Chroniques du travail

15 | 2025
L'intelligence artificielle au travail

Réglementer l'IA dans l'entreprise

Mode d'emploi de l'AI Act appliqué aux relations de travail

Regulating AI in the Workplace. A User's Guide to the AI Act as applied to Employment Relationships

Sophie Sereno

Édition électronique
URL : https://journals.openedition.org/chroniquestravail/1719
DOI : 10.4000/159lw
ISSN : 3074-7899

Éditeur
Presses Universitaires de Provence

Édition imprimée
Pagination : 131-152
ISBN : 979-10-320-0587-3
ISSN : 2257-5650

Référence électronique
Sophie Sereno, « Réglementer l'IA dans l'entreprise », *Chroniques du travail* [En ligne], 15 | 2025, mis en ligne le 02 décembre 2025, consulté le 02 décembre 2025. URL : http://journals.openedition.org/chroniquestravail/1719 ; DOI : https://doi.org/10.4000/159lw

Le texte seul est utilisable sous licence CC BY-SA 4.0. Les autres éléments (illustrations, fichiers annexes importés) sont susceptibles d'être soumis à des autorisations d'usage spécifiques.

7 Réglementer l'IA dans l'entreprise

Mode d'emploi de l'*AI Act* appliqué aux relations de travail

*Sophie Sereno**

Résumé

L'irruption de ChatGPT a amorcé une prise de conscience s'agissant de la diversité des applications de l'intelligence artificielle (IA), particulièrement dans le monde du travail. Les systèmes d'IA présentent aussi bien des potentialités que des risques pour les droits des personnes et les entreprises. Cette ambivalence a conduit l'Union européenne à adopter, en 2024, un règlement visant à encadrer le recours à ces technologies. Fondé sur une approche par les risques, ce texte classe les systèmes d'IA en fonction de leur impact potentiel sur la santé, la sécurité et les droits fondamentaux, avec des obligations différenciées selon les usages. L'article propose une analyse de ce cadre juridique appliqué au monde du travail, en s'attardant sur les spécificités liées à l'activité salariée et sur les obligations renforcées mises à la charge des employeurs. Il questionne également les apports concrets de ce texte en matière de transparence et de responsabilité algorithmique ainsi que son articulation avec d'autres instruments juridiques, tels que la directive européenne sur le travail de plateforme.

Mots-clés

intelligence artificielle, algorithme, salariat, gestion du personnel, ressources humaines, recrutement, management algorithmique, plateforme, biais, discriminations, droit du travail

Abstract

ChatGPT has triggered greater awareness of the wide-ranging applications of artificial intelligence (AI). This is especially true in the world of work. AI systems offer both opportunities and risks for individual rights. The European Union has adopted, in 2024, a regulation aimed at governing the use of these technologies. The EU regulation classifies AI systems according to their potential impact on health, safety, and fundamental rights, with differentiated obligations depending on their use. This article offers an analysis of this legal framework as applied to the world of work, focusing on the specific features of employment relations and the reinforced obligations placed on employers. It also examines the regulation's concrete contributions in terms of transparency and algorithmic accountability, as well as its interaction with other legal instruments, such as the UE platform work directive.

Keywords

artificial intelligence, algorithm, wage employment, personnel management, human resources, recruitment, algorithmic management, platform, biases, discrimination, labour law

* Aix Marseille Université, CDS (UR 901), Aix-en-Provence, France.

Les applications de l'intelligence artificielle (IA) se sont démultipliées de manière exponentielle au cours des dernières décennies au point de devenir omniprésentes dans de nombreux secteurs[1]. Pourtant, ce n'est qu'en 2022, lors du lancement de ChatGPT, que s'est amorcée une prise de conscience collective des enjeux liés au déploiement de cette technologie. Depuis, les débats pullulent sur les scènes médiatique et politique. Protagonistes et détracteurs de l'IA ne cessent de débattre des enjeux, avantages et risques, liés à cette technologie. En Europe, un consensus politique a cependant émergé sur la nécessité de disposer d'un cadre juridique commun pour le développement d'une « IA digne de confiance […] fondée sur les valeurs et les règles européennes »[2]. C'est chose faite avec le Règlement européen sur l'intelligence artificielle (dit *AI Act*)[3]. Adopté en juin 2024[4], ce texte procède d'une recherche d'équilibre entre deux impératifs. Il s'agit d'offrir un terrain propice à l'innovation technologique[5], tout en garantissant la protection de la santé, de la sécurité et des droits fondamentaux. Les sanctions prévues s'avèrent particulièrement dissuasives, puisqu'elles peuvent atteindre 35 millions d'euros ou 7 % du chiffre d'affaires annuel mondial (art. 99 et s.). Pour autant, à l'instar du RGPD, les entreprises risquent fort de concentrer leurs efforts de mise en conformité à l'égard des traitements informatiques déployés dans leurs activités, en omettant la gestion des ressources humaines. La question est donc entière : quelle applicabilité (effective) de ce texte en matière de relations de travail ?

À titre préliminaire, il convient de déterminer les technologies couvertes par cette réglementation européenne. L'expression « système d'IA » désigne tout système automatisé, utilisé seul ou comme composant d'un produit, conçu pour fonctionner à différents niveaux d'autonomie et capable de faire preuve d'une capacité d'adaptation après son déploiement (art. 3). Cette définition commune délimite le champ d'application de l'*AI Act* en excluant les systèmes de traitements de données de base n'intégrant pas de technologies d'apprentissage, de raisonnement ou encore de modélisation. La qualification de « système d'IA » est conditionnée à l'existence

1 V. not. : Commission de l'intelligence artificielle, *IA : notre ambition pour la France*, rapp. mars 2024, p. 18 *sq.*

2 Commission européenne, *Intelligence artificielle. Une approche européenne axée sur l'excellence et la confiance*, Livret blanc, COM(2020) 65 final, février 2020, p. 4.

3 Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 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, *JOUE* du 12 juill. 2024.

4 Publié au *JOUE* le 12 juillet 2024, l'entrée en vigueur du règlement européen relatif à l'IA est échelonnée sur plusieurs années, entre 2024 et 2027 : en février 2025, l'interdiction relative aux systèmes à risque inacceptable ; en août 2025, les règles pour modèles à usage général ; en août 2026, les règles relatives à l'IA à haut risque (annexe III) ; en août 2027, les règles pour l'IA à haut risque relevant de l'annexe I.

5 V. not. : Commission européenne, *Plan coordonné dans le domaine de l'intelligence artificielle. Révision de 2021*, annexe à la communication au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM(2021) 205 final, avril 2021.

d'une capacité d'inférence c'est-à-dire la faculté de générer des raisonnements, des déductions ou des prédictions à partir des informations disponibles. Toutefois, cette définition juridique n'emporte pas la pleine application de l'*AI Act*[6]. Ce texte n'institue nullement un régime juridique uniforme pour tout système d'IA. Il n'existe pas un droit commun de l'IA qui s'appliquerait à toutes les personnes ayant recours à une technologie répondant à la définition posée par l'*AI Act*. Les autorités européennes ont privilégié une approche par risques à deux variables. Le risque peut résulter soit de la technologie utilisée, soit de son domaine d'application. Cette classification donne corps à un cadre juridique à gradation, au sein duquel les principes directeurs sont combinés à des enchevêtrements d'exceptions et de règles particulières.

