

RÉSOLUTION SUR L'INTELLIGENCE ARTIFICIELLE (y compris note explicative)

dans le contexte de l'emploi

(Traduction FR – la version anglaise fait foi)

Texte adopté : octobre 2023

45ème Conférence de l'Assemblée mondiale pour la protection des données et de la vie privée d'octobre 2023

Cette résolution est présentée par les autorités sponsors suivantes au nom du Groupe de travail sur l'éthique et la protection des données en intelligence artificielle.

Présentée par:

- Le Bureau du commissaire à l'information (ICO), Royaume-Uni
- Le Commissaire fédéral à la protection des données et à la liberté d'information (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit - BfDI), Allemagne
- L'Autorité de protection des données (Garante per la protezione dei Dati Personali - GPDP), Italie

Soutenue par:

- Le Préposé fédéral à la protection des données et à la transparence (PFPDT), Suisse
- La Commission Nationale de l'Informatique et des Libertés (CNIL), France
- L'Autorité de protection des données (URCDP), Uruguay
- L'Institut national pour la transparence, l'accès à l'information et la protection des données personnelles (INAI), Mexique
- La Commission d'accès à l'information du Québec, Canada
- Le Commissaire à l'information et à la protection de la vie privée de l'Ontario, Canada
- Le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, Canada
- Le Commissariat à la protection de la vie privée du Canada (OPC Canada)
- Le Conseil de l'Europe
- Le Bureau du commissaire à la protection des données personnelles (PCPD), Hong Kong, Chine
- La Commission Nationale de Contrôle de Protection des Données à Caractère Personnel, (CNDP), Maroc
- Le Contrôleur européen de la protection des données (EDPS)

La 45ème session annuelle à huis clos de l'Assemblée mondiale sur la protection de la vie privée :

Notant que les activités professionnelles peuvent impliquer la recherche et le recrutement de candidats, la conclusion d'un contrat de travail entre l'employeur et le salarié, le suivi et gestion de la performance, du développement et du comportement des salariés sur le lieu de travail par l'employeur et l'acte de mettre fin à une relation de travail, et qu'elles peuvent inclure le recrutement et la gestion des travailleurs des plateformes de travail numériques, des employés contractuels, des syndicats, ainsi que la prise en charge de la santé et la sécurité au travail et le respect des règles du travail et de la protection sociale ;

Rappelant [la Déclaration sur l'éthique et la protection des données dans l'intelligence artificielle faite par la 40^{ème} Conférence internationale des commissaires à la protection des données et de la vie privée, le 23 octobre 2018](#), et [la résolution sur la responsabilité dans le développement et l'utilisation de l'intelligence artificielle adoptée lors de la 42^{ème} séance à huis clos de la conférence GPA](#).

Reconnaissant les gains d'efficacité et les avantages potentiels que l'utilisation de l'intelligence artificielle (IA) peut apporter à la prise de décision tout au long du parcours professionnel, que les organisations explorent dans le cadre de diverses activités menées par les employeurs, incluant notamment la recherche et la sélection initiales des candidats potentiels, le suivi et la gestion des employés;

Soulignant que l'IA utilisée dans le contexte professionnel peut présenter un risque élevé pour les individus¹, les groupes, les représentants des travailleurs (tels que les syndicats), les communautés et les organisations. Lorsque cette utilisation est opaque, mal appliquée, mal conçue ou utilisée de manière inappropriée, elle peut entraîner des préjudices ou une atteinte aux droits et libertés fondamentaux, notamment à la vie privée, à la dignité humaine et à l'égalité des droits, comme la discrimination déloyale. Cela peut avoir un impact significatif sur le développement personnel et professionnel d'un travailleur et entraîner un déni d'égalité des chances d'accès à l'emploi en raison de l'utilisation de données historiques biaisées pour entraîner certains outils d'IA ou de l'utilisation de valeurs ou de paramètres inappropriés ou illégaux dans un système d'IA;

De plus, soulignant d'autres risques, tels que la collecte disproportionnée ou non autorisée de données personnelles pour prendre des décisions entièrement automatisées ou assistées par l'IA concernant la performance d'un employé ou la répartition du travail ou toute autre décision susceptible d'affecter les droits des personnes. Ces risques comprennent entre autres :

¹ L'évaluation des risques peut s'appuyer sur des outils tels que [le Cadre de gestion des risques liés à l'intelligence artificielle publié par l'Institut national américain des normes et de la technologie \(NIST\)](#) en début d'année, et [la norme ISO/CEI 23894:2023 : Lignes directrices sur la gestion des risques liés à l'IA](#), entre autres. Voir également [le rapport du Groupe de travail sur l'IA de l'Assemblée mondiale de la protection de la vie privée : Risques pour les droits et libertés des individus posés par les systèmes d'intelligence artificielle – Proposition de cadre général de gestion des risques](#)

- Des risques au droit au respect de la vie privée et familiale (par exemple, si des systèmes d'IA sont utilisés pour surveiller les télétravailleurs ou s'ils entraînent un micro-management excessif des employés et une surveillance sur le lieu de travail)
- des atteintes à la santé et au bien-être,
- des risques affectant la liberté de réunion et d'association (par exemple, si les données ou les déductions relatives à l'appartenance syndicale sont utilisées au détriment des employés ou des candidats),
- des risques affectant la capacité d'une personne à exercer son droit de ne pas faire l'objet d'une décision fondée exclusivement, ou partiellement, sur un processus décisionnel automatisé, ou à exercer d'autres droits individuels à la vie privée ou à la protection des données, et
- l'atteinte aux droits individuels à l'information et à la protection des données, par exemple en cas de manque de transparence, c'est-à-dire lorsque les candidats ou les employés ne sont pas informés de l'utilisation de l'IA et/ou de l'étendue de cette utilisation.

