FO Cadres

Juin 2026

LIVRE BLANC

IA ET DIALOGUE SOCIAL

Négocier l'IA pour une innovation responsable

Guide à usage des militants et élus syndicaux

Édito

Le développement rapide des technologies d'intelligence artificielle (IA) soulève des enjeux majeurs dans le monde du travail. L'IA n'est plus une innovation marginale : elle est désormais intégrée dans les logiciels de gestion des ressources humaines, les outils de planification, les dispositifs d'évaluation de la performance, les centres de contact, les systèmes de sécurité informatique, les outils bureautiques dits « copilotes » ainsi que dans les chaînes de production et de maintenance. Elle intervient ainsi, directement ou indirectement, dans des décisions qui touchent au cœur de la relation de travail.

Dès lors qu'un système algorithmique influence l'organisation ou les conditions de travail, il ne s'agit plus d'une simple question technique mais d'un enjeu central du dialogue social relevant notamment des compétences des représentants du personnel.

Les organisations syndicales sont donc appelées à intervenir afin de définir des usages acceptables de l'IA, de maintenir une vigilance à l'égard des systèmes à haut risque, de défendre les droits des travailleurs et leur intégrité physique et psychique face aux transformations technologiques, et d'accompagner les mutations professionnelles.

Dans cette perspective de prévention et de responsabilité, ce guide a été conçu comme un outil d'action destiné à celles et ceux qui, au sein des entreprises et des structures FO, sont amenés à intervenir lorsque des outils d'intelligence artificielle sont introduits, expérimentés ou généralisés. Ces systèmes sont souvent déployés sans véritable débat, sous des appellations telles que « optimisation », « pilotage par la donnée », « assistant » ou « automatisation », alors même qu'ils peuvent relever de procédures d'information et de consultation et transformer en profondeur l'organisation du travail : modalités d'évaluation des salariés, charge et rythme de travail,

marges d'autonomie, formes de contrôle et de surveillance ou encore perspectives de carrière. Dans ce contexte, les membres du comité social et économique ainsi que ceux des commissions santé, sécurité et conditions de travail sont en première ligne. Leur rôle consiste notamment à identifier les dispositifs relevant de l'intelligence artificielle et, le cas échéant, du règlement sur l'intelligence artificielle (RIA), à demander les informations nécessaires, à décider d'un éventuel recours à l'expertise et à suivre dans la durée les effets de ces technologies sur les conditions de travail.

Ce guide ne vise donc pas à proposer une approche théorique de l'IA, mais à fournir un appui concret aux représentants du personnel confrontés à des projets souvent présentés comme techniques, inéluctables ou déjà arrêtés. Il offre un socle commun de références — compréhension du RIA, obligations de l'employeur et méthodes d'action — que chaque équipe syndicale pourra adapter à son contexte et aux réalités de son entreprise.

Éric Pérès
Secrétaire général de l'Union des cadres
et ingénieurs – FO

Sommaire

PARTIE #1

L'IA de quoi parle-t-on ?

1 L'IA de quoi parle-t-on ?

Avant de mobiliser le règlement sur l'intelligence artificielle (RIA) ou d'ouvrir une discussion en CSE, il convient de clarifier précisément de quoi l'on parle. Le terme « intelligence artificielle » est utilisé de façon très large, parfois délibérément floue, et souvent stratégique : une direction peut qualifier un outil d'« assistant » ou d'« outil d'optimisation » pour éviter de le soumettre aux obligations légales qui s'attachent aux systèmes d'IA.
Pour les représentants des salariés, la maîtrise de la définition n'est pas une question académique : c'est un levier juridique fondamental.

Cette section retrace d'abord l'histoire de l'intelligence artificielle pour montrer qu'elle n'est ni une innovation récente ni une révolution spontanée, mais le résultat d'une longue trajectoire scientifique, industrielle et politique. Elle présente ensuite les définitions juridiques qui s'imposent aujourd'hui aux entreprises et aux partenaires sociaux, en insistant sur leurs implications concrètes pour l'action syndicale.

L'IA n'est pas une nouveauté : une longue histoire d'ambitions et de désillusions

L'intelligence artificielle est souvent présentée comme une rupture récente, portée par des entreprises technologiques qui auraient tout inventé au XXIe siècle. Cette présentation est inexacte, et cette inexactitude n'est pas anodine : elle sert à construire un sentiment d'inévitabilité technologique qui prive les organisations syndicales de leur capacité à se projeter dans l'histoire longue du rapport entre technologie et travail. En réalité, l'intelligence artificielle est une discipline scientifique vieille de plus de soixante-dix ans, marquée par des cycles d'enthousiasme et de désillusion, et dont les avancées les plus récentes s'inscrivent dans une continuité théorique bien établie.

Les fondations théoriques (1943–1956)

Les premières formalisations de ce qui deviendra l'intelligence artificielle émergent dans les années 1940, au croisement de la logique mathématique, de la neurologie et de la cybernétique. En 1943, les mathématiciens Warren McCulloch et Walter Pitts publient un article fondateur proposant un modèle mathématique du neurone biologique, posant la première pierre de ce qui deviendra les réseaux de neurones artificiels. En 1945, le mathématicien John von Neumann formalise l'architecture du calculateur programmable, qui constituera le substrat matériel de toute l'informatique ultérieure.

Mais c'est Alan Turing qui, en 1950, pose la question philosophique et scientifique centrale dans un article resté célèbre : « *Computing Machinery and Intelligence* ». Il y propose ce qui sera connu sous le nom de « test de Turing » : peut-on distinguer, à travers un échange textuel, un être humain d'une machine ? Cette question n'est pas seulement philosophique — elle est opérationnelle. Elle définit un critère fonctionnel pour évaluer l'intelligence artificielle : non pas ce qu'une machine est intrinsèquement, mais ce qu'elle est capable de faire.

> « *Je propose d'examiner la question : les machines peuvent-elles penser ? […] Au lieu de tenter de produire un programme qui simule l'esprit adulte, que ne pas plutôt essayer de produire un programme qui simule l'esprit d'un enfant ?* » — **Alan Turing** | Computing Machinery and Intelligence, Mind, 1950

Cette approche fonctionnelle — définir l'IA par ses capacités et ses effets plutôt que par sa nature — est précisément celle qui a été retenue par le législateur européen soixante-dix ans plus tard dans la rédaction du règlement sur l'intelligence artificielle (RIA, 2024). C'est un premier pont entre l'histoire des sciences et le droit positif.

La naissance officielle d'une discipline (1956)

L'année 1956 marque la naissance institutionnelle de l'intelligence artificielle comme discipline scientifique autonome. À l'initiative de John McCarthy,

Marvin Minsky, Nathaniel Rochester et Claude Shannon, une conférence d'été est organisée à Dartmouth College (New Hampshire, États-Unis). La proposition soumise aux participants affirme que « *tout aspect de l'apprentissage ou toute autre caractéristique de l'intelligence peut être décrit avec une telle précision qu'une machine peut être conçue pour le simuler* ».

Cette formulation est d'une importance considérable. Elle pose deux hypothèses fondamentales qui ont structuré toute la recherche ultérieure : premièrement, l'intelligence humaine est décomposable en fonctions décrivables avec précision ; deuxièmement, ces fonctions peuvent être implémentées dans une machine. Ces deux hypothèses sont aujourd'hui au cœur des débats juridiques sur la responsabilité des systèmes d'IA et sur la question du contrôle humain — l'une des obligations centrales du RIA.

La conférence de Dartmouth voit également naître les premiers programmes d'IA au sens strict : le *Logic Theorist* d'Allen Newell et Herbert Simon, capable de démontrer des théorèmes mathématiques, et le *General Problem Solver*, qui constitue une tentative de modéliser le raisonnement humain général. Ces programmes reposent sur la manipulation symbolique de règles logiques — ce que l'on appellera plus tard l'IA symbolique, première grande famille des systèmes d'IA.

Les cycles de l'IA : entre promesses et hivers

L'histoire de l'intelligence artificielle est structurée par une alternance remarquable de phases d'optimisme intense et de périodes de retrait, que les historiens des sciences nomment les « hivers de l'IA ». Comprendre cette dynamique est utile aux représentants du personnel : elle permet de relativiser les discours d'inévitabilité technologique et de comprendre que les choix de déploiement sont toujours des choix politiques et économiques, jamais de simples nécessités techniques.

Le premier âge d'or (1956–1974) est marqué par un optimisme sans limites. Les pionniers annoncent que les machines équivaudront aux humains dans toutes leurs tâches cognitives dans moins d'une génération. Ces prédictions se révèlent très largement inexactes, mais elles génèrent des financements considérables,

notamment de l'armée américaine et de la DARPA. Les limites des systèmes symboliques apparaissent progressivement : ils fonctionnent bien dans des domaines étroitement définis mais s'effondrent dès que la situation sort du périmètre prévu.

Le premier hiver de l'IA (1974–1980) est déclenché par la publication du rapport Lighthill en 1973 au Royaume-Uni, qui conclut à l'échec des ambitions les plus larges et conduit à une réduction drastique des financements publics. Cette phase de désillusion est instructive : elle montre que le déploiement de l'IA est conditionné autant par des décisions politiques et économiques que par des avancées scientifiques.

Le renouveau des années 1980 est porté par les systèmes experts — des programmes spécialisés dans un domaine précis (diagnostic médical, configuration industrielle, conseil juridique) qui connaissent une diffusion commerciale significative. L'entreprise DEC déploie en 1982 le système XCON pour configurer ses commandes d'ordinateurs, économisant selon elle 40 millions de dollars par an. C'est la première vague de déploiement massif de l'IA dans les organisations du travail — et les premières questions syndicales sur l'automatisation des compétences qualifiées.