La mise en œuvre de cette réglementation européenne, en général, et la détermination du régime applicable à un SIA, en particulier, dépendent du risque associé à chaque SIA. L'*AI Act* repose sur une classification en quatre catégories faisant varier la nature et l'intensité des obligations selon le type de technologie et le potentiel d'atteinte aux droits. D'abord, les systèmes présentant un risque inacceptable sont interdits. Ceux présentant un risque élevé sont soumis à des exigences strictes. Ensuite, en cas de risque limité, des obligations particulières de transparence s'imposent. Enfin, les systèmes d'IA à risque minimal ou nul ne sont soumis à aucune obligation spécifique au titre de l'*AI Act*. Partant, plus le risque est important pour les droits des personnes, plus la réglementation est stricte. Cependant, cette présentation simplifiée ne doit pas induire en erreur. Avec 180 considérants, 113 articles et 13 annexes, le règlement européen s'avère « verbeux »[7] et complexe à manier. Outre sa technicité technologique et juridique, son appréhension est complexifiée par la multiplication des exceptions et des adaptations en fonction des technologies et des secteurs concernés. Or, la maîtrise de ce corpus juridique s'avère incontournable au regard aux enjeux de protection des droits des travailleurs et de transformation de l'emploi[8].

Le cadre général étant ainsi posé, il convient d'identifier les usages de l'IA au travail couverts par le règlement européen et, par conséquent, les obligations nouvelles et renforcées que ce texte impose aux employeurs.

Les relations de travail confrontées à l'*AI Act*

Loin de relever de la science-fiction, des systèmes d'IA sont d'ores et déjà déployés dans différents aspects des

6 Le développement et le déploiement de SIA dans certains secteurs sont, par principe, exclus de l'application de l'*AI Act*. Il s'agit des domaines hors du droit de l'Union, de la sécurité nationale, des fins militaires ou de la Défense, de la recherche et du développement *exclusivement* scientifiques ainsi que des activités *strictement* personnelles (art. 2).

7 P. Adam, « Intelligence artificielle et relations de travail salarié », *BJT*, 2025, n° 3, p. 43.

8 Pour une réflexion sur le sujet, v. not. la contribution de E. Zerillo.

relations de travail[9], et ce, sans que les utilisateurs et les personnes concernées en soient toujours conscients. Ce déploiement s'opère parfois à bas bruit dans un contexte d'expansion des usages des technologies de l'information et de la communication (TIC). Les applications déployées ou déployables dans un contexte de travail concernent tant les environnements de travail que la gestion des relations de travail. Ces usages d'IA relèvent – en fonction de leurs finalités, de leurs technologies et de leurs paramétrages – d'une catégorie de risque et d'un régime juridique déterminé. Aussi, il convient de dresser un état des lieux des systèmes d'IA, en distinguant les pratiques interdites de celles qui sont autorisées dans un contexte de travail.

Les applications d'IA interdites au travail

L'interdiction instituée par l'*AI Act* recouvre un nombre restreint de systèmes d'IA en raison du risque inacceptable que leur usage représente pour la sécurité, les droits fondamentaux ou à la démocratie (art. 5). Il s'agit des outils et logiciels impliquant une manipulation comportementale, une exploitation des vulnérabilités de groupes spécifiques, une notation sociale, une catégorisation biométrique, un profilage à visée répressive, un contrôle biométrique à distance ou une reconnaissance des émotions.

Le texte européen vise spécifiquement les relations de travail en interdisant « la mise sur le marché, la mise en service ou l'utilisation de systèmes d'IA destinés à évaluer l'état émotionnel de personnes physiques dans des situations liées au lieu de travail et à l'enseignement » (consid. 44). Ces logiciels permettent à partir de vidéos l'analyse des expressions faciales ou vocales afin de reconnaître l'état émotionnel des travailleurs[10]. L'*AI Act* proscrit ainsi l'utilisation d'un tel système dans le cadre professionnel. Toutefois, la portée de cette interdiction est discutée en raison de la formulation retenue. La référence faite aux *situations liées au lieu de travail* interpelle dès lors qu'elle pourrait instaurer une condition

9 V. not. : J. Condé, Y. Ferguson, *Usages et impacts de l'IA sur le travail, au prisme des décideurs*, rapp., LaborIA, mars 2023 ; F. Barcellini *et al.*, *Le travail et l'emploi à l'épreuve de l'IA : État des lieux et analyse critique de la littérature*, rapp., IRES, mars 2024. D'ailleurs, les accords collectifs adoptés en la matière attestent de la variété des thématiques couvertes (N. Greenan, S. Napolitano, J. Pillosio, « L'IA dans les entreprises : que révèlent les accords négociés ? », *Connaissance de l'emploi*, octobre 2024, n° 200, p. 4.

10 L'*AI Act* définit le *système de reconnaissance des émotions* comme « un système d'IA servant à identifier les émotions ou les intentions de personnes physiques ou à faire des déductions quant à leurs émotions ou intentions, sur la base de leurs données biométriques. Cette notion renvoie à des émotions ou des intentions telles que le bonheur, la tristesse, la colère, la surprise, le dégoût, la gêne, l'excitation, la honte, le mépris, la satisfaction et l'amusement. Cette notion ne recouvre pas les états physiques, tels que la douleur ou la fatigue, qui comprennent, par exemple, des systèmes utilisés pour déceler l'état de fatigue des pilotes ou des conducteurs professionnels aux fins de la prévention des accidents. Elle ne recouvre pas non plus la simple détection d'expressions, de gestes ou de mouvements dont l'apparence est immédiate, à moins que ceux-ci ne soient utilisés pour identifier ou déduire des émotions. Ces expressions peuvent être des expressions faciales toutes simples telles qu'un froncement de sourcils ou un sourire, ou des gestes tels qu'un mouvement de mains, de bras ou de tête, ou encore des caractéristiques de la voix d'une personne, comme le fait de parler fort ou de chuchoter » (consid. 18). Pour une réflexion sur cette application de l'IA, v. not. : G. Loiseau, « Le traitement algorithmique des émotions du travailleur », *Dr. soc.*, 2023, p. 889.

spatiale à la classification d'un système d'IA émotionnelle comme interdit. Or, il conviendrait de privilégier une autre lecture, plus en phase avec l'esprit du texte[11], en retenant que la reconnaissance des émotions est exclue en milieu professionnel[12]. À défaut, échapperaient à cette interdiction de principe des traitements algorithmiques visant à identifier l'état émotionnel des travailleurs, à partir de chatbots, de caméras ou de capteurs[13]. Pour autant, il serait possible de questionner la légalité d'un tel système au regard des exigences de justification et de proportionnalité[14] ou celles de pertinence[15] posées par le Code du travail. En outre, une protection particulière est offerte par la Directive sur le travail de plateforme[16] qui interdit, en son article 7, le traitement des données liées à l'état émotionnel et psychologique des travailleurs.

D'autres usages professionnels de l'IA sont susceptibles d'être qualifiés de pratiques interdites. C'est notamment le cas des technologies biométriques utilisées à des fins de contrôle des accès et de gestion des présences[17]. Ces applications reposent sur la catégorisation biométrique pour identifier les personnes à partir de caractéristiques physiques[18]. Si cette technologie n'est pas proscrite en tant que telle, les systèmes de catégorisation basés sur des données biométriques ne peuvent être utilisés pour établir des déductions concernant certains motifs discriminatoires (art. 5, §1 g) ; consid. 30 : « leur race, leurs opinions politiques, leur affiliation à une organisation syndicale, leurs convictions religieuses ou philosophiques, leur vie sexuelle ou leur orientation sexuelle »). Par ailleurs, des suites RH intègrent des modules permettant de procéder à des analyses prédictives afin d'évaluer la performance, planifier les évolutions de carrière ou la mobilité interne des travailleurs. Selon le paramétrage et les critères retenus, ces systèmes d'IA peuvent être utilisés pour évaluer voire classifier des personnes en fonction de leur comportement ou de caractéristiques personnelles. Ces procédés de

11 Le considérant 44 souligne la faillibilité de cette technologie ainsi que les atteintes aux droits pouvant être induites par son déploiement dans le « cadre du travail » eu égard au déséquilibre de pouvoir résultant du lien de subordination. Or, une approche fondée sur un critère spatial apparaît réductrice de la finalité poursuivie par l'instauration de l'interdiction.