Renforçant l'importance de la transparence afin de garantir que les employés et les syndicats soient informés de l'utilisation des systèmes d'IA sur le lieu de travail avant leur mise en place, en fournissant suffisamment de détails pour leur permettre d'en comprendre la finalité, le fonctionnement et les indicateurs utilisés.

Soulignant que les systèmes d'IA utilisés par les organisations à des fins professionnelles doivent être explicables de manière compréhensible pour les personnes soumises aux décisions prises uniquement ou avec l'aide de ces systèmes, ainsi que pour celles qui les utilisent. Les organisations déployant de tels systèmes, au titre de leurs responsabilités et de leurs obligations en vertu du droit du travail, de la protection sociale, de la santé et de la sécurité au travail, doivent prévoir cette explicabilité et les mécanismes nécessaires, qui peuvent être détaillés dans une politique organisationnelle dédiée à l'utilisation de l'IA. Les employés, les candidats ou les travailleurs doivent pouvoir comprendre la logique du processus décisionnel grâce à ces mécanismes et politiques, ainsi que la possibilité de demander de l'aide et des réparations par exemple en cas de problèmes de discrimination, de partialité et d'opacité;

Notant que la plupart des applications d'IA développées ou déployées dans un contexte professionnel traiteront des données personnelles lors de leur développement ou de leur déploiement. Bien que les sources, la distribution et la nature des données traitées à ces différentes étapes puissent varier, toutes les phases de cette IA dans le parcours professionnel sont dans la plupart des cas tenues de prendre en compte la protection des données, le respect de la vie privée et les droits des travailleurs.

Préoccupés par les risques élevés que l'utilisation de l'IA dans le domaine de l'emploi peut engendrer en matière de protection des données et de respect de la vie privée, et qui

pourraient impacter, entre autres, le recrutement et le suivi des travailleurs. Ces risques peuvent inclure, entre autres :

- un manque de transparence
- la présence de pratiques discriminatoires fondés sur des biais
- le manque de réflexion sur la nécessité et la proportionnalité de l'utilisation de l'IA dans le contexte spécifique de l'emploi
- l'absence d'intervention humaine significative
- le manque de formation adéquate et d'expertise pertinente en matière d'utilisation des systèmes d'IA et de prise de décision à haut risque dans l'écosystème de l'emploi
- l'absence de base juridique valable générale ou spécifique à l'emploi
- la perte de contrôle des individus sur la collecte et le traitement de leurs données personnelles
- les difficultés rencontrées par les employés pour exercer leurs droits sur les données
- l'absence de garanties spécifiques
- une sécurité des données insuffisante
- le détournement d'usage
- le traitement de données sensibles telles que les données de santé ou biométriques sans respect du principe de proportionnalité ni de la dignité humaine

Soulignant que l'utilisation de systèmes d'IA pour déduire les émotions d'une personne physique² et plus généralement toute forme de « catégorisation biométrique», présente un risque élevé et devrait, dans la plupart des cas, être interdite dans le contexte professionnel. Si elle est utilisée dans des cas limités et définis, elle doit faire l'objet de garanties appropriées, notamment de tests rigoureux et/ou d'autres évaluations afin de garantir que ces systèmes utilisent des méthodologies valides et fiables et fonctionnent comme prévu;

Soulignant que, face au recours croissant des organisations des secteurs public et privé à l'IA dans le contexte de l'emploi, et à la possibilité de fournir des systèmes et services d'IA à distance et au-delà des frontières, il est essentiel que les autorités de protection des données et de la vie privée, de concert avec les autorités compétentes en matière de travail et de santé et sécurité au travail, comprennent l'origine des données d'entraînement des systèmes d'IA, la conformité de leur développement et de leur fonctionnement avec les cadres juridiques nationaux, ainsi que l'impact sur les droits des employés en matière de protection des données et de respect de la vie privée, tant au niveau national qu'international ;

Prenant en compte l'importante contribution des autorités de protection des données et de la vie privée, des gouvernements et des organismes internationaux au débat mondial, notamment par la publication de lois, de politiques et de documents d'orientation ;

² Par exemple, dans le cas des systèmes de reconnaissance des émotions utilisés sur un lieu de travail pour surveiller l'humeur des employés.

