence sur l'exercice des droits et libertés fondamentaux, à savoir les droits à la vie privée et à la protection des données, dans la mesure où ces types d'activités de traitement peuvent impliquer l'utilisation de données à caractère personnel des citoyens de l'UE. Étant donné que le RGPD s'applique essentiellement à tous les traitements de données à caractère personnel, chaque fois qu'un système d'IA ou d'apprentissage automatique implique un traitement de données à caractère personnel, alors le RGPD s'applique à ces technologies. À première vue, cette approche est relativement simple, cependant, il y a des nuances à prendre en compte. Tout d'abord, tous les systèmes d'IA ou d'apprentissage automatique n'impliquent pas le traitement de données à caractère personnel, de sorte que dans ces circonstances, le RGPD ne s'applique pas. En outre, l'article 2, paragraphe 2, du RGPD prévoit que l'utilisation d'un système d'IA ou d'apprentissage automatique dans certaines circonstances est également exclue (qu'il traite ou non des données à caractère personnel).

Étant donné que toutes les applications d'IA et d'apprentissage automatique ne donneront pas lieu à une activité impliquant un traitement de données à caractère personnel, le règlement IA reconnaît que l'utilisation et le déploiement de systèmes d'IA et d'apprentissage automatique représentent un domaine de préoccupation éthique et sociétale plus large qui échappera en souvent au champ d'application du RGPD. Par exemple, certaines pratiques utilisant des techniques basées sur l'IA ou l'apprentissage automatique pourraient entraîner la perpétuation de préjugés culturels ou de pratiques discriminatoires, ou poser des risques de sûreté et de sécurité en temps réel. Le RGPD pourrait tout simplement être peu pertinent ou peu applicable dans ces circonstances. Ainsi, compte tenu de ses limites dans le traitement de domaines plus vastes qui ne relèvent pas de la protection de la vie privée et des données, le règlement IA

s'engage à élaborer un cadre complet et technologiquement adapté qui complétera invariablement le RGPD dans ses efforts pour promouvoir une innovation responsable en matière d'IA en Europe, tout en respectant les droits et les valeurs fondamentaux de l'Union.

# 6. Comment certains des principes fondamentaux de la protection des données s'appliquent-ils à l'IA et à l'apprentissage automatique ?

Comme indiqué précédemment, chaque fois que des données à caractère personnel sont traitées par des systèmes d'IA/d'apprentissage automatique, le RGPD s'applique de manière générale à cette activité et, par conséquent, tous les principes fondamentaux de la protection des données s'appliquent nécessairement. Toutefois, certains principes fondamentaux du RGPD sont particulièrement adaptés et applicables aux contextes de l'IA et de l'apprentissage automatique. Dans ces cas, il y a un fort chevauchement entre la protection des données et la gouvernance de l'IA.

Premièrement, le principe fondamental de transparence, tel qu'il est consacré par l'article 12 du RGPD, est important pour la gouvernance des systèmes d'IA/d'apprentissage automatique. Dans bon nombre de ces systèmes, il n'est pas toujours évident pour les personnes concernées que leurs données sont traitées, en arrière-plan, au moyen de ces technologies. Par ailleurs le fonctionnement de ces systèmes n'est pas non plus intelligible pour les personnes concernées. À cet égard, les DPO doivent être conscients des obligations de transparence du RGPD et du règlement IA, qui exigent toutes deux à leur façon la transparence vis-à-vis des personnes.

Le RGPD impose une obligation générale de transparence en cas de traitement automatisé. L'article 12 dispose que le responsable de traitement prend des mesures appropriées pour fournir à la personne concernée, toute information relative au traitement d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. Par exemple, si l'utilisation proposée par votre organisation d'un système d'IA nécessite l'utilisation de données à caractère personnel collectées directement auprès des personnes pour entrainer un modèle, vous devez d'abord vous demander si vous avez respecté l'obligation de transparence prévue par le RGPD et informer les personnes concernées de la manière dont leurs données seront utilisées au cours du cycle de vie de votre système d'IA.