12 Pour autant, la lecture de l'*AI Act* dans ses versions anglaise (« *in situations related to the workplace* »), espagnole (« *en situaciones relacionadas con el lugar de trabajo* ») ou encore allemande « *in Situationen, ableiten sollen, die mit dem Arbeitsplatz* ») ne permet pas de résoudre cette difficulté.

13 Sur ce point : G. Loiseau, « Le règlement européen relatif à l'intelligence artificielle. Application et implications dans les relations de travail », *JCP S*, 2024, p. 1265.

14 C. trav., art. L. 1121-1.

15 C. trav., art. L. 1221-6 (en matière de recrutement) et art. L. 1222-6 (en matière d'exécution du contrat).

16 Directive (UE) 2024/2831 du 23 octobre 2024 relative à l'amélioration des conditions de travail dans le cadre du travail via une plateforme. Les États doivent procéder à sa transposition pour le 2 décembre 2026.

17 Toutefois, le déploiement de cette technologie est généralement appréhendé à travers le contrôle des espaces publics (V. not. : Défenseur des droits, *Perception du développement des technologies biométriques en France. Entre manque d'information et demande d'encadrement*, octobre 2022).

18 L'*AI Act* définit successivement les notions de « données biométriques » (consid. 14), d'« identification biométriques » (consid. 15), de « catégorisation biométrique » (consid. 16), et de « système d'identification biométrique à distance » (consid. 17).

notation dans un contexte de travail sont prohibés en raison de leurs effets préjudiciables et potentiellement discriminatoires (consid. 31). Sur ce point, les travailleurs de plateforme bénéficient d'une protection élargie, car l'interdiction tenant à ces données sensibles couvre tout traitement algorithmique[19]. La directive sur le travail de plateforme proscrit également le recours à des indicateurs apparemment neutres pouvant révéler ou déduire l'existence d'une caractéristique protégée par le droit de la non-discrimination.

Du reste, d'autres pratiques interdites sont susceptibles d'être déployées dans un contexte de travail. Il s'agit des systèmes d'IA utilisant des techniques subliminales ou manipulatrices ainsi que celles exploitant des vulnérabilités qui sont susceptibles d'altérer le comportement des individus et de leur causer un préjudice. De telles technologies pourraient notamment être intégrées dans les environnements numériques de travail afin d'influencer les salariés à leur insu. Ces différentes applications sont certes proscrites au regard de l'*AI Act*, mais également au regard du droit du travail, en raison de leur caractère discriminatoire[20] et attentatoire aux droits des travailleurs[21].

Il est bon de rappeler que le droit commun du travail offre nombre de normes protectrices qui régissent toute relation de travail salariée, numérisée ou non[22]. Plusieurs dispositions du Code du travail peuvent ainsi être mobilisées lorsque le déploiement d'un système d'IA induit un risque d'atteintes aux droits des travailleurs. Le droit du travail s'applique pleinement et doit être combiné avec les normes du numériquetelles que le RGPD, l'AI Act ou la directive relative au travail de plateforme.

Surtout, l'effectivité de ces interdictions de principe se heurte à une difficulté centrale tenant à la détection de ces pratiques jugées inacceptables par les personnes concernées, les salariés, leurs représentants, mais également les gestionnaires de ressources humaines. L'intégration de l'IA dans les outils de travail est souvent invisible et échappe alors à la vigilance de la collectivité de travail. L'absence de mécanisme de veille et d'appropriation des enjeux de l'IA au travail entrave *de facto* la possibilité pour les salariés et les représentants du personnel de se prévaloir de la prohibition de certaines pratiques d'IA, mais également des règles particulières à l'égard des applications autorisées.

Les applications d'IA autorisées au travail

Les pratiques interdites représentent une (faible ?) part des systèmes d'IA

19 Directive (UE) 2024/2831, art. 7.

20 C. trav., art. L. 1132-1.

21 C. trav., art. L. 1121-1.

22 Le considérant 9 de l'*AI Act* rappelle que la réglementation européenne sur l'IA complète les législations existantes sans s'y substituer et ne doit pas avoir une incidence négative sur la protection conférée par le droit national pour les droits des travailleurs.

déployés ou déployables dans les entreprises. Le champ des possibles technologiques demeure immense. Les cas de recours à l'IA ne tombant pas sous le coup de l'interdiction relèvent d'un régime plus ou moins restrictif en fonction de leur niveau de risque.

Certains systèmes d'IA présentent un risque important pour les droits des personnes en raison de leur utilisation dans des domaines sensibles. Si ces applications qualifiées « à haut risque » ne sont pas prohibées en tant que telles, leurs usages sont soumis à des exigences renforcées à l'égard des fournisseurs qui conçoivent ou commercialisent ces technologies, mais également à l'égard des déployeurs qui utilisent ces technologies. La classification à haut risque repose sur une logique sectorielle, selon une double entrée. En premier lieu, l'article 6 de l'*AI Act* prévoit que sont à haut risque les systèmes d'IA intégrés à des produits couverts par une législation européenne spécifique (visée à l'annexe I). En second lieu, cette qualification est étendue à certains usages d'IA dans des domaines d'activité considérés comme sensibles (visés à l'annexe III), tels que l'emploi. À ce stade, il serait réducteur et erroné de retenir une approche parcellaire en considérant que l'application de cette réglementation européenne se limite aux cas d'utilisation listés à l'annexe III. En effet, l'intégration de l'IA dans les domaines d'activité énumérés en annexe I est susceptible de transformer en profondeur l'organisation de travail et d'affecter les droits des travailleurs.

Au sens de l'*AI Act*, un système d'IA est automatiquement considéré à haut risque s'il est destiné à être un composant de sécurité d'un produit couvert par la législation d'harmonisation de l'Union, figurant en annexe I, ou s'il est lui-même un tel produit, soumis à une évaluation de conformité par un tiers (art. 6). La liste retenue recouvre une grande diversité de secteurs d'activité, puisque sont visés des produits, tels que les dispositifs médicaux, les jouets, les véhicules à moteur, les machines industrielles, les équipements sous pression ou encore l'aviation civile. Des applications professionnelles d'IA peuvent ainsi relever de cette qualification en fonction de l'activité de chaque entreprise. Ainsi, même s'ils ne concernent pas la gestion du personnel, leurs déploiements peuvent présenter des risques pour les travailleurs qui conçoivent ou utilisent des outils et produits intégrant une telle technologie. Aussi, le développement, la commercialisation ou l'utilisation de ces systèmes d'IA par les entreprises dans ces activités sensibles emportent des obligations spécifiques pour les employeurs.