Reconnaissant que les différentes utilisations et applications de l'IA dans le domaine de l'emploi présentent des risques de nature et de niveau différents et nécessitent donc une attention particulière tout au long de leur déploiement et de leur cycle de vie afin d'identifier les garanties appropriées à chaque contexte et à chaque utilisation ;

Rappelant que l'Assemblée mondiale de la protection de la vie privée a déjà souligné la nécessité d'œuvrer à l'élaboration de politiques, de normes et de modèles mondiaux, et de renforcer la coopération réglementaire afin d'améliorer la prévention, la détection, la dissuasion et la résolution efficace des problèmes de protection des données et de respect de la vie privée, et d'assurer la cohérence et la prévisibilité du système de surveillance dans l'économie axée sur les données ;

Affirmant la nécessité pour les autorités chargées de la protection des données et des autorités chargées de l'application de la loi en matière de vie privée de coordonner leurs efforts, de concert avec les autorités compétentes du travail et de la santé et sécurité au travail, afin d'influencer l'élaboration et la mise en œuvre de ces approches en matière de protection des données et de respect de la vie privée à l'échelle mondiale, et de prendre des mesures le cas échéant ; et

Réaffirmant la Résolution sur la protection de la vie privée dès la conception adoptée par la 32^{ème} Conférence en 2010 à Jérusalem, la Résolution sur le profilage adoptée par la 35^{ème} Conférence en 2013 à Varsovie, la Résolution sur les mégadonnées (Big Data) adoptée par la 36^{ème} Conférence en 2014 à Fort Balaklava, la Déclaration sur l'éthique et la protection des données dans l'IA adoptée par la 40^{ème} Assemblée mondiale de la protection de la vie privée en 2018 à Bruxelles, et la Résolution sur la responsabilité dans le développement et l'utilisation de l'IA adoptée par la 42^{ème} Assemblée mondiale de la protection de la vie privée en 2020 (en ligne).

Par conséquent, la 45^{ème} Assemblée mondiale de la protection de la vie privée souligne l'importance des points suivants:

1. Garantir que l'utilisation des systèmes d'IA dans le contexte professionnel soit centrée sur l'humain.
2. Les principes de protection des données et de respect de la vie privée dès la conception et par défaut lors du développement d'outils d'IA destinés à être déployés dans le contexte professionnel, notamment pour les salariés, les travailleurs contractuels, les travailleurs syndiqués, les travailleurs journaliers et les travailleurs des plateformes de travail numériques, en tenant compte de l'impact que les systèmes d'IA peuvent avoir sur leur vie personnelle et professionnelle.
3. Reconnaître l'importance de disposer d'une base juridique adéquate pour le traitement des données personnelles à toutes les étapes du cycle de vie de l'IA, ainsi que les limites du

consentement comme base légale dans le contexte professionnel, compte tenu des déséquilibres de pouvoir potentiels entre un candidat ou un salarié et un employeur.

4. Préciser les garanties adéquates pour éviter une surveillance disproportionnée des travailleurs, portant atteinte à leur vie privée et à leur dignité, lors du traitement de leurs données personnelles à des fins professionnelles pertinentes, y compris la participation des syndicats aux décisions relatives à la gestion du travail par l'IA.

5. La nécessité d'assurer la pleine conformité du développement et du déploiement des systèmes d'IA dans le domaine de l'emploi avec les lois et principes applicables en matière de protection des données, tels que la nécessité, la proportionnalité, la minimisation des données, la spécification et la limitation des finalités, et le droit de ne pas faire l'objet d'une décision fondée exclusivement ou principalement sur des traitements automatisés, ainsi qu'avec la réglementation du travail applicable et toute autre réglementation, telle que les cadres établis en matière de droits de l'homme, qui peuvent être pertinents dans un contexte spécifique, notamment, les principes mentionnés dans la présente résolution ;

6. Licéité, équité et transparence du traitement des données personnelles, notamment : le développement, le déploiement et les résultats des traitements liés à l'IA. Ceci implique, entre autres, l'obligation pour l'employeur de fournir aux salariés – faisant l'objet d'une décision assistée par l'IA, lorsque des algorithmes ou des systèmes d'IA sont déployés dans le contexte de l'emploi, au regard des cadres réglementaires spécifiques à chaque juridiction – et aux syndicats, avant tout déploiement de systèmes d'IA, des informations détaillées sur l'utilisation et le fonctionnement de ces systèmes qui déterminent. Ceci inclut par exemple, le classement, l'attribution des tâches, la gestion ou le licenciement d'un candidat ou d'un salarié, ainsi que la supervision, l'évaluation et l'exécution des obligations contractuelles du salarié, sans préjudice des droits des travailleurs, par exemple recevoir des informations relatives à l'emploi, contester et obtenir réparation en cas d'évaluation illégale des performances, de paiement insuffisant ou de licenciement abusif;

7. Le droit d'un candidat ou d'un employé faisant l'objet d'une décision assistée par l'IA d'accéder aux informations concernant les données détenues à son sujet par un employeur et la manière dont ses données personnelles sont utilisées dans le cadre d'une telle décision assistée par l'IA, ainsi qu'aux informations concernant les données déduites et les profils établis à l'aide de ces systèmes d'IA.