Le règlement IA complète toutefois cette exigence générale en imposant un certain nombre d'exigences spécifiques en matière de transparence. En particulier, l'article 52 impose des obligations en ce qui concerne la création de ce que l'on appelle les « deep fakes », qui sont

basés sur la technologie de l'IA et de l'apprentissage automatique. L'article 52, paragraphe 1, dispose que : « Les fournisseurs veillent à ce que les systèmes d'IA destinés à interagir avec des personnes physiques soient conçus et développés de manière à ce que les personnes physiques soient informées qu'elles interagissent avec un système d'IA, sauf si cela ressort clairement des circonstances et du contexte d'utilisation ».

Un autre principe où la protection des données et la gouvernance de l'IA se recoupent est celui de la loyauté. L'article 5, paragraphe 1, point a), du RGPD crée une obligation de grande envergure selon laquelle les données à caractère personnel doivent être « traitées de manière [...] loyale ». Le principe de loyauté est volontairement adaptable, destiné à saisir la multitude de façons dont une entité peut traiter de manière déloyale les données personnelles. Toutefois, dans le contexte de l'IA et de l'apprentissage automatique, la loyauté tend à avoir une application plus précise. Par exemple, si, en tant que DPO, vous examinez la loyauté d'une application d'IA/d'apprentissage automatique, vous serez préoccupé par le risque de partialité et/ou de discrimination dans les algorithmes utilisés. Il peut s'agir de préjugés raciaux, lorsque les données d'apprentissage elles-mêmes sont biaisées à l'encontre d'une race particulière, ou de préjugés sexistes, lorsqu'un sexe est affecté de manière disproportionnée. Ces cas constituent un traitement déloyal des données à caractère personnel.

Enfin, le principe d'explicabilité, un terme de gouvernance de l'IA qui signifie qu'une décision prise par un algorithme d'IA/d'apprentissage automatique peut être expliquée en termes lisibles par l'homme, a également son analogue dans le RGPD. En termes de gouvernance de l'IA, l'exigence d'explicabilité, dans la mesure où elle est réalisable, requiert des parties responsables qu'elles décrivent les liens de causalité entre les données d'entrée et les décisions finales. Or l'article 14, paragraphe 2, point g) du RGPD, énonce clairement cette exigence dans lors de l'existence d'une prise de décision automatisée, y compris le profilage, en précisant que « des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement » doivent être mises à la disposition des personnes concernées.

## 7. IA et apprentissage automatique ! C'est la même chose, non ?

L'IA et l'apprentissage automatique sont deux domaines étroitement liés mais distincts de l'informatique.

L'IA fait référence au concept plus large de la création de machines capables d'effectuer des tâches qui nécessiteraient normalement l'intelligence humaine. Cela peut inclure une série de technologies, telles que le traitement du langage naturel, la robotique, la vision par ordinateur, etc. L'objectif de l'IA est de créer des systèmes capables d'accomplir des tâches qui requièrent

généralement l'intelligence humaine, telles que la reconnaissance d'images ou la compréhension du langage naturel, et de prendre des décisions. Le niveau de capacité d'un système d'IA dépend du niveau et de la complexité du système. La création d'un système d'IA implique le développement d'algorithmes et de systèmes capables de raisonner, d'apprendre et de prendre des décisions sur la base de données d'entrée.

L'apprentissage automatique, quant à lui, est un sous-ensemble de l'IA qui se concentre sur le développement d'algorithmes capables d'apprendre et de s'améliorer au fil du temps. Essentiellement, l'apprentissage automatique consiste à enseigner aux machines à apprendre à partir de données sans être explicitement programmées. Par essence, l'apprentissage automatique est le processus qui consiste à former un ordinateur à reconnaître des modèles et à faire des prédictions sur la base de grandes quantités de données. Il peut s'agir d'un apprentissage supervisé, d'un apprentissage non supervisé ou d'un apprentissage semi-supervisé. L'apprentissage supervisé consiste à entrainer un algorithme avec des données étiquetées, ce qui signifie que la sortie correcte pour une entrée donnée est fournie. L'algorithme apprend à faire correspondre les entrées aux sorties sur la base des exemples étiquetés qui lui ont été fournis. L'apprentissage non supervisé, quant à lui, implique l'entrainement d'un algorithme sur des données non étiquetées, et l'algorithme doit trouver des modèles et des structures dans les données par lui-même. L'apprentissage semi-supervisé est une combinaison de l'apprentissage supervisé et non supervisé, où certaines données étiquetées sont fournies, mais où l'algorithme doit également apprendre à partir de données non étiquetées.