Le deuxième hiver (1987–1993) résulte de l'effondrement du marché des stations de travail spécialisées pour l'IA et des limites des systèmes experts dans des environnements dynamiques et incertains. Cette période marque néanmoins un tournant : la recherche se déplace progressivement vers l'apprentissage automatique, abandonnant partiellement la programmation explicite des connaissances au profit de l'apprentissage à partir de données.

La période 1993–2010 voit l'avènement du *Machine Learning* et les premières applications grand public : les moteurs de recherche, les filtres anti-spam, les systèmes de recommandation. En 1997, Deep Blue d'IBM bat le champion du monde d'échecs Garry Kasparov — événement médiatique qui marque l'entrée de l'IA dans la conscience collective. En 2006, Geoffrey Hinton relance l'intérêt pour les réseaux de neurones profonds (*Deep Learning*), ouvrant la voie à la vague suivante.

L'accélération contemporaine (2010–2026) est sans précédent. La conjonction de trois facteurs l'explique : la disponibilité de masses de données numériques (big data), la puissance de calcul des processeurs graphiques (GPU), et les avancées théoriques du *Deep Learning*. En 2012, le réseau AlexNet réduit de moitié le taux d'erreur en reconnaissance d'images sur la compétition ImageNet. En 2016, AlphaGo bat le champion du monde de jeu de Go, un jeu réputé inaccessible aux machines pour sa complexité combinatoire. En 2022, GPT-3 puis GPT-4 inaugurent l'ère de l'IA générative grand public, transformant en profondeur les pratiques professionnelles dans un nombre considérable de secteurs.

À RETENIR

• **L'IA n'est pas née en 2022.** Elle a soixante-dix ans d'histoire, jalonnée de cycles d'optimisme et de désillusion. Cette histoire long terme doit nourrir la prudence face aux discours d'inévitabilité technologique.

• **Les transformations du travail liées à l'IA ne sont pas automatiques.** Elles résultent de choix organisationnels, politiques et économiques qui peuvent être discutés, orientés et encadrés par le dialogue social.

• **Les premières questions syndicales sur l'IA datent des années 1980,** lorsque les systèmes experts ont commencé à automatiser des tâches qualifiées. Cette expérience historique est une ressource pour l'action présente.

Chronologie commentée — L'IA et le monde du travail

ÉTAPE HISTORIQUE		IMPORTANCE POUR LE MONDE DU TRAVAIL
Fondations théoriques (McCulloch & Pitts, Turing). Premier modèle de neurone artificiel. Test de Turing (1950).	**1943 – 1950**	Naissance du concept de machine pensante. Première formulation de la question : une machine peut-elle imiter l'intelligence humaine ?
Conférence de Dartmouth : naissance officielle de l'IA comme discipline scientifique. Première définition formelle.	**1956**	L'IA est reconnue comme domaine de recherche autonome. Ambition initiale : reproduire l'ensemble des capacités cognitives humaines.
IA symbolique et systèmes experts. Programmes de démonstration de théorèmes, de résolution de problèmes (GPS).	**1960 – 1970**	Premiers systèmes d'automatisation de raisonnements. Application dans les industries (diagnostic, planification).
Premier « hiver de l'IA » : réduction drastique des financements. Limites des systèmes symboliques.	**1974 – 1980**	Prise de conscience des limites de l'automatisation : les tâches humaines sont plus complexes que prévu.
Renouveau avec les systèmes experts commerciaux (XCON, MYCIN). Développement dans les entreprises.	**1980 – 1987**	Première vague de déploiement industriel. Émergence des questions d'assistance à la décision et de substitution.
Deuxième « hiver de l'IA » : effondrement du marché des systèmes experts.	**1987 – 1993**	L'IA n'est pas la panacée. Les organisations apprennent la nécessité d'encadrer le déploiement.
Apprentissage automatique (*Machine Learning*). Victoire de Deep Blue aux échecs (1997). Moteurs de recherche.	**1993 – 2010**	Changement de paradigme : l'IA apprend à partir de données. Diffusion progressive dans les outils de gestion.
Deep Learning, big data, GPU. ImageNet (2012). AlphaGo (2016). Reconnaissance vocale, traitement du langage.	**2010 – 2022**	Accélération massive. L'IA pénètre les RH, le recrutement, la logistique, la surveillance. Premiers débats éthiques.
IA générative (GPT-4, Claude, Gemini, LLaMA). Agents IA. Adoption de masse en entreprise. IA Act (2024).	**2022 – 2026**	Rupture : l'IA devient un outil du quotidien professionnel. Encadrement juridique d'urgence au niveau européen.

À RETENIR L'histoire de l'IA est une histoire de cycles politiques et économiques autant que scientifiques. À chaque vague, les effets sur le travail ont été sous-estimés dans les phases d'enthousiasme et surestimés dans les phases de retrait. La vigilance syndicale doit être permanente et ne pas se laisser dicter son agenda par l'intensité médiatique du moment.

Définir l'IA en droit : un enjeu de qualification aux conséquences concrètes

La définition juridique de l'intelligence artificielle n'est pas une question abstraite réservée aux juristes spécialisés. Elle conditionne directement l'applicabilité de l'ensemble des obligations légales qui s'attachent à ces systèmes — en particulier celles du règlement européen sur l'intelligence artificielle, du RGPD et du Code du travail. Pour les représentants du personnel, savoir qualifier un système est donc un outil d'action : c'est ce qui permet d'exiger des documents, d'imposer une consultation et de contester un déploiement.

La définition centrale du Règlement européen sur l'IA (RIA, 2024)

Le règlement européen sur l'intelligence artificielle, adopté en 2024 et entré en vigueur progressivement à partir du 2 février 2025, constitue le premier cadre juridique horizontal contraignant applicable aux systèmes d'IA dans l'Union européenne. Son article 3, paragraphe 1, en donne la définition suivante :

>> « *Un système d'intelligence artificielle est un système basé sur une machine, conçu pour fonctionner avec des degrés variables d'autonomie, qui peut faire preuve d'adaptabilité après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des données qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions, susceptibles d'influencer des environnements physiques ou virtuels*. » — **Règlement (UE) 2024/1689 dit « *AI Act* »** — Article 3 §1 | Journal officiel de l'UE, 12 juillet 2024

Quatre critères permettent de qualifier un système d'IA au sens du RIA, et chacun mérite une attention particulière des représentants du personnel

1 **Premièrement, le critère de la machine.**
Le système doit être basé sur une machine — un dispositif informatique. Cette précision exclut les processus purement humains ou les procédures organisationnelles, mais inclut toute forme de logiciel, d'application ou de dispositif automatisé dès lors qu'il remplit les autres critères. Le terme « machine » est volontairement large : il couvre les systèmes hébergés dans le *cloud*, les applications mobiles et les systèmes embarqués dans des équipements industriels.

2 **Deuxièmement, le critère de l'autonomie variable.**
Le système fonctionne « avec des degrés variables d'autonomie ». Cette formulation est essentielle : elle inclut aussi bien les systèmes qui exécutent des tâches de manière totalement autonome que ceux qui assistent un humain en lui proposant une recommandation. Un outil qui génère automatiquement une liste de candidats classés est un système d'IA même si un recruteur humain prend formellement la décision finale.

3 **Troisièmement, le critère de l'inférence à partir de données.**
Le système déduit, à partir des données qu'il reçoit, la manière de générer ses sorties. C'est ce critère qui distingue un système d'IA d'un simple programme informatique déterministe suivant des instructions fixes. Un système qui applique mécaniquement des règles prédéfinies sans les avoir inférées de données peut, selon les circonstances, ne pas relever du RIA — bien qu'il reste soumis au Code du travail s'il affecte l'organisation du travail.

4 **Quatrièmement, le critère de l'influence sur les environnements.**
Les sorties du système — prédictions, contenus, recommandations, décisions — sont susceptibles d'influencer des environnements physiques ou virtuels. Ce critère est particulièrement large : toute recommandation RH, toute note de performance générée par algorithme, tout planning automatisé entre dans ce champ dès lors qu'il peut influencer une décision ou une situation concrète.

À RETENIR

Le RIA ne s'applique pas pour :
• Les systèmes purement symboliques (règles fixes, sans inférence à partir de données) dans certaines interprétations — bien qu'une qualification au cas par cas soit nécessaire.
• Les usages militaires, de défense ou de sécurité nationale.
• Les systèmes développés exclusivement pour la recherche scientifique. Attention : un système issu de la recherche et déployé en production entre dans le champ du RIA dès sa mise en service.
• Les utilisateurs individuels dans un cadre strictement personnel.

En revanche, un logiciel standard (traitement de texte, tableur) qui intègre des fonctionnalités d'IA relève du RIA pour ces seules fonctionnalités, même si l'outil global ne se présente pas comme un « système d'IA ».

La définition de l'OCDE : une référence internationale

La définition adoptée par l'OCDE dans sa Recommandation du Conseil sur l'intelligence artificielle (OECD/LEGAL/0449, 2019, révisée en 2023) constitue la référence internationale la plus largement adoptée. Elle a directement inspiré la définition retenue par le règlement européen :

>> *« Un système d'IA est un système basé sur une machine qui, pour des objectifs explicites ou implicites, déduit, à partir des données qu'il reçoit, comment générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions pouvant influencer des environnements physiques ou virtuels. Les systèmes d'IA varient dans leurs niveaux d'autonomie et d'adaptabilité après leur déploiement. »* — **OCDE** — Recommandation du Conseil sur l'intelligence artificielle | OECD/LEGAL/0449 (révisé 2023)

L'importance de la définition OCDE tient à son adoption par quarante-six pays membres et partenaires, dont l'ensemble des États membres de l'Union européenne, les États-Unis, le Japon, le Brésil et l'Inde. Elle constitue également la base des travaux de l'Organisation internationale du travail (OIT) sur le management algorithmique, ce qui lui confère une portée directe dans le champ du droit du travail international. La révision de 2023 a précisé la notion d'autonomie et d'adaptabilité après déploiement, alignant la définition sur les enjeux posés par les systèmes d'apprentissage automatique capables d'évoluer après leur mise en service.