Indépendamment des produits faisant l'objet d'une législation spécifique (listés en annexe I), peuvent également être classifiés à haut risque les systèmes d'IA utilisés dans certains domaines, énumérés en annexe III, jugés sensibles au regard des risques importants pour les droits des personnes. Une approche sectorielle est, de nouveau, retenue. Le texte pose une liste exhaustive – susceptible d'évoluer[23] – des

23 *AI Act*, art. 7.

activités pour lesquelles l'usage de l'IA est à haut risque, parmi lesquels figurent l'emploi, la gestion de la main-d'œuvre, l'accès à l'emploi indépendant (§4) et la formation professionnelle (§3). Ainsi, le particularisme des relations de travail a été pris en considération. Le texte fournit des exemples concrets d'utilisations présentant un risque élevé pour les droits des personnes. La gestion des ressources humaines intègre de plus en plus d'outils d'IA[24]. Pour le recrutement et la sélection de personnes physiques, il s'agit notamment des systèmes d'IA utilisés pour la publication d'offres d'emploi ciblées, l'analyse et le filtrage de candidatures ou l'évaluation des candidats[25]. Les applications en matière de gestion du personnel sont envisagées de manière plus ouverte. En effet, l'annexe III énumère différents usages, tels que la gestion des performances et des promotions. Plus généralement, des systèmes d'IA peuvent être qualifiés à haut risque lorsqu'ils sont utilisés pour prendre des décisions affectant les conditions de travail, voire l'existence du contrat[26]. Pour autant, le déploiement au travail d'un système d'IA visé à l'annexe III n'emporte pas sa classification automatique en haut risque, à la différence des activités et produits spécifiés en annexe I. Encore faut-il que la technologie utilisée présente un risque significatif pour les personnes. Le système d'IA doit soit présenter un risque de préjudice important pour la santé, la sécurité ou les droits fondamentaux des personnes, soit impliquer un profilage de personnes physiques. Cette conditionnalité génère *in fine* une forte incertitude quant à la portée effective des normes de protection instituées par l'*AI Act* dans le domaine de l'emploi. L'exclusion des systèmes sans profilage n'ayant pas un impact substantiel sur la décision est susceptible de restreindre, de manière conséquente, le champ d'application de ce texte en matière de gestion du personnel. Toute la difficulté réside donc dans la détermination du caractère « à haut risque » d'un système d'IA. Celui-ci dépendra des modalités et des éléments d'appréciation retenus par les entreprises et les autorités de contrôle pour retenir l'existence d'un *risque important de préjudice*. Or, les systèmes d'IA traitant des données sensibles au sens du RGPD ou des éléments protégés par le droit présentent inexorablement un risque d'atteinte aux droits, la concrétisation de ce risque dépendant *in fine* du paramétrage. Sur ce point, le règlement identifie l'incidence potentiellement négative sur les droits fondamentaux, y compris le droit à la non-discrimination,

24 V. not. : M. Barabel, T. Ferras, C.-H. Besseyre Des Horts, dir., *L'intelligence artificielle au service des RH*, Paris, Dunod, 2020.

25 Sur les enjeux en matière de recrutement, v. : M. Peyronnet, « L'usage des algorithmes et de l'IA dans le recrutement : une occasion de (ne) plus discriminer ? », in P. Adam, M. Le Friant, Y. Tarasewicz, dir., *Intelligence artificielle, gestion algorithmique du personnel et droit du travail*, *op. cit.*, p. 139.

26 Annexe III, §4 b) : « systèmes d'IA destinés à être utilisés pour prendre des décisions influant sur les conditions des relations professionnelles, la promotion ou le licenciement dans le cadre de relations professionnelles contractuelles, pour attribuer des tâches sur la base du comportement individuel, de traits de personnalité ou de caractéristiques personnelles ou pour suivre et évaluer les performances et le comportement de personnes dans le cadre de telles relations ».

comme un critère pertinent pour classer un système d'IA à haut risque (consid. 48, 56, 57 et 58). Il conviendrait donc de retenir que les usages de l'IA pour la gestion du travail ou du personnel, qui intègrent des données personnelles ou ont un potentiel (directement ou indirectement) discriminatoire, laissant présumer l'existence d'un risque élevé, et sont donc soumis au régime juridique des systèmes d'IA à haut risque.

Du reste, le déploiement de l'IA dans le monde du travail ne saurait être appréhendé par le seul prisme des systèmes à risque inacceptable ou élevé. Une telle conception aboutirait à réduire drastiquement la portée effective du champ d'application de l'*AI Act*. Le plus grand nombre des cas d'usage de l'IA dans un contexte professionnel ne présentent pas de danger majeur pour les droits des personnes. Or, pour les systèmes présentant peu ou pas de risque, le règlement n'impose aucune obligation particulière. Pour autant, certaines applications d'IA ont une capacité non négligeable d'influencer les individus et les environnements. Il s'agit notamment des systèmes de chatbots, d'assistance virtuelle, de génération de contenu, de filtrage de contenu ou de recommandations personnalisées. Face à ce « risque spécifique » de manipulation, des exigences de transparence et d'information sont instituées par l'*AI Act*. Selon une logique proche, des contraintes réglementaires particulières s'appliquent aux IA à usage général (GPAI) qui sont des modèles capables d'exécuter un large éventail de tâches distinctes et pouvant ainsi intégrer une variété de systèmes ou d'applications. Les exemples les plus emblématiques sont ChatGPT, Copilot, Gemini ou Mistral large. Or, ces modèles généraux accessibles au grand public sont répandus dans les entreprises et utilisés par les travailleurs, sans qu'ils aient (toujours) conscience que cette exploitation relève du champ de la réglementation européenne.

En définitive, l'applicabilité de l'*AI Act* dépend de la manière dont les parties prenantes – employeurs, salariés et représentants du personnel – vont s'approprier le texte afin de saisir les usages réels de l'IA dans les organisations. Deux principaux écueils sont susceptibles de limiter la portée des protections instituées par la réglementation européenne. D'une part, le périmètre des classifications demeure ambigu en raison de la mobilisation de notions sujettes à interprétation. D'autre part, la détection même du recours à l'IA constitue un défi majeur. Cette inquiétude est nourrie par le potentiel de contournements de la classification basée sur les risques, notamment par la dissimulation de la technologie déployée ou de la finalité poursuivie. Il en résulte que l'effectivité du droit européen de l'IA est conditionnée à la clarification des critères de classification et à la (re)connaissance des systèmes d'IA.

Les obligations instituées par l'*AI Act* confrontées au travail

L'adoption de l'*AI Act* constitue une étape importante pour la régulation de

l'IA dans l'Union européenne (et au-delà de ses frontières)[27]. Ce texte retient une logique de protection à double détente, axée sur la sûreté des systèmes d'IA et le respect des droits fondamentaux. Ainsi institue-t-il des obligations inédites à l'égard principalement des protagonistes de l'IA, que sont les *fournisseurs*[28] et les *déployeurs*[29]. En miroir, des droits sont consacrés au profit des *personnes concernées* par les systèmes d'IA. Appliquée au monde du travail, cette réglementation européenne soulève des questionnements quant à l'articulation de ces exigences nouvelles avec d'autres corpus juridiques, qu'il s'agisse du Code du travail ou encore de la récente directive européenne sur le travail de plateforme[30]. À y regarder de plus près, l'*AI Act* organise la régulation de l'IA en s'appuyant sur deux logiques complémentaires : consacrer une *compliance* technique des systèmes d'IA et préserver l'*empowerment* sur les systèmes d'IA[31]. *Dans une visée didactique, le choix a été fait de présenter les principales règles applicables aux employeurs privés sous forme de tableaux.*

La consécration d'une *compliance* technique[32] de l'IA

Le développement et le déploiement des systèmes d'IA génèrent des risques majeurs en termes d'atteintes aux droits des personnes, largement documentés ces dernières années. De manière générale, une défaillance peut induire une décision biaisée, erronée, voire non maîtrisée, ayant des conséquences graves sur les individus[33]. En particulier, les traitements algorithmiques peuvent reproduire et amplifier les discriminations, alors même que l'opacité des systèmes rend difficiles la compréhension et la contestation des décisions (partiellement ou totalement) automatisées[34]. Ces menaces ont motivé l'adoption de règles de gouvernance et de conformité technique. Les entreprises sont sou-

27 À l'instar du Réglement général de protection des données (Règlement (UE) 2016/679 dit RGPD), l'*AI Act* a une portée extraterritoriale. Ses dispositions s'appliquent aux fournisseurs et déployeurs de systèmes d'IA établis dans un État tiers à l'Union européenne si les sorties produites sont destinées à être utilisées au sein de l'Union (consid. 21). Pour une réflexion sur la portée du texte, v. not. : G. Loiseau, « Le règlement européen relatif à l'intelligence artificielle », art. cit., p. 1265.