En résumé, l'IA est un concept plus large qui englobe une série de technologies, tandis que l'apprentissage automatique est un sous-ensemble spécifique de l'IA qui se concentre sur le développement d'algorithmes capables d'apprendre et de s'améliorer au fil du temps.

## 8. Je suis DPO. Dois-je m'inquiéter de la croissance de l'IA et de l'apprentissage automatique ?

En tant que DPO, vous devriez en effet vous préoccuper de la croissance de l'IA et de l'apprentissage automatique, car ces technologies peuvent conduire à une prise de décision automatisée qui peut potentiellement avoir de graves implications pour les droits et libertés des personnes concernées. Par exemple, l'IA peut être utilisée pour prendre des décisions automatisées concernant la présélection des candidats à l'emploi. Comprendre le fonctionnement des algorithmes vous permet d'identifier les risques potentiels en matière de protection des données et de mettre en œuvre, le cas échéant, des mesures de protection appropriées.

Quelle que soit la taille de votre organisation, en tant que DPO, vous allez être affecté par l'intégration de l'IA et de l'apprentissage automatique dans les systèmes informatiques de votre organisation. Par exemple, les applications suivantes les utilisent déjà ou prévoient de les utiliser prochainement :

- Microsoft Office prévoit d'intégrer l'IA et l'apprentissage automatique dès cette année, en 2023 ;
- De nombreux systèmes de RH, de paie, de vente et/ou de codage utilisent déjà l'IA et l'apprentissage automatique, et ceux qui ne le font pas prévoient d'intégrer ces technologies dans un avenir proche ;
- Les chatbots qui utilisent les données personnelles des entreprises et des clients pour fournir des réponses personnalisées sont déjà utilisés dans de nombreuses organisations et leur utilisation ne fera que croître à l'avenir.

En tant que DPO, vous et votre équipe devrez mener des analyses d'impact relatives à la protection des données (AIPD) pour toutes les nouvelles activités de traitement de données. Ce faisant, il est essentiel de comprendre les implications et les limites du système d'IA, en particulier en ce qui concerne les biais qui pourraient exister. La possibilité que l'IA génère des résultats inexacts doit également être prise en compte.

En outre, comme nous l'avons déjà souligné dans les questions précédentes, dans un avenir proche, les organisations qui développent leurs propres systèmes d'IA à haut risque devront non seulement respecter le RGPD, mais aussi le règlement IA. Des exemples de ces systèmes à haut risque peuvent être trouvés dans les scénarios suivants :

- l'éducation ou la formation professionnelle ;
- pour le recrutement, l'évaluation ou la répartition des tâches des employés ;
- l'évaluation de la solvabilité des personnes ;
- déterminer l'éligibilité des individus aux services et prestations sociales.

En tant que DPO travaillant pour une organisation qui met en œuvre des systèmes d'IA, vous devez jouer un rôle dans la procédure de gestion des risques liés à l'IA. Le RGPD exigeant la mise en œuvre de la protection des données dès la conception et par défaut, le DPO est chargé d'identifier, de réduire ou d'atténuer les risques connus et prévisibles par une conception et un développement adéquats de tout système d'IA qui traite des données à caractère personnel.