La définition fonctionnelle retenue par les juridictions du travail

Le Code du travail français ne contient pas de définition de l'intelligence artificielle. En l'absence de texte spécifique, les juridictions sociales ont développé une approche fonctionnelle : ce qui compte n'est pas la qualification technique du système mais son effet sur l'organisation du travail et sur les droits des salariés.

Cette approche a été clairement affirmée dans deux décisions récentes majeures.

Le Tribunal judiciaire de Nanterre, dans son ordonnance du 29 janvier 2026 (n° 25/02856), a jugé que l'introduction d'un outil intégrant des fonctionnalités d'intelligence artificielle constitue une nouvelle technologie au sens de l'article L.2312-8 du Code du travail, dès lors que ce système est utilisé pour des fonctions sensibles telles que la gestion des compétences, l'affectation des salariés aux missions et la préparation des entretiens annuels. Le tribunal a ordonné la suspension du déploiement dans l'attente de la consultation du CSE. Cette décision est d'une importance pratique considérable : elle établit que l'obligation de consultation ne dépend pas de la qualification du système par l'employeur, mais de ses effets concrets sur le travail.

Le Tribunal judiciaire de Créteil, dans une décision du 15 juillet 2025, a confirmé cette orientation en précisant que la procédure d'information-consultation doit intervenir avant toute décision définitive de l'employeur, y compris lorsque l'outil est présenté comme une simple « mise à jour » ou une « évolution

fonctionnelle » d'un logiciel existant. Cette précision est directement utile aux élus confrontés à des employeurs qui tentent de soustraire un déploiement à l'obligation de consultation en le présentant comme une amélioration technique marginale.

>> « *Ce qui est déterminant n'est pas la nature de la technologie utilisée mais ses effets réels sur les conditions de travail et les processus décisionnels. Dès lors qu'un système algorithmique contribue à déterminer des affectations, à hiérarchiser des priorités ou à produire des éléments d'évaluation, il constitue une composante du dispositif de gouvernance de l'entreprise.* » — **Tribunal judiciaire de Nanterre**, 29 janvier 2026 (n° 25/02856) | TJ Nanterre, ord. réf., 29 janv. 2026

Cette jurisprudence s'inscrit dans la continuité d'une doctrine ancienne du droit social français, qui a toujours soumis l'introduction de nouvelles technologies à des obligations d'information et de consultation des représentants du personnel. La loi du 13 novembre 1982 (dite « loi Auroux ») avait déjà consacré ce principe en inscrivant dans le Code du travail l'obligation de consulter les comités d'entreprise sur les projets d'introduction de nouvelles technologies susceptibles d'affecter les conditions de travail. Ce droit, renforcé par les ordonnances de 2017 qui ont créé le Comité social et économique (CSE), constitue aujourd'hui le principal levier d'action syndicale face au déploiement de l'IA.

La définition de la CNIL et son articulation avec le RGPD

La Commission nationale de l'informatique et des libertés (CNIL) n'a pas adopté de définition formelle de l'intelligence artificielle distincte de celle du RIA, mais ses guides pratiques sur l'IA (2022, 2023, 2024) proposent une approche opérationnelle centrée sur les traitements de données personnelles. La CNIL attire l'attention sur un point souvent méconnu des acteurs de terrain : conformité RGPD et conformité RIA sont deux exigences distinctes et cumulatives.

Un système d'IA peut être parfaitement conforme au RGPD — avoir une base légale valide pour le traitement des données personnelles, respecter le principe de minimisation, informer les personnes concernées — et pourtant être non conforme au RIA, par exemple parce qu'il constitue un système à haut risque

déployé sans documentation technique adéquate ou sans contrôle humain réel. Inversement, un système d'IA peut respecter les exigences du RIA en matière de gouvernance et de traçabilité tout en présentant des lacunes dans le traitement des données personnelles qu'il exploite.

Cette distinction est d'une importance pratique majeure pour les représentants du personnel : elle signifie qu'un employeur qui présente un avis favorable de son délégué à la protection des données (DPO) ou une analyse d'impact RGPD (DPIA) ne s'est pas pour autant acquitté de ses obligations au titre du RIA ni de ses obligations au titre du Code du travail.

Tableau comparatif des définitions juridiques applicables

SOURCE	DÉFINITION	PORTÉE JURIDIQUE
RIA (AI Act) art. 3 §1 (UE, 2024)	Un système basé sur une machine, conçu pour fonctionner avec des degrés variables d'autonomie, susceptible d'évoluer après sa mise en service, et qui, à partir des données reçues, génère des sorties (prédictions, contenus, recommandations, décisions) influençant des environnements physiques ou numériques.	Définition contraignante pour toutes les entreprises opérant dans l'UE. Détermine l'applicabilité du règlement et les obligations associées. Toute qualification erronée engage la responsabilité du déployeur
OCDE OECD/LEGAL/0449 (2019, révisé 2023)	Un système basé sur une machine qui, pour des objectifs explicites ou implicites, déduit, à partir des données qu'il reçoit, comment générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions pouvant influencer des environnements physiques ou virtuels. Les systèmes varient dans leurs niveaux d'autonomie et d'adaptabilité.	Définition de référence internationale adoptée par 46 pays. Sert de base à la définition retenue par le RIA. Utilisée dans les travaux de l'OIT sur le management algorithmique.
Parlement européen Résolution 2017/2013 (précédant le RIA)	Un système capable d'acquérir, de traiter, d'adapter et de transférer des informations, de raisonner sur des données et de fournir des résultats adaptés à des objectifs spécifiques.	Définition transitoire, avant l'adoption du RIA. Pose le principe de l'adaptabilité comme caractéristique centrale, distinguant l'IA des simples logiciels déterministes.

SOURCE	DÉFINITION	PORTÉE JURIDIQUE
CNIL Guides pratiques (2022-2024)	Tout système automatisé utilisant des méthodes d'apprentissage statistique ou symbolique pour traiter des données et produire des résultats (décisions, recommandations, classifications) ayant un impact sur les droits des personnes.	Interprétation retenue pour l'application du RGPD aux systèmes d'IA. Guide les obligations en matière de protection des données personnelles dans les contextes professionnels.
Code du travail (jurisprudence) TJ Nanterre, 2026	Toute technologie automatisée susceptible de modifier l'organisation du travail, les méthodes d'évaluation ou les conditions d'emploi, indépendamment de sa qualification comme « IA » par l'employeur.	Définition fonctionnelle retenue par les juridictions sociales. L'appellation commerciale ou technique importe peu : c'est l'effet sur le travail qui détermine l'obligation de consultation du CSE.

L'enjeu de la qualification juridique

L'enjeu de la qualification n'est pas théorique : il détermine directement les droits et obligations qui s'appliquent.

Si un système est qualifié de système d'IA au sens du RIA : l'employeur est soumis aux obligations du règlement selon le niveau de risque du système. Pour les systèmes à haut risque — catégorie dans laquelle entrent la plupart des outils d'IA utilisés en matière de recrutement, d'évaluation et de gestion des travailleurs — ces obligations incluent la mise en place d'un contrôle humain réel, la documentation technique, la traçabilité des décisions, l'information des salariés et la gestion des risques. Le non-respect de ces obligations peut exposer l'entreprise à des sanctions allant jusqu'à 15 millions d'euros ou 3 % de son chiffre d'affaires mondial.

Si un système affecte l'organisation du travail, les conditions d'emploi ou les méthodes d'évaluation : l'employeur est soumis à l'obligation d'information et de consultation du CSE au titre du Code du travail, indépendamment de la qualification RIA du système. La jurisprudence récente confirme que cette obligation s'applique même à des systèmes qui ne relèvent pas formellement du champ du RIA.

Si un système traite des données personnelles : le RGPD s'applique, avec ses obligations de base légale, de minimisation des données, d'analyse d'impact et de droits des personnes. Le droit à l'explication prévu par l'article 22 du RGPD s'applique en cas de décision entièrement automatisée produisant des effets juridiques ou affectant significativement une personne.

À RETENIR La question que les représentants du personnel doivent poser en premier n'est pas « Est-ce vraiment de l'IA ? » mais « Cet outil produit-il des résultats — recommandations, classements, prédictions, décisions — susceptibles d'influencer l'organisation du travail ou des décisions concernant des personnes ? » Si la réponse est oui, la qualification s'impose et les obligations légales s'enclenchent — qu'il s'agisse du RIA, du RGPD ou du Code du travail.

• **La définition du RIA (art. 3 §1) est contraignante.** Tout système remplissant les quatre critères (machine, autonomie, inférence à partir de données, influence sur l'environnement) relève du règlement, quelle que soit l'appellation commerciale utilisée par l'employeur.

• **Les juridictions sociales retiennent une définition fonctionnelle :** c'est l'effet sur le travail qui compte, pas la qualification technique. Un système peut être soumis aux obligations de consultation du CSE sans relever formellement du RIA.

• **RGPD et RIA sont cumulatifs, non alternatifs**. La conformité à l'un ne dispense pas de la conformité à l'autre. Un employeur qui présente une DPIA n'a pas pour autant rempli ses obligations au titre du RIA.