28 Le « fournisseur » est la personne physique ou morale qui a développé ou fait développer le système d'IA et a procédé à sa mise en service ou sur le marché (art. 3).

29 Le « déployeur » est la personne physique ou morale qui utilise le système d'IA sous son autorité, à l'exclusion d'une activité exclusivement personnelle (art. 3).

30 V. not. : S. Robin-Olivier, « Le droit social européen face à l'IA », *RDT eur.*, 2024, p. 477.

31 La classification proposée pour les obligations issues de l'*AI Act* relève d'un choix de l'auteur dans un souci de clarté. Cette catégorisation est perfectible dès lors qu'il existe une perméabilité visible entre les règles et les instruments de régulation institués par cette réglementation européenne.

32 Dans le cadre de la présente étude, l'expression « compliance technique » désigne l'ensemble des exigences techniques spécifiques et des obligations processuelles instituées par l'*AI Act* qui constitue *in fine* un cadre réglementaire (d'appréciation) de conformité des systèmes d'IA.

33 Pour une étude sur les conséquences dans l'accès aux droits, v. not. : E. Bonifay, S. Sereno, « Le recueil et l'exploitation de données genrées par des algorithmes : entre omniprésence et méconnaissance », in E. Bonifay, S. Sereno, dir., *Droit, algorithmes et genre*, Aix-en-Provence, PUAM, coll. « Droits, pouvoirs & sociétés », 2025, p. 89.

34 V. not. : S. Merabet, « Les algorithmes et le droit, quelle(s) interaction(s) ? », in E. Bonifay, S. Sereno, dir., *Droit, algorithmes et genre*, *op. cit.*, p. 19 ; S. Sereno, « Les biais discriminatoires des algorithmes : du constat à l'action », in Ph. Pedrot, A. Papaux, dir., *Penser, calculer, délibérer*, Paris, Mare & Martin, 2023, p. 173.

mises à des obligations « multi-dimensionnelles » ; leur nature et leur intensité varient selon leur qualité (de fournisseur ou d'utilisateur/déployeur) et la classification du système de l'IA (haut risque, risque spécifique de transparence, modèle à usage général). Les principales règles applicables aux employeurs privés sont exposées ci-dessous sous forme de tableaux, en distinguant les obligations de gouvernance (tableau 1) de celles de conformité (tableau 2), en fonction de leur qualité de fournisseurs ou de déployeurs des systèmes d'IA.

Tableau 1. Les principales obligations de gouvernance

Obligation	Catégorie(s) des systèmes d'IA concernés	Personne(s) assujettie(s) à l'obligation	Descriptif de l'obligation
Gouvernance et qualité des jeux de données	Haut risque	Fournisseurs	**S'assurer de la qualité des données d'entraînement, de validation et de test** (art. 10 ; consid. 67 et 433). Les fournisseurs doivent garantir que les données utilisées à toutes les étapes du développement du système d'IA sont pertinentes, représentatives et exemptes d'erreurs ou de biais afin de garantir un fonctionnement fiable. Disposer de données de haute qualité tend à limiter le risque que le système d'IA soit source de discrimination. Des mesures doivent être prévues afin d'atténuer les biais, notamment ceux inhérents aux données historiques (consid. 59 et 67). Les entreprises sont autorisées à traiter des catégories de données sensibles afin de détecter et corriger les biais (art. 10, §10).
Mise en place d'un système de gestion de la qualité	Haut risque	Fournisseurs	**Établir, documenter et maintenir un système de gestion de la qualité** (art. 17). Cette obligation recouvre la gestion des risques, des données, les essais et le suivi après la mise sur le marché. Son respect est apprécié au regard de la taille de l'entreprise. **Mettre en place une gouvernance interne dédiée à l'IA** (pour le pilotage et la supervision), avec la désignation d'un responsable IA.
Identification, cartographie et enregistrement des systèmes d'IA	Haut risque	Fournisseurs	**S'enregistrer et enregistrer les systèmes d'IA dans une base de données avant sa mise sur le marché ou en service** (art. 49, §1). Cette exigence expresse d'enregistrement emporte une obligation préalable, pour les fournisseurs, consistant à identifier et à classifier les systèmes d'IA développés. Cette obligation s'applique également aux utilisateurs publics et aux personnes privées agissant en leur nom (art. 49, §3).

Surveillance et contrôle humain	Haut risque	Fournisseurs	**Concevoir et développer des systèmes d'IA intégrant la supervision humaine effective** (art. 14, §1). Cette obligation implique que la conception du système d'IA doit permettre son contrôle par un humain, pour vérifier le respect des objectifs, identifier et corriger les erreurs. Des moyens techniques doivent être intégrés pour faciliter la surveillance et l'intervention humaine. Les outils adaptés sont laissés à l'appréciation du fournisseur et peuvent notamment consister en des interfaces, des alertes, des tableaux de bord…
		Déployeurs.	**Prendre des mesures techniques et organisationnelles adaptées pour garantir une utilisation conforme à la notice d'utilisation fournie par le fournisseur** (art. 26, §1) ainsi qu'**assurer une surveillance continue de leur fonctionnement** (art. 26, §5). Cette exigence implique un contrôle humain effectif. L'*AI Act* impose ainsi aux entreprises de confier le contrôle à des individus disposant de la compétence, de la formation et de l'autorité nécessaires (art. 26, §2). De plus, au-delà de l'utilisation conforme à la notice d'utilisation (art. 26, §1). Cette exigence impose aux utilisateurs de mettre en place une procédure interne et des outils permettant de contrôler que le système d'IA ne génère pas d'erreurs ou de biais. Cette exigence de contrôle humain est renforcée pour les systèmes automatisés de surveillance et de prise de décision dans le cadre des plateformes de travail numérique (Directive sur le travail de plateforme, art. 10). *Outre l'obligation d'instituer des garanties techniques et organisationnelles, il existe un enjeu fort à s'assurer, au sein des entreprises, que les travailleurs en charge du contrôle disposent d'une formation et d'une compétence suffisantes pour procéder à une surveillance effective du fonctionnement des systèmes d'IA, d'autant que la tentation peut être forte de s'en remettre à l'IA*[35].

35 Pour une étude en matière de recrutement, v. : C. Martin-Lacroux, A. Lacroux, « Faire confiance à l'humain mais suivre l'IA ? Le paradoxe de la confiance des recruteurs envers les avis reçus dans les situations de recrutement augmenté », *34e Congrès de l'AGRH*, AGRH, 2023.