## 9. J'ai entendu parler de ChatGPT et d'IA générative. En tant que DPO, dois-je m'inquiéter ?

ChatGPT est actuellement le modèle d'IA générative (ou Gen-AI) le plus utilisé au monde, avec plus de 100 millions d'utilisateurs deux mois seulement après son lancement. L'IA générative est une catégorie d'intelligence artificielle capable de créer une grande variété de contenus ou de données, tels que des images, des vidéos, du son, du texte et des modèles 3D. Comme pour les autres formes d'IA, la Gen-AI est entraînée sur de grandes quantités de données (par exemple, récoltées sur des sites web). Un cas d'utilisation typique consiste à fournir des données d'entrée et une demande ou un prompt, qui guide ensuite la technologie Gen-AI pour créer une réponse. La réponse peut être de n'importe quelle forme de données.

Les autorités de contrôle de la protection des données en Europe ont exprimé un certain nombre de préoccupations concernant le traitement des données personnelles par ChatGPT. L'Agence espagnole de protection des données (AEPD) a déclaré début avril 2023, qu'elle avait ouvert une enquête sur OpenAI, l'entreprise à l'origine de ChatGPT, afin d'examiner « une possible violation de la réglementation » sur la protection des données en Espagne.

La décision de l'AEPD d'enquêter sur ChatGPT fait suite à une décision similaire prise fin mars 2023 par l'autorité italienne de protection des données (Garante per la protezione dei dati personali) de bloquer temporairement le chatbot en Italie en raison de préoccupations concernant son utilisation des données personnelles appartenant à des citoyens italiens.

L'autorité italienne de protection des données a déclaré qu'il n'existait aucune base juridique pour justifier « la collecte et le stockage massifs de données personnelles dans le but d'entraîner les algorithmes qui sous-tendent le fonctionnement de la plateforme ». L'autorité a également affirmé qu'étant donné qu'il n'y avait aucun moyen de vérifier l'âge des utilisateurs, l'application « expose les mineurs à des réponses absolument inadaptées par rapport à leur degré de développement et de conscience ».

L'autorité italienne de protection des données a ensuite retiré son blocage de l'application ChatGPT à condition qu'OpenAI adopte une série de mesures visant à protéger les droits et libertés des personnes italiennes concernées, notamment :

- La fourniture d'informations adéquates sur les droits accordés aux personnes concernées, qu'elles soient utilisatrices ou non de ChatGPT, ainsi que des détails sur la manière dont les données sont traitées par l'application.
- Démontrer le consentement explicite des personnes concernées ou identifier l'intérêt légitime du responsable du traitement comme base juridique du traitement des données.
- Mise en place d'un système de vérification de l'âge des utilisateurs.
- Mise en place de mesures techniques et organisationnelles pour l'exercice des droits des personnes concernées, y compris ceux de rectification, de suppression ou d'opposition au traitement des données à caractère personnel.

En outre, ChatGPT est déjà inaccessible dans plusieurs pays en dehors de l'Europe, dont la Chine, l'Iran, la Corée du Nord et la Russie.

En raison de ces réactions rapides face à cette nouvelle technologie, les DPO doivent être vigilants et jouer un rôle dans le contrôle et la sensibilisation aux risques que pose cette technologie, en particulier son utilisation non réglementée et potentiellement imprudente de en ce qui concerne la protection des données à caractère personnel des personnes concernées. Les données saisies par les utilisateurs dans ChatGPT peuvent inclure des données personnelles, sensibles notamment biométriques, encadrées par le RGPD, tandis que d'autres formes de données peuvent inclure des données confidentielles ou relevant de la propriété intellectuelle, régies par des politiques organisationnelles et/ou d'autres législations.

L'une des principales responsabilités du DPO en ce qui concerne cette technologie est donc de promouvoir une approche éclairée de la conception, du développement et de l'utilisation de ces systèmes d'IA génératives. Une série de contrôles techniques et de gouvernance sont également possibles pour permettre aux DPO de s'assurer de l'utilisation appropriée des services d'IA générative au sein de leur organisation :

- Les politiques de protection des données et de sécurité de l'information peuvent nécessiter des ajouts et des mises à jour.
- La prévention de la perte de données (DLP) et les outils connexes peuvent être configurés pour bloquer ou limiter le partage de données avec des services Gen-AI ou des domaines internet.
- Les programmes de sensibilisation et de formation sont également appropriés, car la prolifération des services de l'IA générative et des canaux permettant de les utiliser dépassera les moyens techniques de gouvernance.
- Les DPO ayant une portée internationale doivent également être conscients du statut juridique variable des services d'IA générative dans plusieurs pays, tant au sein de l'UE qu'à l'échelle mondiale.