8. L'explicabilité du système d'IA utilisé à chaque étape du parcours professionnel afin de garantir que : les salariés, candidats ou travailleurs concernés par les résultats de ce système, ainsi que les employeurs déployant le système d'IA, comprennent la décision prise par ce dernier et puissent accéder à cette explication de manière simple et rapide; et que l'explication fournie aux salariés, candidats ou travailleurs comprenne des informations intelligibles sur la logique sous-jacente, la signification et les conséquences envisagées de l'utilisation du système d'IA, tant en général que dans le cas particulier du salarié, afin de

leur permettre de déposer des réclamations éclairées et d'exercer leur droit à réparation conformément au cadre juridique national applicable;

9. La possibilité pour la personne concernée par un système d'IA utilisé par un employeur à n'importe quelle étape du parcours professionnel d'obtenir un examen humain significatif et documenté des décisions prises à l'aide de systèmes d'IA, d'exprimer son point de vue et de contester les décisions automatisées ou fondées sur l'IA pertinentes, ou de demander un audit indépendant du système d'IA utilisé par l'employeur ou toute exigence générale d'audit par un tiers ;

10. La formation des utilisateurs d'outils d'IA, y compris ceux qui effectuent un examen humain des décisions assistées par l'IA, afin de garantir que ces décisions ne soient pas sujettes à des biais d'automatisation qui pourraient conduire à une confiance excessive dans les outils d'IA, et que les utilisateurs d'outils d'IA possèdent l'expertise, l'expérience et les qualifications techniques requises, prennent en compte les niveaux de risque que la tâche soit influencée par le résultat du système d'IA, et le suivi ou la surveillance de l'utilisation des outils d'IA afin de déterminer si cette formation est efficace.

11. Le principe de responsabilité exige que les organisations et les employeurs prennent en compte, atténuent et, le cas échéant, préviennent les risques pour les droits et libertés des candidats, des employés et des travailleurs découlant de l'utilisation de l'IA pour le traitement des données personnelles (par exemple, le droit d'association et de se syndiquer, qui peuvent être entravés par une surveillance excessive des activités des travailleurs), et qu'ils démontrent qu'ils ont agi en ce sens ;

12. Des politiques organisationnelles qui soutiennent les évaluations d'impact de l'IA avant son déploiement, en tenant compte de tous les risques raisonnablement prévisibles pour les candidats, les employés et les travailleurs découlant de l'utilisation du système d'IA sur le lieu de travail, l'accréditation ou la certification des systèmes d'IA, l'identification des risques spécifiques à l'IA et définissent les mécanismes de signalement et de recours pour les systèmes d'IA utilisés pendant le parcours professionnel , également comme moyen de faciliter le contrôle par les autorités compétentes;

13. Réduire et atténuer les biais ou la discrimination, directs et indirects, lors du développement et du déploiement d'un système d'IA dans le contexte de l'emploi, notamment en prenant des mesures raisonnables pour garantir que les données personnelles utilisées dans l'apprentissage du système et dans la prise de décision entièrement automatisée sont représentatives du contexte dans lequel le système sera utilisé, exactes et régulièrement mises à jour, et en mettant en œuvre des mesures techniques et organisationnelles appropriées pour garantir, en particulier, que les facteurs des systèmes de recrutement et de gestion du travail qui entraînent des inexactitudes dans les données personnelles soient corrigés et que le risque d'erreurs soit minimisé, ainsi que le respect des lois nationales applicables ; et

La 45^{ème} Assemblée mondiale de la protection de la vie privée s'engage à prendre les mesures suivantes :

1. Inciter les organisations qui développent ou utilisent des systèmes d'IA dans le contexte de l'emploi à prendre en compte les considérations énoncées dans la présente résolution ;
2. Inviter tous les membres de l'Assemblée mondiale de la protection de la vie privée à collaborer avec les organisations qui développent ou utilisent des systèmes d'IA dans le contexte de l'emploi, tant au niveau national qu'international, afin de les aider à intégrer les considérations énoncées dans la présente résolution ;
3. Mettre à jour, le cas échéant, les résultats de l'enquête du Groupe de travail sur l'éthique et la protection des données en matière d'intelligence artificielle (voir le rapport d'enquête dans la note explicative ci-dessous) en cas d'évolution du cadre juridique ou technique de l'utilisation de l'IA dans le domaine de l'emploi.

NOTE EXPLICATIVE

LE GROUPE DE TRAVAIL SUR L'ÉTHIQUE ET LA PROTECTION DES DONNÉES DANS LE DOMAINE DE L'INTELLIGENCE ARTIFICIELLE DE L'ASSEMBLÉE MONDIALE DE LA PROTECTION DE LA VIE PRIVÉE (GPA, « Global Privacy Assembly ») a mené une enquête de mai à juillet 2022 afin de recueillir l'avis des membres de l'Assemblée sur les principaux risques et les mesures d'application prises par ces derniers concernant l'utilisation de l'IA dans le milieu professionnel. Le rapport est disponible ci-dessous.

1. Introduction

Ces dernières années ont vu une prolifération de l'utilisation de l'intelligence artificielle (IA) dans le monde du travail, notamment pour le recrutement, au sein de l'entreprise et après l'embauche. L'IA est un terme générique désignant un ensemble de technologies et d'approches qui tentent souvent d'imiter la pensée humaine pour résoudre des tâches complexes³.

Le terme « IA » est souvent employé sans définition précise pour désigner tous types d'outils algorithmiques disponibles sur le marché, ce qui peut mener à une instrumentalisation trompeuse de l'IA. Du point de vue de la protection des données, il est essentiel de distinguer la phase de conception ou d'apprentissage de la phase d'application ou de déploiement de l'IA dans le contexte professionnel. La plupart des applications d'IA dans ce contexte utilisent des données personnelles lors des deux phases, ce qui implique l'application des principes de protection des données et de respect de la vie privée. Ces principes concernent notamment la transparence, dont l'exactitude des données relatives aux employés, aux travailleurs et aux candidats ; les questions au sujet du respect des droits des personnes concernées et les garanties appropriées ainsi que les questions de présence de biais et de discrimination ; les fondements juridiques ou le degré d'intervention humaine significative ; ainsi que la proportionnalité, la confiance et l'équité.