Mise en place d'une politique interne de gestion des risques *Cette obligation s'inscrit dans le prolongement de l'obligation de « surveillance et contrôle humain ».*	Haut risque	Fournisseurs	**Mettre en place et maintenir un système de gestion des risques** (art. 9) prenant obligatoirement la forme d'un processus itératif continu et planifié, sur l'ensemble du cycle de vie du système d'IA (consid. 65). Ce dispositif de contrôle vise à identifier et à atténuer les risques prévisibles. Aussi, il doit lui-même être régulièrement examiné et mis à jour afin de conserver son efficacité.
		Déployeurs	**En cas de risque détecté, suspendre l'utilisation et informer le fournisseur ainsi que les autorités compétentes** (art. 26, §5). Cette exigence emporte une responsabilisation des utilisateurs de systèmes d'IA en leur imposant une obligation de vigilance et de réaction afin de prévenir et de limiter les atteintes aux droits des personnes. Toutefois, sa mise en œuvre est délicate eu égard à la difficulté d'apprécier ce que recouvre précisément la notion de « risque » au sens de l'article 79 de l'*AI Act* (qui renvoie elle-même à l'article 3 §19 du Règlement UE 2019/1020).

Tableau 2. Les principales obligations de conformité

Obligation	Catégorie(s) des systèmes d'IA concernés	Personne(s) assujettie(s) à l'obligation	Descriptif de l'obligation
Constitution et tenue d'une documentation technique et d'un registre de conformité	Haut risque	Fournisseurs	**Établir une documentation technique complète, claire et intelligible et la maintenir à jour** (art. 11, §1). Cette exigence impose aux fournisseurs de constituer et de conserver un dossier technique pour chaque système d'IA à haut risque. Cette documentation doit être mise à disposition des autorités compétentes (art. 11, § 1 ; art. 16, § 2) et des organismes d'évaluation de la conformité (art. 43). L'*AI Act* n'instaure pas l'obligation pour les fournisseurs de remettre cette documentation technique (complète) aux déployeurs, destinataires d'une notice d'utilisation. Ce défaut d'accès de droit à la documentation technique complète pourrait constituer un frein important dans le contrôle du fonctionnement des systèmes d'IA à haut risque. Pour autant, les entreprises utilisatrices pourraient intégrer cette condition dans le contrat d'acquisition[36].

36 V. not. sur les clauses de ce type de contrat : L. Bidault, « Les clauses spécifiques au contrat d'acquisition d'un système d'intelligence artificielle », *Contrats publics*, 2025, n° 265, p. 46.

			Les fournisseurs de modèles d'IA à usage général (GPAI) sont soumis à une obligation particulière concernant l'élaboration et la tenue d'une documentation technique (art. 53 §1). **Prévoir la possibilité d'enregistrer automatiquement des évènements (journaux) tout au long de la durée de vie du système d'IA** (art. 12). Cette exigence imposée aux fournisseurs est essentielle et conditionne l'obligation de tenir des journaux (figurant ci-dessous).
		Fournisseurs et Déployeurs	**Tenir des journaux générés automatiquement par le système d'IA pour assurer la traçabilité des événements.** Cette fonctionnalité permet de retracer le fonctionnement du système d'IA, d'identifier des situations à risque ou des anomalies et donc de vérifier sa conformité. L'obligation s'impose à la personne, fournisseur ou déployeur, exerçant un contrôle effectif sur les journaux. La durée de conservation doit être adaptée à la finalité du système, sans être inférieure à 6 mois (art. 19, §1 ; art. 26, §6). Cette traçabilité est essentielle pour l'explicabilité du système d'IA, mais également pour la détermination des responsabilités en cas d'atteintes aux droits. L'accès à ces journaux constitue un enjeu central pour détecter et prouver d'éventuelles atteintes aux droits. En mobilisant ses moyens d'action (information-consultation, expertise, alerte), le CSE peut demander à accéder à ces informations lorsqu'elles sont en cause. Toutefois, la durée minimale de conservation de 6 mois constitue une limite temporelle importante à la capacité de contrôle.

Contrôle régulier de la conformité des systèmes	Haut risque	Fournisseurs	**Instaurer des procédures d'examen, de test et de validation à chaque étape du cycle de vie du système d'IA** (art. 17, §1). Cette exigence prend la forme d'une auto-évaluation devant intervenir avant, pendant et après le développement du système d'IA. Pour certains systèmes (visés à l'annexe 3, §1), cette obligation est complétée par une évaluation externe de conformité. Celle-ci doit être effectuée par un organisme agréé par les autorités (art. 28) qui délivrera un certificat de conformité (art. 43 §1).
		Déployeurs	**Mettre en place des contrôles réguliers du fonctionnement des systèmes d'IA** (art. 26, §5). Cette exigence impose la mise en place de mécanismes structurés et réguliers de vérification. L'*AI Act* ne fixe pas de modalités de réalisation ou de fréquence particulières pour les évaluations. Toutefois, les utilisateurs doivent réaliser ce contrôle dans le respect des obligations instituées en matière d'utilisation conforme, de mise en place des moyens organisationnels et techniques appropriés, de surveillance humaine compétente, de vérification des données d'entrée, de conservation des journaux, d'analyse d'impact et de signalement et de suspension en cas de risque.
	Modèles d'IA à usage général à risque systémique	Fournisseurs de modèle	**Effectuer des évaluations de modèle, y compris des essais contradictoires, afin d'identifier et d'atténuer les risques systémiques** (art. 55, §1).

Prises dans leur ensemble, ces exigences font écho à plusieurs garanties offertes par le Code du travail dont le respect s'impose aux employeurs lorsque le déploiement de l'IA concerne les travailleurs. C'est notamment le cas de l'interdiction des discriminations directes ou indirectes[37], de la protection de la santé et de la sécurité et des attributions du Comité social et économique (CSE). Outre la protection conférée aux données sensibles par l'*AI Act* et le RGPD, l'employeur doit s'assurer que la data soit de haute qualité. Plus particulièrement, les données d'apparence neutre doivent faire l'objet d'une attention particulière afin d'éviter que leur traitement automatisé produise des effets discriminatoires. Pour autant, les employeurs peuvent prendre des mesures spécifiques à visée corrective. Cette précision souligne l'intérêt de recourir à ces technologies dans la lutte contre les discriminations systémiques, susceptibles d'être générées ou révélées par un système d'IA[38].

L'objectif est d'assurer la fiabilité, la sécurité, l'absence de discrimination et le respect des droits fondamentaux. Aussi, chaque entreprise doit articuler

37 L. n° 2008-496 du 27 mai 2008 portant diverses dispositions d'adaptation au droit communautaire dans le domaine de la lutte contre les discriminations, art. 1er.

38 V. not. : A. Lacroux, et C. Martin-Lacroux, « L'intelligence artificielle au service de la lutte contre les discriminations dans le recrutement », *Management & Avenir*, 2021, n° 122, p. 121.

cette exigence avec celles induites par le Code du travail, notamment l'obligation de sécurité de l'employeur[39] et, dans son prolongement, l'obligation d'évaluation des risques professionnels auxquels sont exposés les salariés[40]. Le déploiement de l'IA doit être examiné s'agissant de ses éventuelles répercussions sur les conditions de travail, la santé et la sécurité des salariés.

L'*AI Act* n'impose pas la création d'une instance paritaire de gouvernance ou même la participation de représentants du personnel à la gouvernance des données ou à la surveillance. Toutefois, la constitution d'une instance particulière, voire d'une commission, peut être envisagée et prévue par un accord collectif, d'autant que cette voie a été empruntée par certaines entreprises[41]. D'ailleurs, cette co-régulation fait l'objet de recommandations[42]. En outre, une information ou une consultation du CSE peut s'imposer selon les circonstances[43], notamment lors de l'introduction de nouvelles technologies[44]. À la réflexion, les exigences tant techniques que processuelles instituées par l'*AI Act* tendent à s'assurer que l'humain reste dans la bouche (« *Human-in-the-Loop* ») voire soit au cœur de l'IA (« *Human-centric IA* »).