• **La qualification est un outil syndical.** Exiger que l'employeur qualifie formellement un système et justifie cette qualification est un droit — et un levier pour imposer la consultation et la négociation.

PARTIE #2

Les différentes formes d'IA

2 Les différentes IA et leurs modes d'apprentissage

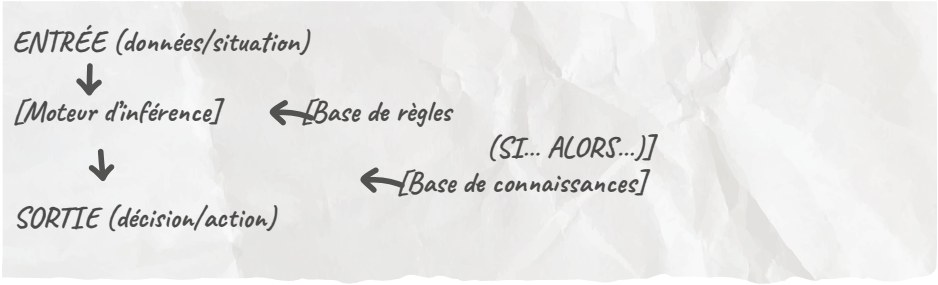
L'intelligence artificielle recouvre une grande diversité de technologies. Toutes ne fonctionnent pas de la même manière, n'ont pas les mêmes effets sur l'organisation du travail et ne soulèvent pas les mêmes enjeux du point de vue des salariés. Pour les représentants du personnel, comprendre le type d'IA déployé dans l'entreprise est une condition préalable indispensable : c'est ce qui permet d'identifier les risques, de poser les bonnes questions en CSE et d'activer les bons leviers juridiques — notamment au regard du règlement sur l'intelligence artificielle (RIA).

Cette partie présente chaque grande famille d'IA en décrivant son mode de fonctionnement, ses usages dans le monde du travail et les enjeux syndicaux qu'elle soulève. Elle se conclut par des tableaux de synthèse comparatifs permettant d'identifier rapidement le type de système en présence et les obligations qui s'y attachent.

L'IA symbolique ou IA basée sur des règles

L'IA symbolique constitue l'approche historique et la plus ancienne de l'intelligence artificielle. Elle repose sur des règles logiques explicites, formulées et codées par des êtres humains. Le système n'apprend pas de manière autonome : il applique mécaniquement une logique du type « si telle condition est remplie, alors telle décision est prise ». Son comportement est donc entièrement déterminé par les règles qu'on lui a définies, ce qui le rend prévisible, mais peu flexible face à des situations nouvelles ou non anticipées.

Schéma de fonctionnement — IA symbolique



Fonctionnement technique

L'architecture d'un système symbolique repose sur trois composants. La base de règles contient l'ensemble des instructions logiques (ex. : « si le candidat n'a pas le diplôme requis, rejeter la candidature »). La base de connaissances rassemble les faits et données utilisés pour évaluer les conditions (profils de candidats, seuils de performance, paramètres métiers). Le moteur d'inférence est le composant qui applique les règles aux données disponibles et produit une décision ou une recommandation. Ce moteur peut fonctionner de manière déductive (appliquer des règles générales à des cas particuliers) ou abductive (remonter d'effets observés vers des causes probables). L'IA symbolique n'évolue pas d'elle-même : toute modification de son comportement exige une intervention humaine explicite sur la base de règles.

Usages dans le monde du travail

On retrouve ce type de système dans de nombreux environnements professionnels, souvent sans que le terme « intelligence artificielle » soit utilisé. Les moteurs de règles métiers automatisent des procédures de traitement (validation de dossiers, routage d'alertes, génération de documents standardisés). Les systèmes experts sont utilisés dans le diagnostic technique, le conseil juridique ou la conformité réglementaire. Certains outils de tri de candidatures fonctionnent encore selon cette logique : une liste de mots-clés obligatoires, l'absence desquels entraîne automatiquement le rejet d'un dossier. Les assistants de réponse automatique (*chatbots* simples) et les outils de planification fondés sur des règles de priorité en sont d'autres illustrations.

Enjeux syndicaux spécifiques

• **Standardisation et rigidité :** les systèmes symboliques appliquent des règles uniformes, sans nuance ni prise en compte des situations individuelles. Ils peuvent exclure des profils atypiques, des parcours non-conventionnels ou des situations non prévues par les règles.
• **Déqualification :** lorsqu'un système symbolique prend en charge des décisions qui relevaient auparavant du jugement professionnel, il peut conduire à une perte d'autonomie et à une dévalorisation des compétences d'analyse et d'appréciation.
• **Responsabilité diluée :** la décision est imputée au système, ce qui peut masquer les choix humains qui ont présidé à la définition des règles. La question « qui a décidé que cette règle était légitime ? » est souvent impossible à poser.
• **Apparente transparence trompeuse :** si la logique SI/ALORS semble explicable, les bases de règles sont souvent volumineuses et leur combinaison peut produire des effets non intentionnels difficilement identifiables.

QUESTIONS À POSER EN CSE

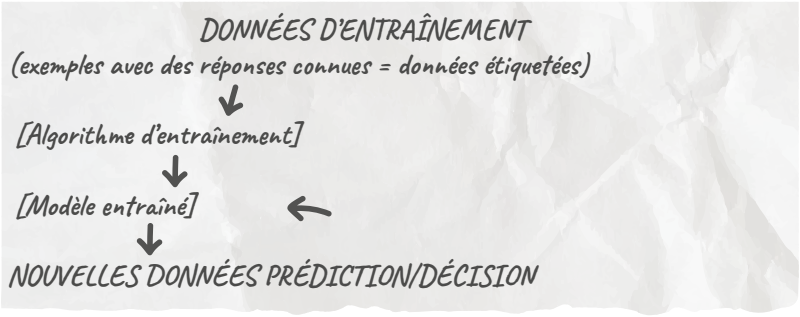
• **Quelles décisions sont automatisées** et lesquelles restent soumises à un examen humain ?
• **Qui a défini les règles** intégrées dans le système ? Sur quelle base ? Ces règles ont-elles été validées avec les équipes concernées ?
• Les règles peuvent-elles être **consultées et expliquées** aux salariés et aux élus ?
• Le système peut-il **être mis en cause** en cas de décision injuste ou inadaptée ? **Quelle procédure de contestation ?**
• Le déploiement de ce système a-t-il donné lieu à une **modification des tâches ou des qualifications** requises ?

L'apprentissage automatique (*Machine Learning*)

L'apprentissage automatique, ou *Machine Learning* (ML), constitue aujourd'hui la forme la plus répandue de l'intelligence artificielle dans les organisations. À la différence de l'IA symbolique, le système n'est pas programmé avec des règles explicites : il apprend à partir de données.

En analysant des volumes importants d'exemples, il identifie des corrélations, des régularités et des patterns statistiques qui lui permettent de produire des prédictions ou des décisions pour de nouvelles situations. Ce mode de fonctionnement implique trois grandes variantes selon la nature des données et de l'objectif poursuivi.

Schéma de fonctionnement —L'apprentissage supervisé



L'apprentissage supervisé

Le système apprend à partir de données pour lesquelles le résultat attendu est connu. On lui fournit des milliers ou des millions d'exemples (données étiquetées) : des CV acceptés et refusés, des dossiers de crédit remboursés ou défaillants, des pièces conformes ou défectueuses. L'algorithme ajuste progressivement ses paramètres internes pour produire des prédictions aussi proches que possible des résultats connus, puis est ensuite capable d'appliquer ce qu'il a appris à de nouveaux cas.

Les algorithmes d'apprentissage supervisé les plus courants comprennent les arbres de décision et les forêts aléatoires, qui construisent des règles de classification arborescentes ; les réseaux de neurones artificiels, qui modélisent des relations complexes non-linéaires ; les machines à vecteurs de support (SVM), utilisées pour des classifications à haute précision ; et les modèles de régression, qui prédisent des valeurs continues (niveau de performance, risque d'absentéisme, probabilité de départ).

Usages dans le monde du travail

• **Gestion des ressources humaines :** tri automatique de CV, scoring de candidats, prédiction de performance future, analyse des risques de départ (attrition), système de notation des entretiens d'évaluation.
• **Banque et assurance :** détection de fraude, évaluation du risque client, notation automatisée des dossiers de prêt.
• **Industrie :** maintenance prédictive (anticiper les pannes avant qu'elles surviennent), contrôle qualité automatisé par vision par ordinateur.
• **Logistique et distribution :** prévision de la demande, optimisation des stocks, détection d'anomalies dans les flux.

Enjeux syndicaux spécifiques

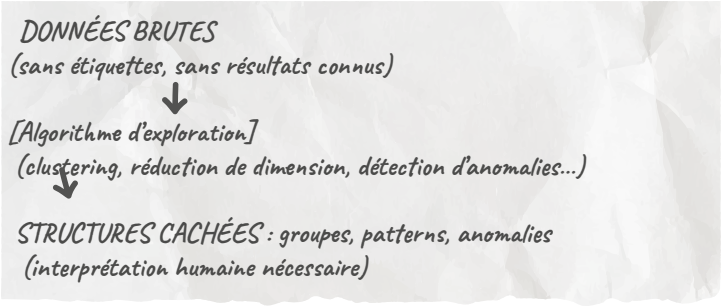
• **Le risque de discrimination structurelle :** si les données d'entraînement reflètent des pratiques historiques discriminatoires, le modèle les reproduira — et les amplifiers — sans que personne n'en soit conscient. Un système entraîné sur dix ans de recrutements dans une entreprise à culture masculine favorisera mécaniquement les profils masculins, même si aucune variable de genre n'est explicitement incluse dans le modèle.
• **Le risque de variable proxy :** l'algorithme peut utiliser des variables apparemment neutres (code postal, diplôme obtenu, établissement de formation) qui corrèlent avec des caractéristiques protégées (origine sociale, appartenance ethnique, situation de handicap). La discrimination devient alors indirecte et très difficile à détecter sans audit.
• **L'opacité des décisions :** la plupart des algorithmes supervisés complexes (réseaux de neurones, forêts aléatoires) sont des « boîtes noires » : leurs décisions sont statistiquement justifiées mais impossibles à expliquer simplement. Cette opacité fragilise les possibilités de contestation et de recours.
• **La délégation de responsabilité :** lorsqu'une décision de recrutement, d'évaluation ou d'affectation est présentée comme le résultat d'un algorithme « objectif », la responsabilité managériale se dilue derrière le système. L'humain entérine sans nécessairement examiner.