En 2018, il a été révélé qu'Amazon avait abandonné un outil de recrutement basé sur l'intelligence artificielle après avoir constaté des biais sexistes. Cet outil, conçu pour évaluer les candidatures, pénalisait celles contenant le mot « femmes », comme dans « capitaine du club d'échecs pour femmes », et sous-évaluait les diplômées de deux établissements d'enseignement supérieur exclusivement féminins. Ce fut l'un des premiers cas médiatisés démontrant que l'intelligence artificielle était non seulement utilisée pour prendre des décisions importantes en matière d'emploi, mais aussi qu'elle causait un préjudice injustifié à des individus.

³ [Part 1 The basics of explaining AI | ICO](#) – L'ensemble des lignes directrices sur l'explication de l'IA, y compris sur les bases de l'explication de l'IA, qui se trouve sur le site web du Bureau du commissaire à l'information (ICO), Royaume-Uni

Depuis, d'autres affaires retentissantes ont fait état de l'utilisation de l'IA dans le contexte professionnel, entraînant des préjudices potentiels pour les individus. En voici quelques exemples :

- Une décision de justice néerlandaise portant sur la question de savoir si la désactivation des licences de certains chauffeurs Uber constituait une décision exclusivement automatisée ayant des effets juridiques ou des effets similaires significatifs au sens de l'article 22 du RGPD et si des informations pertinentes concernant la logique ayant conduit à cette décision avaient été fournies aux chauffeurs⁴.
- L'Autorité de protection des données (Garante per la protezione dei Dati Personali - GPDP), a infligé des amendes aux entreprises de livraison de repas pour non-respect des principes de protection des données (transparence, sécurité, respect de la vie privée dès la conception et par défaut) et pour défaut de mise en œuvre de mesures adéquates visant à protéger les droits et libertés de leurs employés contre les discriminations liées à la prise de décision automatisée lors de l'utilisation d'un système de notation automatisé pour l'attribution des créneaux de livraison aux livreurs. Ce système a privé certains livreurs d'opportunités de travail⁵.

Les législateurs et les autorités de réglementation ont commencé à se pencher sur les risques potentiels liés à l'utilisation de l'IA dans le contexte de l'emploi. Par exemple, la Commission européenne a proposé de considérer l'utilisation de l'IA pour le recrutement ainsi que pour les décisions relatives à la performance au travail et à la répartition des tâches comme présentant un risque élevé ; par ailleurs, une proposition concernant les travailleurs des plateformes numériques est en cours de négociation⁶.

Cela signifie que les employeurs devront se conformer à des exigences supplémentaires en vertu de la loi sur l'IA, par rapport aux autres utilisateurs de systèmes d'IA considérés comme ne présentant pas de haut risque. Le Bureau du commissaire à l'information (ICO), l'autorité de protection des données du Royaume-Uni, s'est engagé à enquêter sur les préoccupations liées à l'utilisation d'algorithmes pour le tri des candidatures, ce qui pourrait nuire aux perspectives d'emploi des personnes issues de la diversité. De nombreuses applications de l'IA utilisées dans le contexte professionnel auront des conséquences sur la protection des données et le respect de la vie privée. Par exemple :

⁴ [Décisions de justice néerlandaises font jurisprudence en matière de droits des travailleurs indépendants sur leurs données](#) | Financial Times (ft.com)

⁵ Voir le résumé de l'ordonnance de l'autorité italienne de protection des données à l'adresse [Abstract of Italian SA's order as issued against Foodinho S.r.l. - Garante Privacy](#) ; Une autre décision est publiée à l'adresse : [Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l. - 22 luglio... - Garante Privacy](#)

⁶ [Travailleurs des plateformes numériques : les règles de l'UE se rapprochent](#) (europa.eu)

- Une décision prise par une IA concernant la réussite ou l'échec des candidats à un emploi sera-t-elle explicable aux personnes concernées ?
- Un système d'IA conçu dans un but précis (par exemple, accroître la sécurité des employés sur leur lieu de travail) sera-t-il utilisé à des fins différentes et incompatibles (par exemple, évaluer la productivité des travailleurs) ?
- La décision d'un système d'IA de licencier un employé peut-elle être considérée comme juste ?

En 2022, l'Assemblée mondiale de la protection de la vie privée (GPA), emmenée par l'ICO et l'agence allemande BfDI, a mené une enquête auprès de ses membres afin de comprendre les perspectives mondiales sur les implications de l'IA en matière de protection des données et de respect de la vie privée dans le contexte professionnel. Les objectifs de cette enquête étaient les suivants :

- Identifier les principaux enjeux politiques et juridiques liés au développement et à l'utilisation de l'IA dans le contexte de l'emploi, y compris le recrutement, qui sont importants pour les autorités de protection des données et de la vie privée dans le monde entier.
- Constituer et maintenir un répertoire international de cas concrets d'application de la technologie de l'IA sur le lieu de travail, pertinents pour la prise en compte de la vie privée, de la protection des données et de l'éthique de l'IA de manière plus générale.
- Éclairer l'élaboration et la promotion d'un ensemble de principes et d'attentes concernant l'utilisation de l'IA et des informations personnelles sur le lieu de travail.
- Examiner et discuter les pistes d'action possibles.