Outre le partage non désiré de données, la Gen-AI augmente également le risque d'hameçonnage sophistiqué pour obtenir des données confidentielles, car elle permet l'automatisation des courriels et autres communications et documents qui ressemblent à ceux de l'organisation ou des individus.

## 10. D'accord, alors quelles sont les conversations clés que je devrais avoir en interne pour me préparer à l'émergence de l'IA et de l'apprentissage automatique ?

À l'avenir, les DPO devraient tendre la main et travailler en étroite collaboration avec d'autres parties prenantes au sein de leur organisation, telles que les data scientists, les professionnels de l'informatique, les experts juridiques et les cadres supérieurs, afin de former un réseau de relais de l'IA (similaire à un réseau de relais DPO). Ce réseau de relais veillera à ce que

l'utilisation des technologies et des systèmes d'IA dans l'organisation soit transparente, responsable et équitable et, surtout, à ce que l'utilisation de l'IA soit conforme au RGPD.

Voici quelques mesures que les DPO et leur réseau de relais peuvent prendre pour se préparer à l'augmentation des systèmes d'IA dans leur organisation :

1. Comprendre la technologie de l'IA : Les DPO doivent avoir une bonne compréhension de la technologie d'IA utilisée dans leur organisation. Cette compréhension est facilitée par la collaboration avec le réseau de relais pour comprendre les technologies d'IA spécifiques à chaque département, y compris leur fonctionnement, les données qu'elles collectent et traitent dans chaque département, et les types de décisions que les systèmes d'IA sont capables de prendre.
2. Spécifier et documenter clairement les finalités du traitement des données liées au système d'IA : cela est particulièrement important lors de la phase de conception et de développement du nouveau système d'IA afin de garantir la validation des principes clés du RGPD tels que la minimisation des données et le respect de la vie privée dès la conception et par défaut, ainsi que lors du déploiement du système d'IA auprès des utilisateurs finaux, en particulier dans les systèmes d'IA qui traitent des catégories particulières de données telles que les données de santé.
3. Réaliser des analyses d'impact relatives à la protection des données (AIPD) : la réalisation d'une AIPD est un processus qui aide les personnes à identifier et à minimiser les risques liés à la protection des données dans le cadre d'un projet. Les évaluations d'impact sur la protection des données doivent être menées chaque fois qu'un projet est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes concernées, conformément à l'article 35 du RGPD. Les DPO doivent travailler en collaboration avec le réseau de relais et les différents services de l'organisation pour réaliser des AIPD afin d'évaluer les risques associés aux systèmes d'IA dans chaque département de l'organisation et d'identifier tout impact potentiel sur les droits à la vie privée et à la protection des données des individus. Un élément clé d'une AIPD pour les systèmes d'IA consiste à vérifier que l'algorithme n'est pas biaisé, ce qui pourrait conduire à une discrimination.
4. Examiner les accords de traitement des données : Les DPO doivent examiner les accords de traitement des données conclus avec des fournisseurs d'IA tiers afin de s'assurer qu'ils prévoient des garanties appropriées pour le traitement des données à caractère personnel par les systèmes d'IA.
5. Mettre en œuvre des mesures de sécurité appropriées : Les DPO doivent veiller à ce que des mesures de sécurité appropriées soient mises en place pour protéger les données à caractère personnel contre l'accès non autorisé, la perte ou la destruction lors de l'utilisation de systèmes d'IA.

6. Contrôler et auditer les systèmes d'IA : Les DPO doivent contrôler et auditer régulièrement les systèmes d'IA afin de s'assurer qu'ils fonctionnent comme prévu et que les risques liés à la protection des données sont gérés efficacement.