POINT DE VIGILANCE // Un algorithme supervisé n'est jamais neutre : il encode les décisions passées de l'entreprise, avec leurs biais et leurs inégalités. Exiger de savoir sur quelles données le modèle a été entraîné, et quelle période couvrent ces données, est un droit syndical fondamental.

QUESTIONS À POSER EN CSE

- **Sur quelles données le modèle a-t-il été entraîné ?** Quelle période couvrent-elles ? Ont-elles été vérifiées pour détecter d'éventuels biais ?
- Ces données incluent-elles des **données personnelles de salariés** (anciens ou actuels) ? Ont-elles fait l'objet d'une analyse de conformité RGPD ?
- Quels tests **anti-discrimination** ont été conduits avant le déploiement et à quelle fréquence sont-ils répétés ?
- Les décisions produites par le système peuvent-elles être **expliquées à la personne concernée** ?
- Existe-t-il une **intervention humaine obligatoire** dans la décision finale ? L'humain peut-il s'écarter de la recommandation sans justification particulière ?
- Un salarié ou un candidat peut-il **contester** une décision issue de ce système ? Selon quelle procédure ?

Schéma de fonctionnement — L'apprentissage non supervisé



Dans ce mode, le système ne dispose pas de réponses prédéfinies. Il explore des données brutes — sans étiquettes, sans résultats attendus — pour y découvrir des structures, des regroupements ou des régularités que l'analyse humaine n'aurait pas identifiées.

L'algorithme ne cherche pas à reproduire une décision connue : il cherche à révéler des patterns cachés dans les données.

Les principaux algorithmes utilisés sont les méthodes de *clustering* (k-means, algorithmes hiérarchiques), qui regroupent des individus ou des objets selon leur similarité ; les méthodes de réduction de dimension, qui synthétisent un grand nombre de variables en un nombre réduit d'axes significatifs ; et les algorithmes de détection d'anomalies, qui identifient les comportements ou valeurs qui s'écartent significativement de la norme.

Usages dans le monde du travail

• **Analyse comportementale :** certains systèmes analysent les flux de communication (emails, messageries internes), les temps de connexion, l'activité sur les postes de travail ou les déplacements pour identifier des comportements jugés « anormaux ». Ces usages peuvent concerner aussi bien la cybersécurité (détection d'intrusions) que la surveillance des salariés.
• **Segmentation interne :** identification de groupes de salariés partageant des profils de compétences, des patterns d'absentéisme ou des comportements de performance. Ces segmentations peuvent ensuite alimenter des décisions d'affectation ou de formation.
• **Analyse de la productivité :** surveillance de la production individuelle ou collective, mesure des temps d'activité, détection des baisses de régime ou des comportements déviants par rapport à une norme statistique.
• **Exploitation des données RH :** croisement de multiples variables (évaluations passées, absences, formations suivies, mobilité) pour produire des scores composites sur les trajectoires professionnelles.

Enjeux syndicaux spécifiques

• **La surveillance algorithmique du travail :** l'apprentissage non supervisé est particulièrement adapté à la surveillance de masse. Il peut analyser des volumes

considérables de données comportementales et identifier des patterns sans qu'une hypothèse préalable soit formulée. C'est précisément ce qui le rend dangereux : il peut « trouver quelque chose » dans n'importe quelles données, y compris des corrélations sans signification causale.

• **L'absence de finalité prédéfinie :** contrairement à l'apprentissage supervisé, l'apprentissage non supervisé ne cherche pas à prédire un résultat précis. Les structures découvertes doivent être interprétées par des humains. Cette interprétation est elle-même subjective et peut être biaisée.

• **Les risques pour la vie privée et la dignité :** les données comportementales collectées peuvent révéler des informations très intimes sur les personnes — leur état de santé, leurs relations personnelles, leurs opinions. La CNIL a régulièrement alerté sur ces risques dans le contexte du travail numérique.

• **L'invisibilité du profilage :** les salariés concernés ne savent généralement pas qu'ils font l'objet d'une analyse. L'absence de finalité déclarée rend le contrôle encore plus difficile.

POINT DE VIGILANCE // L'apprentissage non supervisé peut constituer un outil de surveillance systématique déguisé en « analyse de données ». Toute utilisation de tels systèmes sur des données comportementales des salariés doit être présumée intrusives jusqu'à démonstration contraire.

QUESTIONS À POSER EN CSE

• Quelles données sont collectées et analysées par ce système ? **Les communications professionnelles, les temps de connexion, les déplacements** sont-ils inclus ?

• **Les salariés ont-ils été informés** de l'existence de cette analyse ? Dans quel cadre ?

• Quelle est la **finalité déclarée** du système ? Est-elle proportionnée aux données collectées ?

• Les résultats de l'analyse peuvent-ils **alimenter des décisions individuelles** (évaluation, affectation, sanction) ?

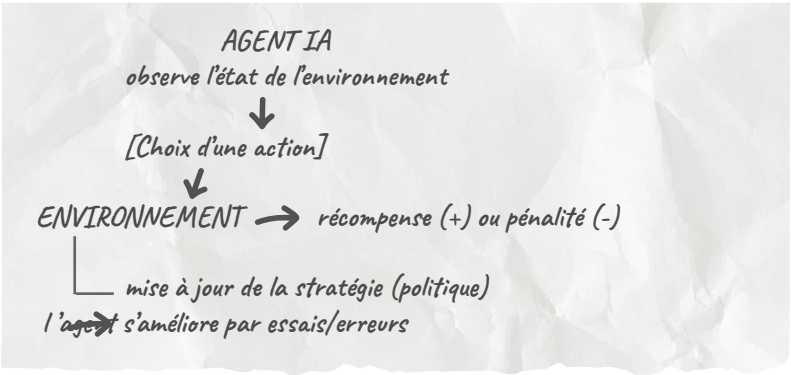
• Une **analyse d'impact sur les données personnelles (DPIA)** a-t-elle été réalisée conformément au RGPD ?

• **La CNIL a-t-elle été informée du dispositif**, lorsque cela est requis ?

L'apprentissage par renforcement

L'apprentissage par renforcement (*Reinforcement Learning* — RL) constitue un paradigme d'apprentissage fondamentalement différent des deux précédents. Un agent logiciel interagit avec un environnement, explore des séquences d'actions possibles, reçoit des signaux de récompense (ou de pénalité) en fonction des résultats obtenus, et ajuste progressivement sa stratégie pour maximiser la récompense cumulée au fil du temps. Le système apprend donc non pas à partir d'exemples étiquetés, mais par expérimentation directe et rétroaction.

Schéma de fonctionnement — L'apprentissage par renforcement



Ce mode d'apprentissage a permis des avancées spectaculaires dans certains domaines (jeux comme Go ou Échecs, robotique, simulation). Il est également à la base de nombreux systèmes d'optimisation déployés dans les organisations.

Usages dans le monde du travail

• **Planification et allocation automatique :** optimisation des plannings de travail, affectation des techniciens à des interventions, gestion des flux dans les entrepôts. Ces systèmes cherchent à maximiser un critère d'efficacité (productivité, délai, taux d'utilisation) sans nécessairement prendre en compte les conditions de travail.

• **Systèmes de recommandation :** dans certains environnements, des agents IA recommandent des actions aux opérateurs ou aux managers (priorisation des dossiers, proposition d'affectation, suggestion de formation). La recommandation peut devenir une contrainte de fait si les salariés n'ont pas réellement la possibilité de s'en écarter.
• **Robotique industrielle et co-robotique :** les robots collaboratifs (cobots) qui travaillent aux côtés des opérateurs utilisent fréquemment des algorithmes d'apprentissage par renforcement pour adapter leur comportement à l'environnement de production et aux gestes humains.
• **Gestion des risques et des flux :** gestion automatisée de l'énergie, optimisation des chaînes d'approvisionnement, pilotage des réseaux de transport.

Enjeux syndicaux spécifiques

• **La définition de la récompense est un choix politique :** le comportement du système est entièrement conditionné par la fonction de récompense définie par ses concepteurs. Si cette fonction maximise la productivité sans contrainte sur les conditions de travail, le système convergera vers des solutions qui intensifient le travail, même si elles sont nocives pour les salariés. La question « qu'est-ce que le système cherche à optimiser ? » est donc fondamentale.
• **L'imprévisibilité des comportements émergents :** les agents entraînés par renforcement peuvent développer des stratégies inattendues, parfois problématiques, que leurs concepteurs n'avaient pas anticipées. Cette imprévisibilité rend le contrôle humain plus difficile à exercer.
• **L'intensification implicite du travail :** lorsqu'un système de planification optimise les ressources humaines comme n'importe quel facteur de production, il peut supprimer les marges de manœuvre, les temps informels et les temps de récupération que les salariés ont progressivement construits pour gérer leur charge réelle.