L'enquête portait sur les positions et les lignes directrices actuelles des autorités de protection des données concernant l'utilisation des données personnelles et de l'IA au travail (question 1), sur les mesures d'exécution ou les enquêtes relatives à cette utilisation (question 2), sur le degré d'engagement des membres auprès des parties prenantes sur ce sujet et sur les finalités les plus risquées de l'IA au travail selon eux (questions 3 et 4), sur les principaux risques pour la vie privée et la protection des données selon ceux-ci (question 5), ainsi que sur les caractéristiques d'un cadre réglementaire efficace (question 6). Enfin, l'enquête demandait des exemples d'utilisation de l'IA au travail (question 7) et des informations sur ses impacts plus généraux (question 8).

L'enquête s'est déroulée du 11 au 25 mai 2022. Les questions ont été diffusées par courriel par le secrétariat de la GPA pour le Groupe de travail sur l'éthique et la protection des données en intelligence artificielle, accompagnées d'une note introductive. Afin de maximiser le nombre de réponses, l'enquête a été envoyée à l'ensemble des membres de la GPA, et non uniquement aux membres du Groupe de travail sur l'éthique et la protection des données en intelligence artificielle. Au total, 29 réponses de membres de la GPA ont été reçues. La majorité des réponses provenaient d'autorités basées en Europe (20/29), suivies

par l'Asie et l'Australie (6/29), l'Amérique du Nord (1/29) et l'Amérique centrale et du Sud (2/29).

2. Résultats

L'enquête a suscité des réponses variées de la part des autorités chargées de la protection des données et de la vie privée. Les questions posées et un résumé des réponses reçues sont présentés ci-dessous.

Question 1 : Votre autorité a-t-elle élaboré des prises de position ou des recommandations publiques concernant l'utilisation des données personnelles et de l'IA au travail ?

Huit personnes ont répondu « oui » à cette question. Les informations complémentaires fournies illustraient diverses publications. Par exemple, certaines portaient sur les risques généraux liés à l'utilisation de l'IA, d'autres sur les risques généraux associés au traitement des données personnelles en milieu professionnel, et enfin, plusieurs exemples portaient sur l'utilisation conjointe des données personnelles et de l'IA au travail. Une réponse, par exemple, soulignait les considérations à prendre en compte pour concilier le principe de minimisation des données et le principe d'équité lorsque la méthode de détection et de lutte contre la discrimination nécessite le traitement d'un plus grand nombre de données personnelles.

Question 2: Votre autorité, ou d'autres instances juridiques ou judiciaires de votre juridiction, a-t-elle enquêté ou pris des mesures réglementaires, coercitives ou juridiques formelles concernant l'utilisation des données personnelles et de l'IA sur le lieu de travail ?

Huit personnes interrogées ont répondu « oui » à cette question. Voici quelques exemples de problèmes évoqués dans ces réponses:

- Les enquêtes sur les entreprises de livraison de repas en ligne et leur utilisation de l'IA pour traiter les données personnelles des livreurs ;
- Le traitement des données personnelles des employés par des techniques avancées d'exploration de données afin d'identifier d'éventuels congés maladie injustifiés ;
- L'utilisation de la prise de décision algorithmique pour l'attribution des postes d'enseignants dans les écoles ;
- L'utilisation de l'analyse automatique de la voix et de l'image lors des entretiens vidéo dans le cadre d'une procédure de recrutement ;
- L'utilisation de la biométrie sur le lieu de travail ; et
- L'utilisation de l'IA pour analyser les données et prédire la probabilité qu'un candidat refuse une offre d'emploi.

Question 3 : Votre autorité a-t-elle collaboré avec des acteurs externes régionaux, nationaux ou internationaux pour élaborer ses positions et orientations politiques ou faire progresser la réglementation relative à l'utilisation de l'IA au travail (par exemple, l'industrie, les syndicats, la société civile, les législateurs) ?

Onze répondants ont répondu « oui ». Cette collaboration a notamment porté sur des instances internationales telles que le Comité ad hoc sur l'intelligence artificielle du Conseil de l'Europe, l'OCDE et le Partenariat mondial sur l'IA (GPAI), ainsi que sur d'autres autorités et organismes de réglementation nationaux, des entreprises et des organisations professionnelles, des instituts de recherche, des syndicats, la société civile et les ministères et services gouvernementaux nationaux.

Question 4 : Parmi les cas d'utilisation ci-dessous, lesquels présentent selon vous les risques les plus importants en matière de confidentialité et de protection des données ?