L'affirmation d'un *empowerment* à l'égard des systèmes d'IA

Appliqué aux systèmes d'IA, l'*empowerment* tend à s'assurer que les êtres humains ne soient pas des sujets passifs subissant les effets de ces technologies, mais des acteurs éclairés (consid. 15 et 16). Cette logique implique que les personnes doivent disposer des moyens pour comprendre et agir, de manière éclairée, face aux risques algorithmiques d'atteintes aux droits. Outre les exigences de gouvernance et de conformité, l'*AI Act* intègre des garanties visant à assurer une réelle capacité d'action des individus et, in fine, un contrôle humain effectif. Les obligations favorisant l'*empowerment* peuvent être regroupées en plusieurs axes : la maîtrise de l'IA (tableau 3), la transparence et l'explicabilité accrues (tableau 4), l'accessibilité et la non-discrimination (tableau 5). Ces exigences constituent autant de ressources (difficilement) mobilisables par les salariés et/ou leurs représentants.

39 C. trav., art. L. 4121-1.

40 C. trav., art. L. 4121-2 et L. 4121-3.

41 V. not. : Société Prisma Media, Accord d'entreprise relatif à la mise en place d'une Commission Facultative au sein du CSE sur l'usage de l'intelligence artificielle, 27 février 2025.

42 V. not. la recommandation n° 3 du rapport *IA : notre ambition pour la France* de la Commission de l'intelligence artificielle, mars 2024.

43 V. la contribution de M. Hallot. V. également : S. Sereno, « « L'intelligence artificielle soumise à la consultation du CSE », *Gaz. Pal.*, 3 juin 2025, n° 19, p. 56.

44 C. trav., art. L. 2312-8.

Tableau 3. L'exigence de maîtrise de l'IA

Exigence	Catégorie(s) des systèmes d'IA concernés	Personne(s) assujettie(s)	Descriptif de l'exigence
Acquisition de la maîtrise de l'IA	Tous les systèmes d'IA	Fournisseurs, Déployeurs, Personnes concernées	**Permettre aux personnes physiques de disposer des compétences, des connaissances et de la compréhension nécessaires pour prendre des décisions éclairées concernant les systèmes d'IA** (art. 4). Les modalités d'acquisition de cette maîtrise ne sont pas précisées par l'*AI Act*. Pour autant, cette exigence conditionne l'effectivité des obligations liées à la surveillance et au contrôle de l'IA.

Tableau 4. Les principales obligations de transparence et d'explicabilité

Exigence	Catégorie(s) des systèmes d'IA concernés	Personne(s) assujettie(s) à l'obligation	Descriptif de l'obligation
Fourniture d'une notice d'utilisation exhaustive	Haut risque	Fournisseurs	**Fournir aux déployeurs une notice d'utilisation intégrant des informations claires et compréhensibles détaillées** (art. 13, §3 ; consid. 65 et 72). L'information écrite doit détailler les caractéristiques, les capacités, les limites, les instructions, les risques résiduels, les exigences en matière de contrôle et, plus largement, toute information nécessaire pour garantir une utilisation conforme du système d'IA. Par son exhaustivité, cette notice d'utilisation permet aux entreprises utilisatrices de disposer d'informations détaillées sur le fonctionnement du système d'IA déployé. Aussi, sa communication aux institutions représentatives du personnel s'impose en cas d'information ou de consultation concernant le déploiement du système d'IA concerné dans l'entreprise.

Marquage et identification des interactions avec un système d'IA ainsi que des contenus générés ou manipulés par l'IA	Tous systèmes d'IA interagissant avec des personnes physiques, tous systèmes d'IA générant ou manipulant du contenu, dont les GPAI	Fournisseurs, Déployeurs	**Signaler, de manière claire et lisible, aux personnes physiques qu'elles interagissent avec un système d'IA** (art. 50, pt. 1). Cette exigence générale de transparence tend à permettre aux individus de différencier les interlocuteurs virtuels et humains. Cette garantie revêt une importance particulière face au développement du management algorithmique. **Signaler, de manière claire et lisible, les contenus générés ou manipulés par l'IA** (art. 50, pt. 2). Cette exigence générale de transparence tend à permettre aux individus d'identifier les contenus générés, intégralement ou partiellement, par un système d'IA. Appliquée à la gestion du personnel, cette obligation impose d'informer les salariés, candidats et représentants du personnel de l'utilisation de contenus produits ou modifiés par l'IA (par exemple, pour des évaluations ou des réponses automatisées). Cette information pourrait constituer un élément d'appréciation lors de l'évaluation des travailleurs et nourrir les réflexions sur la juste rémunération du travail humain[45].
		Déployeurs	**Informer les personnes exposées à un système d'IA émotionnelle ou de catégorisation biométrique** (art. 50, §3). Lorsque l'usage d'un tel système d'IA est autorisé, le déployeur a l'obligation d'informer les personnes concernées sur son utilisation et son fonctionnement. Un employeur qui utilise une technologie d'IA pour analyser les émotions ou catégoriser biométriquement des salariés doit préalablement les informer sur ce recours et son fonctionnement. Cette obligation s'inscrit dans le prolongement des obligations de transparence instituées par les articles L. 1222-3 et L. 1222-4 et du Code du travail en faveur des salariés. Par ailleurs, elle doit être combinée avec l'obligation d'information du CSE sur les méthodes de contrôle de l'activité des salariés et les traitements automatisés de gestion du personnel (C. trav., art. L. 2312-38).

45 L'obligation d'identifier le contenu généré ou manipulé par l'IA fait écho aux enjeux liés à la protection de la propriété intellectuelle et notamment aux préoccupations exprimées par les professionnels des secteurs du cinéma et de la production de l'audiovisuel. V. not. : C. Bouckaert, J.-M. Cavada, « Intelligence artificielle et propriété intellectuelle : quels progrès ? », *Cahiers français*, 2024/5, n° 441, p. 82.

Droit à l'explication des personnes physiques	Haut risque.	Déployeurs	**Fournir, sur demande, à la personne concernée une explication sur la décision automatisée qui l'affecte de manière significative** (art. 86 ; consid. 171 et 485). Toute personne peut demander une explication lorsqu'elle fait l'objet d'une décision, totalement ou partiellement, automatisée qui produit des effets juridiques ou un préjudice important. L'information porte alors sur les principales raisons ayant conduit à la décision, mais aussi sur la place donnée aux données de sortie dans le processus décisionnel. Cette obligation à l'explicabilité participe de la capacité des individus à contester la décision automatisée. L'employeur qui utilise des systèmes d'IA en matière de gestion du personnel pour prendre des décisions salariales doit demeurer en mesure d'expliquer les choix opérés et les mesures prises à l'égard des salariés. Ce droit à l'explication réduit d'autant la place laissée au discrétionnaire dans la gestion des relations de travail. En même temps, son champ est limité aux décisions ayant un impact significatif. Lorsqu'une décision partiellement ou intégralement automatisée est prise à l'égard d'un travailleur de plateforme, l'obligation est renforcée pour l'entreprise de plateforme par l'exigence de fournir une motivation écrite. Le travailleur a également la possibilité de demander des explications et un réexamen humain pour toute décision automatisée (Directive sur le travail de plateforme, art. 9 et 11).