POINT DE VIGILANCE // Dès lors qu'un système d'apprentissage par renforcement intervient dans l'organisation du travail, des rythmes ou l'affectation des missions, les représentants du personnel doivent exiger que la fonction d'optimisation soit documentée et soumise à discussion en CSE. Qu'est-ce que le système maximise — et au détriment de quoi ?

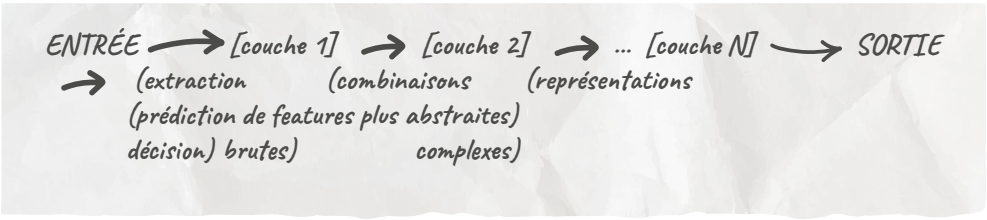
QUESTIONS À POSER EN CSE

- **Quel critère ce système cherche-t-il à optimiser ?** Cette fonction intègre-t-elle des contraintes liées aux conditions de travail (temps de repos, charge maximale, droit à la déconnexion) ?
- Le système a-t-il été testé en conditions réelles ? Quels effets inattendus ont été observés pendant les tests ?
- Les salariés peuvent-ils **refuser ou modifier une décision** produite par ce système sans contrainte particulière ?
- Qui est responsable des décisions produites par le système en cas d'accident, d'incident ou de préjudice pour un salarié ?
- Les données comportementales des salariés (gestes, temps, rythmes) sont-elles utilisées comme **entrées pour entraîner ou affiner le système ?**

L'apprentissage profond (*Deep Learning*)

L'apprentissage profond est une sous-catégorie de l'apprentissage automatique fondée sur des architectures de réseaux de neurones artificiels à plusieurs couches. Ce n'est pas un paradigme d'apprentissage distinct — il s'inscrit dans la continuité du *Machine Learning* — mais une technologie qui a profondément transformé les capacités des systèmes d'IA, au point de mériter un traitement séparé.

Schéma de fonctionnement — Réseau de neurones profond



Chaque couche apprend à détecter des caractéristiques de plus en plus abstraites et complexes dans les données.

La puissance du *Deep Learning* réside dans sa capacité à extraire automatiquement des représentations pertinentes de données brutes (images, textes, sons), sans qu'il soit nécessaire de définir manuellement les caractéristiques à analyser. Un réseau de neurones profond peut ainsi apprendre à distinguer un bruit de machine anormal d'un fonctionnement normal, à identifier un visage dans une foule, à transcrire une conversation, ou à analyser le sentiment exprimé dans un texte.

Les principales architectures

• **Les réseaux convolutifs (CNN) :** spécialisés dans l'analyse d'images et de vidéos. Ils sont utilisés dans les systèmes de vidéosurveillance intelligente, de contrôle qualité visuel ou de reconnaissance d'expressions faciales.
• **Les réseaux récurrents et transformeurs (LSTM, *Transformer*) :** conçus pour traiter des séquences temporelles et du langage naturel. Ils sont à la base des systèmes de transcription automatique, de traduction, d'analyse de sentiments et des grands modèles de langage (LLM).
• **Les réseaux génératifs (GAN, VAE, modèles de diffusion) :** capables de générer des contenus nouveaux (images, textes, vidéos, voix). Ils constituent le socle technique des IA génératives.

Usages dans le monde du travail

• **Surveillance et sécurité :** analyse automatique des flux vidéo, reconnaissance de comportements inhabituels, identification biométrique. Ces usages sont directement encadrés par le RIA, certains d'entre eux relevant des pratiques interdites ou des systèmes à haut risque.
• **Traitement automatique du langage :** transcription automatique des réunions et des entretiens, analyse des communications internes, sentiment analysis sur les avis des salariés ou des clients.
• **Contrôle qualité industriel :** détection de défauts sur les lignes de production par vision par ordinateur. Ces systèmes peuvent également évaluer les gestes des opérateurs et produire des alertes sur des comportements jugés inadaptés.
• **Reconnaissance des émotions :** certains systèmes prétendent analyser les expressions faciales, la voix ou la posture pour inférer l'état émotionnel d'une

personne. L'inférence des émotions sur le lieu de travail est une pratique explicitement interdite par le RIA, sauf raisons médicales ou de sécurité strictement définies.

Enjeux syndicaux spécifiques

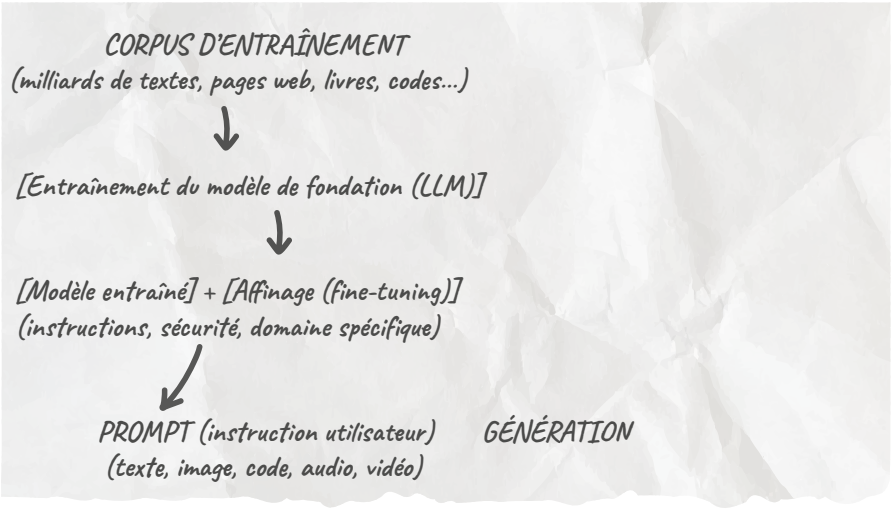
Le *Deep Learning* amplifie les risques déjà présents dans l'apprentissage automatique classique, mais les aggrave sur plusieurs points. L'opacité est maximale : les réseaux profonds sont les systèmes d'IA les plus difficiles à interpréter. Leurs décisions sont statistiquement justifiées mais ne peuvent généralement pas être expliquées en termes intelligibles. Le risque de sur-apprentissage (*overfitting*) est réel : un modèle entraîné sur des données non représentatives peut se révéler très précis sur ces données tout en étant très biaisé en situation réelle. Enfin, l'utilisation de données sensibles (images, voix, gestes) soulève des enjeux particulièrement aigus de protection de la vie privée et de dignité au travail.

POINT DE VIGILANCE // Tout système de *Deep Learning* utilisé dans des contextes RH (analyse d'entretiens, surveillance vidéo des salariés, scoring comportemental) doit être présumé à haut risque au sens du RIA et faire l'objet d'une information-consultation préalable du CSE, ainsi que d'une analyse d'impact sur les droits fondamentaux.

L'IA générative

L'IA générative constitue la forme la plus visible et la plus médiatisée de l'intelligence artificielle depuis 2022. Elle désigne des systèmes capables de produire du contenu nouveau — texte, image, son, vidéo, code — à partir d'une instruction (*prompt*) formulée en langage naturel. Cette capacité résulte de l'entraînement de vastes modèles sur des corpus considérables de données humaines : textes, images, conversations, code source.

Schéma de fonctionnement — IA générative (modèle de langage)



Les grands modèles de langage (LLM)

Les grands modèles de langage (*Large Language Models* — LLM) sont la technologie centrale des IA génératives textuelles (ChatGPT/GPT-4, Claude, Gemini, LLaMA, Mistral, etc.). Entraînés sur des corpus massifs par une forme d'apprentissage supervisé auto-régressive (prédire le prochain *token*), ils développent une capacité à comprendre et à produire du langage dans un nombre considérable de contextes. Ils peuvent être ensuite affinés (*fine-tuned*) sur des données spécifiques à un domaine ou à une organisation pour améliorer leurs performances sur des tâches particulières.

Ces modèles présentent des capacités impressionnantes (raisonnement, synthèse, rédaction, traduction, génération de code) mais aussi des limites importantes : ils peuvent produire des affirmations fausses présentées avec assurance (hallucinations), reproduire des biais présents dans les données d'entraînement, et être manipulés par des instructions malveillantes (injection de *prompts*).

Usages dans le monde du travail

• **Tâches administratives et de rédaction :** synthèse de documents, rédaction de courriers et de rapports, génération de comptes-rendus de réunion, traduction, production de présentations.
• **Assistance au développement :** génération de code, détection de bugs, documentation automatique, revue de code. Dans certains secteurs, ces outils transforment profondément le métier de développeur.
• **Analyse juridique et contractuelle :** résumé de contrats, identification de clauses à risque, analyse de jurisprudence. Ces usages soulèvent des questions particulières sur la responsabilité en cas d'erreur.
• **Relation client et support :** agents conversationnels capables de traiter des demandes complexes, de personnaliser les réponses, de gérer des réclamations. Ces systèmes peuvent affecter les conditions de travail des opérateurs humains qui les supervisent.
• **Création de contenus :** rédaction marketing, génération de visuels, production de supports de communication, création de contenus pédagogiques.