- **Le recrutement (ex. : extraction de CV, évaluations ludiques, entretiens automatisés, etc.)**
- **La gestion du travail (ex. : attribution des congés, gestion des absences, répartition des tâches et des horaires, etc.)**
- **La surveillance (ex. : vérification d'identité, systèmes de suivi, surveillance des postes de travail, etc.)**
- **Autre (veuillez préciser)**

Les personnes interrogées pouvaient choisir plusieurs réponses ; beaucoup en ont sélectionné deux ou trois, certaines une seule, et quelques-unes ont préféré ne pas répondre. Les autorités de protection des données ont considéré que l'utilisation de l'IA à des fins de surveillance présentait les risques les plus importants en matière de protection de la vie privée et des données, suivie de près par son utilisation à des fins de recrutement. Certaines personnes ayant sélectionné « Autre » ont estimé que les trois utilisations présentaient un niveau de risque similaire.

Par ailleurs, 14 répondants ont mentionné d'autres finalités et/ou ajouté des informations complémentaires à leur réponse. Ils ont notamment indiqué que les risques dépendaient de l'ampleur de l'atteinte aux droits et libertés des personnes concernées en matière de protection des données, plutôt que du contexte professionnel ou d'une finalité spécifique. Certains ont attribué un risque élevé à la surveillance permanente par les technologies de reconnaissance faciale par IA, en particulier concernant l'intégration de données sensibles telles que les données biométriques, notamment à des fins d'identification ou de profilage automatisé des employés. L'absence de preuves scientifiques étayant les affirmations et les promesses des vendeurs de ces outils, y compris les prédictions de personnalité et de performance des candidats non fondées sur des méthodes scientifiques rigoureuses, a suscité des inquiétudes. Souvent, les répondants ont constaté que les ensembles de données d'entraînement n'étaient pas obtenus et traités conformément à la réglementation

sur la protection des données. Ils ont également fait part de leurs préoccupations quant à la gouvernance et à la sécurité des bases de données utilisées comme sources des données collectées par l'IA. Par ailleurs, les personnes interrogées ont souligné qu'en plus d'une évaluation concrète des risques, il est indispensable de disposer d'une base juridique valable et de respecter les principes de protection des données (minimisation des données, transparence, équité/non-discrimination, proportionnalité de l'utilisation de l'IA au regard de la finalité précise, etc.). Elles ont également évoqué la nécessité de garanties spécifiques.

Question 5 : Pour le ou les cas d'utilisation identifiés à la question 4, veuillez sélectionner les trois risques les plus importants en matière de protection de la vie privée et des données.

- **Le manque de transparence concernant la collecte de données, notamment l'absence d'information des personnes concernées.**
- **La collecte à grande échelle de données sensibles.**
- **Les biais et la discrimination à l'encontre de certains groupes démographiques.**
- **La sécurité des données insuffisante, y compris les risques de violation de la confidentialité.**
- **La dérive fonctionnelle (utilisation d'un système d'IA au travail à des fins nouvelles et potentiellement moins justifiées).**
- **La perte de contrôle des personnes sur la collecte et le traitement de leurs données.**
- **L'absence de base juridique valable pour le traitement.**
- **Les difficultés rencontrées par les personnes concernées pour exercer leurs droits sur leurs données.**
- **L'absence de législation spécifique encadrant l'utilisation de l'IA au travail.**
- **L'absence de réflexion sur la nécessité et la proportionnalité de l'utilisation de l'IA au travail.**
- **L'absence d'intervention humaine significative pour les décisions ayant des conséquences juridiques ou similaires sur les personnes concernées.**
- **Les implications plus larges en matière de droits humains, telles que définies dans des instruments internationaux comme le Pacte international relatif aux droits économiques, sociaux et culturels ou dans le droit national, notamment le droit à la liberté de réunion et d'association.**
- **Autre (veuillez préciser).**

Le manque de transparence a été considéré par la plupart des autorités de protection des données comme le principal risque pour la protection des données et le respect de la vie privée (15 répondants). Viennent ensuite les biais et la discrimination (10 répondants), le manque de réflexion sur la nécessité et la proportionnalité de l'utilisation de l'IA au travail (9 répondants) et l'absence d'intervention humaine significative (8 répondants). Certains répondants ont également mentionné l'absence de base juridique valable (6 répondants) et l'absence de lois spécifiques encadrant l'utilisation de l'IA au travail (5 répondants). D'autres

ont souligné la difficulté pour les individus d'exercer leurs droits sur les données (3 répondants) et la perte de contrôle des individus sur la collecte et le traitement des données (5 répondants).

La faible sécurité des données (5 répondants) et le glissement des fonctionnalités (4 répondants) ont également été évoqués par plusieurs répondants. Le risque de collecte à grande échelle de catégories particulières de données a été mentionné une fois. Aucun répondant n'a évoqué les implications plus larges en matière de droits humains.

Question six : À quoi ressemblerait un cadre réglementaire efficace pour l'IA au travail ?