Information des travailleurs et de leurs représentants	Haut risque	Déployeurs	**Informer en amont les salariés et le CSE du déploiement du système d'IA sur le lieu de travail** (art. 26, §7 ; consid. 92, 93, 443 et 444). Les salariés et leurs représentants doivent être informés avant la mise en œuvre d'outils d'IA dans les processus les impliquant, en particulier lorsqu'ils peuvent avoir une incidence sur les conditions de travail, la santé et la sécurité ou les droits fondamentaux (consid. 92) L'information couvre un nombre important d'éléments listés : la finalité du système d'IA, la nature des opérations, ses capacités, ses limites, ses principales caractéristiques ainsi que les modalités de surveillance humaine et les procédures de recours (art. 26, §7 ; consid. 93). Il s'en déduit qu'est attendue une information complète portant sur le fonctionnement de l'algorithme ainsi que son incidence potentielle sur les conditions de travail. Du reste, cette exigence ne se substitue pas aux règles en vigueur en matière d'information des salariés et d'information-consultation du CSE. Cette garantie supplémentaire constitue une obligation spécifique lorsque l'intégration de l'IA dans l'entreprise ne relève d'aucune autre obligation d'information ou de consultation. Le CSE doit ainsi être informé lorsque l'entreprise prévoit de déployer un système d'IA à haut risque, alors même que les conditions des informations-consultations obligatoires prévues à l'article L. 2312-8 du Code du travail ne sont pas réunies (notamment s'il ne s'agit pas de l'introduction d'une nouvelle technologie ou si elle n'emporte pas une modification importante des conditions de travail). Lorsque le système d'IA est déployé dans le cadre d'une plateforme numérique, l'employeur doit combiner les exigences susmentionnées avec les obligations d'information et de motivation instituées par l'article 9 de la Directive sur le travail de plateforme. Les travailleurs bénéficient, dans ce cadre, d'une information approfondie sur l'utilisation de systèmes automatisés de surveillance et de prise de décision ou encore de restrictions du compte et de rupture du contrat (§1 et §3). Les représentants des travailleurs en sont également destinataires (§1 et §4). Ces informations doivent être présentées de façon claire, transparente, intelligible et accessible (§2).

Tableau 5. La règle d'accessibilité et de non-discrimination

Obligation	Catégorie(s) des systèmes d'IA concernés	Personne(s) assujettie(s) à l'obligation	Descriptif de l'obligation
Accessibilité à des systèmes d'IA non-discriminatoires et compréhensibles	Haut risque	Fournisseurs, Déployeurs.	**Concevoir des systèmes d'IA accessibles, non-discriminatoires et compréhensibles pour tous les utilisateurs** (art. 10 et 15 ; consid. 80, 338 et 436) Les systèmes d'IA doivent être conçus pour être utilisables par toute personne, y compris des individus en situation de handicap. Cette exigence s'inscrit dans le prolongement des exigences européennes en matière d'accessibilité numérique[46]. L'*AI Act* rappelle que ces technologies n'échappent pas au principe de la non-discrimination. La conception d'un système d'IA et le choix des données utilisées pour l'entraîner, le valider et le tester doivent permettre d'éviter ou de limiter les biais discriminatoires. La haute qualité des données est cruciale (cf. *Gouvernance et qualité des données*). L'exigence de compréhensibilité soutient l'objectif de disposer d'une IA inclusive[47]. Les systèmes d'IA doivent être accompagnés d'instructions claires permettant aux personnes de les utiliser de manière appropriée (art. 13, §1) ainsi que de comprendre leur fonctionnement et leurs résultats produits (consid. 70). Le respect de cette obligation implique de prévoir des compensations techniques en cas de difficultés d'utilisation rencontrées par des salariés, notamment en raison d'un handicap, afin d'assurer un égal accès aux technologies.

Conclusion

Ce panorama des usages de l'IA et de leur encadrement à l'aune de l'*AI Act* met en exergue les enjeux techniques et juridiques liés au déploiement de ces technologies dans les organisations de travail. Les acteurs de l'emploi sont d'ores et déjà confrontés à plusieurs défis.

D'abord, l'*AI Act* établit une réglementation graduée en fonction du niveau de risques. La qualification et le régime juridique de chaque système d'IA dépendent de la technologie utilisée et de son domaine d'application. Aussi, la licéité (ou non) d'un type d'outil ou de logiciel ne peut être affirmée de manière péremptoire ou immuable. Au sens du droit de l'Union européenne, le système d'IA se caractérise, en effet,

46 La Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services est entrée en vigueur le 28 juin 2025. V. également : Directive (UE) 2016/2102 du Parlement européen et du Conseil du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du service public.

47 Pour une réflexion sur l'IA inclusive, v. not. : K. Noori, *A disability-inclusive Artificial Intelligence Act*, EDF Artificial Intelligence Policy Office, octobre 2024.

par sa capacité d'adaptabilité de sorte que son fonctionnement et ses effets peuvent varier au fil du temps du fait de recodage, de reparamétrage et selon la qualité des données implémentées. Cette mouvance technologie a d'ailleurs été appréhendée à travers l'instauration d'obligations de suivi tout au long de la durée de vie du système informatique et la prévision d'évolutions futures du texte européen.

Ensuite, les multiples allers-retours législatifs ont donné corps à une réglementation européenne dense et complexe, composée de règles modulées en fonction du niveau de risque et assorties d'exceptions (parfois) subtiles. La portée concrète de l'*AI Act* reste donc incertaine du fait de l'enchevêtrement de règles particulières et de régimes dérogatoires. Il existe également un risque d'invisibilisation et de contournement. Certaines pratiques d'IA pourtant risquées pourraient être dissimulées, volontairement ou non, derrière des critères d'apparence neutre. Outre l'affirmation d'une responsabilité algorithmique des employeurs, ce texte exhorte les acteurs de l'emploi à un devoir accru de diligence et devrait s'accompagner d'un renforcement du dialogue social.

Enfin (et surtout), la réglementation européenne ne se substitue nullement aux législations existantes applicables selon les secteurs, les types de données ou la finalité de systèmes d'IA. Il convient donc de le combiner avec les autres corpus juridiques, tels que le droit du travail[48], le droit de la non-discrimination ou encore le droit de la protection des données. Tout l'enjeu réside aujourd'hui dans notre capacité à articuler ces normes et à contrôler leur respect. D'ailleurs, l'IA pourrait être une voie à emprunter pour améliorer la santé, la sécurité[49] et les conditions de travail[50] ou encore le respect du droit du travail[51]…

48 V. not. : S. Sereno, « Le déploiement de l'IA dans le monde du travail : entre pratiques et (non-)droits », *RDT*, 2025, n° 1, p. 41.

49 INRS, *L'intelligence artificielle au service de la santé et sécurité au travail. Enjeux et perspectives à l'horizon 2035*, 11/2022.

50 V. not. : J.-M. Truffat, rapp., *Analyse de controverses : intelligence artificielle, travail et emploi*, Étude préc., p. 12 ; en matière de santé : Organisation internationale du travail, *Révolutionner la santé et la sécurité. Le rôle de l'IA et de la numérisation au travail*, rapp., 2025, p. 27.

51 V. not. : A. Huibregtse, « L'IA propose des moyens innovants pour améliorer le respect des lois du travail », Observatoire de l'OIT sur l'IA et le travail de l'économie numérique, 3 février 2025 <https://www.ilo.org/fr/resource/article/lia-propose-des-moyens-innovants-pour-ameliorer-le-respect-des-lois-du>, consulté le 9 juillet 2025.