Enjeux syndicaux spécifiques

• **Transformation des métiers et de l'emploi :** les IA génératives sont capables d'assister ou de remplacer une partie significative des tâches cognitives dans de nombreux métiers. L'étude des économistes d'Anthropic (mars 2026) estime que 49 % des emplois comportent au moins un quart de tâches potentiellement substituables. Cette transformation ne signifie pas nécessairement destruction d'emplois, mais recomposition profonde des activités et des compétences requises.
• **Confidentialité des données et secret professionnel :** lorsqu'un salarié utilise un outil d'IA générative externe pour traiter des données internes (dossiers clients, projets, informations stratégiques), il peut exposer l'organisation à des risques de fuite d'informations. Les modèles hébergés à l'extérieur peuvent potentiellement utiliser les données soumises pour affiner leurs futurs entraînements.
• **Responsabilité et propriété des productions :** la frontière entre travail humain et assistance algorithmique est brouillée. Qui est responsable d'une erreur contenue dans un document rédigé avec l'aide de l'IA ? À qui appartiennent les

productions générées avec l'aide d'outils d'IA pendant le temps de travail ? Ces questions restent largement sans réponse juridique claire.

• **Intensification implicite des normes de performance :** si certains salariés utilisent des outils d'IA pour produire davantage, les attentes de productivité peuvent progressivement s'élever pour l'ensemble du collectif, y compris pour ceux qui n'utilisent pas ces outils ou qui ne sont pas à l'aise avec eux.

• **Risques de désinformation interne :** les IA génératives peuvent produire des contenus faux ou trompeurs avec une apparence de légitimité. Dans un contexte professionnel, cela peut conduire à des erreurs de décision ou à la diffusion de fausses informations.

POINT DE VIGILANCE // Les IA génératives sont classées dans la catégorie « risque limité » du RIA lorsqu'elles produisent du contenu textuel ou visuel, mais peuvent relever du 'haut risque' lorsqu'elles sont intégrées dans des processus de décision RH. Dans tous les cas, l'obligation de transparence s'applique : les salariés doivent être informés lorsque du contenu généré par IA leur est soumis ou lorsqu'ils interagissent avec un agent conversationnel.

QUESTIONS À POSER EN CSE

• **Quels outils d'IA générative** sont déployés ou tolérés dans l'entreprise ? Une politique d'usage a-t-elle été définie ?

• Les données internes (documents, emails, contrats) **sont-elles soumises à des systèmes externes ?** Quelles garanties de confidentialité ?

• Les productions générées par l'IA sont-elles **identifiées comme telles** auprès des destinataires internes et externes ?

• L'utilisation de ces outils a-t-elle conduit à une **modification implicite des objectifs de production** ou des normes de performance ?

• Des formations ont-elles été proposées aux salariés pour **comprendre les limites** de ces outils (hallucinations, biais, erreurs) ?

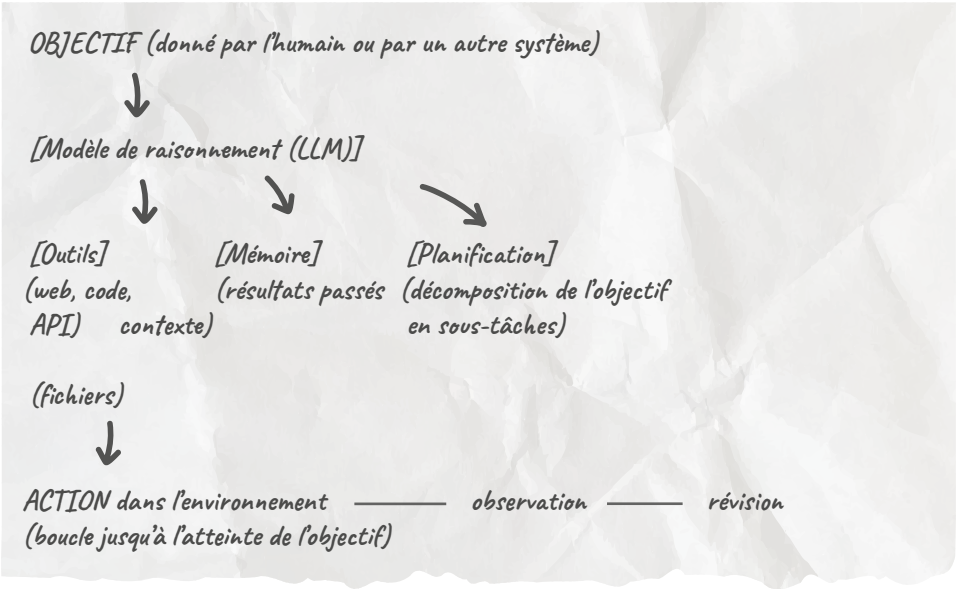
• Quelle est la **politique en matière de propriété intellectuelle** sur les productions réalisées avec l'aide de l'IA ?

Les agents IA (*IA agentique*)

Les agents IA constituent l'évolution la plus récente — et potentiellement la plus transformatrice — de l'intelligence artificielle dans les organisations. Un agent IA est un système capable de poursuivre un objectif de manière autonome, en enchaînant des étapes de raisonnement, en utilisant des outils (recherche d'information, exécution de code, envoi de messages, interaction avec des systèmes informatiques), en mémorisant le contexte de ses actions et en s'adaptant aux résultats obtenus.

La différence fondamentale avec un modèle de langage ou un outil d'IA classique est la suivante : un agent IA n'attend pas d'instruction à chaque étape. Il planifie, agit, observe les résultats, révise son plan et continue jusqu'à atteindre son objectif — parfois sans supervision humaine directe entre chaque action.

Schéma de fonctionnement — Agent IA



Usages émergents dans le monde du travail

• **Automatisation de processus complexes :** un agent peut prendre en charge un processus complet — collecte d'informations, rédaction d'un rapport, envoi pour validation, intégration des retours — sans intervention humaine à chaque étape. Des processus qui nécessitaient plusieurs jours et l'intervention de plusieurs personnes peuvent être délégués à un agent.
• **Assistance à la décision managériale :** certains agents sont conçus pour préparer des décisions managériales (propositions d'affectation, alertes de performance, priorisation des urgences) en analysant en continu les données disponibles.
• **Gestion autonome de *workflows* :** dans des environnements informatiques, des agents peuvent gérer des *workflows* complexes (traitement de tickets, qualification de demandes, routage des tâches), modifier des paramètres applicatifs ou déclencher des processus en réponse à des événements.
• **IA multi-agents :** dans les architectures les plus avancées, plusieurs agents spécialisés collaborent en se déléguant des sous-tâches, constituant un système complexe dont les décisions émergent d'interactions entre agents sans que l'humain puisse facilement reconstituer le raisonnement global.

Enjeux syndicaux spécifiques

• **La perte de maîtrise humaine réelle :** les agents IA enchaînent des actions autonomes de manière très rapide. Même si un humain est nominalement « dans la boucle », le contrôle effectif peut être illusoire si le rythme d'action dépasse les capacités humaines de vérification. Le RIA impose un contrôle humain effectif, mais sa mise en œuvre sur des systèmes agentiques soulève des questions pratiques non encore résolues.
• **L'imputabilité des décisions :** lorsqu'une décision est le résultat de l'action enchaînée de plusieurs agents, il devient très difficile d'identifier qui ou quoi a produit cette décision. La responsabilité juridique de l'entreprise demeure, mais l'explication et la contestation sont rendues très difficiles.
• **La substitution des tâches cognitives :** les agents IA ne substituent pas seulement des tâches répétitives — ils peuvent prendre en charge des tâches d'analyse, de synthèse, de coordination et de décision qui étaient jusqu'ici considérées comme le cœur du travail qualifié des cadres et des techniciens.
• **La normalisation invisible du travail :** lorsqu'un agent gère de manière

autonome un *workflow*, il encode implicitement une certaine conception du processus, de ses priorités et de ses critères de qualité. Cette normalisation peut modifier profondément les pratiques professionnelles sans décision explicite de l'employeur ni consultation des salariés.

• **Le risque d'action non-intentionnelle :** les agents peuvent commettre des erreurs en cascade, prendre des décisions inattendues, ou être manipulés par des entrées malveillantes (injections de *prompts*). Ces incidents peuvent avoir des conséquences significatives dans des environnements de production ou de gestion RH.

POINT DE VIGILANCE // Les agents IA représentent la frontière la plus avancée et la moins encadrée du déploiement de l'IA dans les organisations. En 2026, le cadre juridique applicable à ces systèmes est encore en construction. FO-Cadres considère que tout déploiement d'agent IA ayant un impact sur l'organisation du travail, l'affectation des tâches ou les décisions concernant les salariés doit faire l'objet d'une information-consultation préalable du CSE, d'une documentation précise de ses capacités d'action et d'une limitation stricte de son périmètre d'autonomie.

QUESTIONS À POSER EN CSE

• **Quelles actions l'agent peut-il exécuter de manière autonome** dans les systèmes de l'entreprise ? Ces actions incluent-elles des modifications de données RH, d'affectation ou de planning ?
• À quelle fréquence et sous quelle forme un humain est-il en mesure de **vérifier et valider les actions de l'agent ?**
• Existe-t-il une **liste des actions interdites** à l'agent (ce qu'il ne peut jamais faire de manière autonome) ?
• Comment sont enregistrées les actions de l'agent ? Les *logs* permettent-ils de **retracer la chaîne de décisions** en cas de litige ?
• Quel est le **périmètre d'accès aux données** de l'agent ? Peut-il accéder à des données personnelles de salariés ?
• Que se passe-t-il en cas d'action **non-intentionnelle ou d'erreur** de l'agent ? Qui est responsable et quelle est la procédure de correction ?