Les répondants ont formulé diverses suggestions quant à la forme que devrait prendre un tel cadre. De nombreuses autorités (18) ont suggéré de nouvelles réglementations ou ont mentionné des initiatives juridiques existantes ou futures dans leurs pays/continents, applicables à l'IA dans le contexte de l'emploi. Plusieurs autorités (10) ont également suggéré, voire exclusivement, des mesures de droit souple telles que des lignes directrices ou des formations. Voici quelques suggestions indicatives et non exhaustives:

- Une **réglementation juridique spécifique pour l'utilisation de l'IA au travail**, incluant, par exemple, des définitions, des classifications des risques, la protection des données dès la conception et par défaut, ainsi que des restrictions sur le développement et/ou l'utilisation de l'IA au travail, telles que la limitation des finalités.
- Garantir que les systèmes d'IA utilisés pour les décisions importantes au travail soient **explicables**.
- Les organisations doivent faire preuve de transparence et de responsabilité quant à leur utilisation de l'IA au travail afin de permettre aux individus d'exercer un choix et un contrôle significatifs sur leurs données personnelles.
- Exiger que les systèmes d'IA et leur utilisation par les employeurs **fassent l'objet d'un audit par un tiers ou d'une autre forme de contrôle externe, y compris avant leur déploiement**.
- Garantir un cadre réglementaire pour l'IA au travail cohérent et compatible avec **le droit du travail et les conventions collectives**.
- Permettre aux **représentants des travailleurs de demander des informations** sur les systèmes algorithmiques.
- **Respecter l'article 22 du RGPD lorsqu'il est applicable, ou des restrictions similaires** concernant la prise de décision automatisée dans le contexte de l'emploi.
- Classer certaines utilisations de l'IA dans l'emploi comme présentant un risque élevé et interdire certains systèmes présentant un risque élevé non atténué, tel que les biais injustes et la discrimination, afin de faciliter l'application de la réglementation.
- **Limiter certaines utilisations de l'IA et en interdire d'autres** qui présentent **des risques élevés ou inacceptables pour la vie privée** (par exemple, les systèmes d'identification biométrique automatisés pour l'évaluation sociale basée sur l'IA). Des restrictions légales doivent être mises en place en cas d'absence de base légale pour le traitement des

données personnelles dans le contexte de l'emploi, d'absence de proportionnalité au regard des finalités et de difficulté à trouver des mesures pour atténuer les risques élevés, afin de protéger les libertés et les droits des personnes concernées.

- **Garantir la sécurité juridique, la protection et l'exercice effectif des droits à la protection des données et à la vie privée des candidats et des employés**, ainsi que leur prise en compte adéquate. Pour permettre aux individus d'exercer un choix et un contrôle significatifs sur leurs informations personnelles, les entreprises doivent d'abord agir de manière transparente et responsable et rendre l'IA compréhensible.
- **Des garanties adéquates** prévues par la loi et les cadres réglementaires, le droit souple et les outils pratiques (lignes directrices), les mesures d'autorégulation des entreprises, etc.
- L'exigence que l'IA soit raisonnablement nécessaire aux fonctions ou activités d'une entité pour respecter **le principe de proportionnalité**. Par exemple, cette nécessité pourrait être évaluée en tenant compte du degré de sensibilité des données personnelles concernées, de la légitimité de la finalité et des intérêts de l'organisation, de l'existence de moyens moins intrusifs pour atteindre cette finalité et de la proportionnalité de l'atteinte à la vie privée des personnes concernées par rapport aux avantages que l'organisation retire de l'utilisation du système.
- Des restrictions devraient être mises en place pour garantir que **les données d'entraînement des systèmes d'IA** dans le contexte de l'emploi soient obtenues et traitées de manière licite et transparente.
- Une définition claire des usages acceptables de l'IA sur le lieu de travail, garantissant une utilisation sûre, éthique et pratique de l'IA sur le lieu de travail.
- **Question 7 : Veuillez résumer brièvement des exemples d'utilisation concrète de l'IA en milieu professionnel dans votre juridiction.**

Plusieurs autorités ont souligné l'utilisation de l'IA dans le recrutement : tri des CV, analyse des entretiens vidéo, vérification des antécédents par reconnaissance faciale et comparaison de photos sur les réseaux sociaux, profilage à grande échelle à partir de nombreuses sources de données et utilisation de jeux pour filtrer les candidats. Certaines ont constaté des cas de discrimination liés à des logiciels de présélection et de classement. D'autres ont également noté l'utilisation de l'IA pour surveiller les employés, notamment par le suivi des véhicules et des appareils mobiles, par webcam pour la surveillance des télétravailleurs ou par l'enregistrement des frappes au clavier. L'utilisation de l'IA pour mesurer la performance et l'efficacité individuelle, évaluer le bien-être et la santé des employés au travail, et les tentatives de contrôle des congés maladie par exploration de données afin d'identifier les demandes injustifiées ont également été mentionnées. Enfin, l'utilisation de données biométriques, comme les empreintes digitales ou la reconnaissance faciale, pour l'accès aux locaux, le contrôle du temps de travail, l'analyse des entretiens d'embauche, l'évaluation des traits de personnalité et la vidéosurveillance avec reconnaissance faciale aux entrées des bâtiments ont été observés. D'autres ont constaté l'existence de logiciels de visioconférence

utilisant des algorithmes d'IA sans cadre juridique approprié, tandis que d'autres encore ont noté que les réseaux sociaux professionnels s'appuient fortement sur des algorithmes de mise en relation et de sélection.

Question 8 : Avez-vous identifié des impacts plus larges liés à l'utilisation de l'IA dans le domaine de l'emploi que vous souhaiteriez aborder (impact sur les consommateurs, la concurrence, la conformité au droit du travail, etc.) ?

Plusieurs autorités ont souligné la nécessité d'une compatibilité avec d'autres cadres juridiques, tels que le droit de la consommation et le droit du travail, ainsi que la nécessité de lutter contre les inégalités et les discriminations injustes.