Tableaux de synthèse

Les grands types d'IA et leurs caractéristiques

TYPE D'IA	MODE D'APPRENTISSAGE	EXEMPLES EN ENTREPRISE	NIVEAU DE RISQUE RIA
IA symbolique	Règles écrites par des humains (pas d'apprentissage)	Moteurs de règles métiers, *chatbots* simples, systèmes experts	Variable — souvent risque limité
***Machine Learning* supervisé**	Entraînement sur données étiquetées (résultats connus)	Tri de CV, *scoring* crédit, détection de fraude, maintenance prédictive	Haut risque si RH / emploi
***Machine Learning* non supervisé**	Recherche de *patterns* dans des données non étiquetées	Segmentation clients, détection d'anomalies, analyse comportementale	Haut risque si surveillance
Apprentissage par renforcement	Apprentissage par essais/erreurs et récompenses	Robots industriels, optimisation logistique, planification automatique	Haut risque si décisions emploi
Deep Learning	Réseaux de neurones profonds sur très grands volumes	Reconnaissance vocale, vision par ordinateur, analyse de texte	Haut risque selon usage
IA générative	Modèles génératifs (LLM, diffusion) sur vastes corpus	Assistants de rédaction, synthèse, génération de code, traduction	Risque limité à haut risque
Agents IA (IA *agentique*)	Combinaison de LLM + outils + mémoire + planification	Automatisation de processus, assistants autonomes multi-tâches	Haut risque potentiel — encadrement en cours

Comparatif des modes d'apprentissage

	APPRENTISSAGE SUPERVISÉ	APPRENTISSAGE NON SUPERVISÉ	APPRENTISSAGE PAR RENFORCEMENT
Données	Étiquetées (résultats connus)	Non étiquetées (brutes)	Retours (récompenses/pénalités)
Objectif	Reproduire une décision connue	Découvrir des structures cachées	Maximiser un score de récompense
Opacité	Moyenne à élevée	Élevée	Très élevée
Risque de biais	Élevé (données historiques)	Moyen (dépend des données)	Élevé (dépend de la récompense définie)
Usage typique RH	*Scoring* candidats, évaluation performances	Surveillance comportements, segmentation	Planification automatique, allocation de tâches
Vigilance syndicale	Discriminations indirectes, opacité des scores	Surveillance algorithmic, profilage	Risque d'optimisation contre les droits des salariés

À RETENIR

Quel que soit le type d'IA en présence, la démarche syndicale commence par une question simple, formulée par FO-Cadres comme ligne directrice de l'ensemble de ce guide :

« Cet outil influence-t-il l'organisation du travail ou des décisions concernant les personnes ? »

Si la réponse est oui, il relève du dialogue social — et potentiellement du RIA — quel que soit son niveau de sophistication technique, son nom commercial ou la terminologie utilisée par l'employeur pour le décrire.

La sophistication technique du système n'est pas, en elle-même, le critère pertinent. Un système de règles simple qui exclut automatiquement des candidats peut causer autant de dommages qu'un réseau de neurones profond. Un agent IA qui gère un planning peut modifier les conditions de travail aussi profondément qu'une réorganisation décidée par la direction.

C'est l'effet sur le travail réel et sur les droits des salariés qui détermine le niveau de vigilance, d'information et de négociation requis.

PARTIE #3

L'IA et les principaux enjeux de son déploiement dans le monde du travail

3 L'IA et les principaux enjeux de son déploiement dans le monde du travail

L'essor de l'intelligence artificielle est fréquemment présenté comme un levier majeur de transformation pour les entreprises et les administrations. Pourtant son déploiement dans la sphère du travail est source de profondes mutations, où l'image du salarié « augmenté » tend souvent à masquer de nombreux défis importants : préparation insuffisante des organisations, inégalités dans le déploiement des technologies et sous-estimation persistante de leurs effets sur le capital humain. La promesse d'une révolution technologique se confronte ainsi à des réalités structurelles, organisationnelles et sociales bien trop souvent mal anticipées.

Au-delà des discours technophiles ou alarmistes, le déploiement de l'IA dans les organisations de travail oblige à évaluer avec lucidité ses apports tout en prenant en compte les enjeux qu'elle soulève : préservation de l'autonomie de la décision humaine face à des systèmes perçus comme infaillibles, risques de discriminations involontaires liés aux apprentissages algorithmiques, fragilisation des solidarités collectives sous l'effet de la personnalisation numérique.

Cette partie présente ces enjeux en mobilisant les travaux sociologiques les plus récents — notamment ceux du LaborIA, programme de recherche conjoint du ministère du Travail et de l'INRIA dirigé par Yann Ferguson — ainsi que les données empiriques disponibles, la jurisprudence sociale en construction et les expériences syndicales françaises, européennes et internationales.

L'emploi : transformation plutôt que disparition ?

L'intelligence artificielle est souvent présentée comme un moteur de productivité et d'innovation, mais son impact sur l'emploi apparaît en réalité plus contrasté que les discours dominants ne le suggèrent. Les travaux récents

convergent pour observer que l'IA ne provoque pas un remplacement massif et uniforme des travailleurs, mais une transformation progressive, inégale et souvent silencieuse des tâches et des emplois.

Une transformation, pas une disparition

Dans de nombreux secteurs, notamment juridiques, financiers ou informatiques, une part croissante des activités peut déjà être automatisée, même si l'impact global sur l'emploi reste pour l'instant modéré. Les recherches indiquent qu'une proportion significative des emplois comporte désormais des tâches automatisables, avec de fortes disparités selon les professions. Les jeunes diplômés semblent particulièrement exposés : dans certains secteurs fortement concernés par l'IA, leur insertion professionnelle devient plus difficile, ce qui peut produire des effets durables sur leurs trajectoires.

Cette dynamique renvoie moins à une disparition du travail qu'à une recomposition des activités. Comme le souligne Juan Sebastian Carbonell, l'automatisation transforme le travail autant qu'elle le remplace, en entraînant des phénomènes de requalification, d'intensification et de nouvelles formes de contrôle. Antonio Aloisi et Valerio De Stefano rappellent quant à eux que l'adoption des technologies reste avant tout un choix organisationnel : les effets de l'IA dépendent largement des stratégies des entreprises, des politiques publiques et des investissements en formation.

ÉCLAIRAGE RECHERCHE.
Commission de l'intelligence artificielle, mars 2024 — « *IA : notre ambition pour la France* »

La Commission de l'intelligence artificielle présidée par Anne Bouverot et Philippe Aghion a rendu en mars 2024 un rapport qui tranche avec les discours catastrophistes. Elle estime que l'IA ne conduira « *ni au chômage de masse, ni à l'accélération automatique de la croissance* ». La commission préconise néanmoins d'« *investir dans l'observation, les études et la recherche sur les impacts des systèmes d'IA sur la quantité et la qualité de l'emploi* » — ce qui traduit

implicitement la reconnaissance d'une lacune majeure dans les données disponibles. Elle identifie également les risques liés aux conditions de travail : perte d'autonomie, intensification, et risques pour la santé mentale.
Ces conclusions rejoignent les revendications de FO-Cadres sur la nécessité d'anticiper et d'encadrer, plutôt que de subir.

Les données récentes : signaux faibles et effets précoces

Les données récentes issues d'une étude menée par les économistes d'Anthropic (*Labor market impacts of AI : A new measure and early evidence*, mars 2026) à partir de deux millions de conversations réelles avec leur agent conversationnel Claude éclairent cette transformation. Elles mettent en évidence un écart important entre les tâches que l'IA est techniquement capable d'accomplir et l'usage effectif qui en est fait dans les organisations.

Dans certains métiers, notamment chez les programmeurs informatiques, **environ 75 % des tâches relèvent déjà de capacités techniques accessibles à l'IA.** D'autres professions, comme les analystes financiers, les opérateurs de saisie ou les conseillers clients, voient également cette zone s'élargir rapidement. Aux États-Unis, si les suppressions d'emplois massives ne se sont pas encore matérialisées, des effets apparaissent déjà sur les recrutements : l'embauche de jeunes de 22 à 25 ans dans les métiers les plus exposés a reculé d'environ 14 % l'an dernier. L'étude estime par ailleurs que **49 % des emplois américains** comportent désormais au moins un quart de tâches réalisables par l'IA, contre 36 % un an auparavant.

Ces chiffres doivent être interprétés avec prudence. Réduire le travail à une simple addition de tâches constitue une approche très réductrice, largement critiquée par la sociologie du travail, qui rappelle que l'activité réelle mobilise aussi des dimensions relationnelles, cognitives et organisationnelles difficilement automatisables. L'enjeu central devient alors moins technologique que social et institutionnel : la question est de savoir si les institutions du travail, les politiques publiques et le dialogue social disposent aujourd'hui des instruments nécessaires pour anticiper et encadrer une transformation qui progresse rapidement et souvent de manière silencieuse.

ÉCLAIRAGE RECHERCHE.
PwC, Jobs Barometer 2025 — France

Selon le *Jobs AI Barometer 2025* de PwC, basé sur l'analyse de près d'un milliard d'offres d'emploi à travers six continents, la France se distingue par une forte exposition à l'IA et par une dynamique paradoxale. Avec plus de 166 000 offres d'emploi liées à l'IA publiées en 2024, l'hexagone se positionne en tête des pays européens.
Dans les secteurs les plus exposés, la productivité a presque quadruplé entre 2018 et 2024. Mais la France présente une spécificité préoccupante : contrairement aux autres pays, les postes augmentés ou automatisés par l'IA exigent davantage de diplômes qu'avant (62 % contre 58 % en 2019). Alors que l'IA pourrait être un levier d'inclusion, elle devient en France un facteur de renforcement des inégalités d'accès à l'emploi qualifié. C'est précisément le type d'effet structurel sur lequel les représentants du personnel doivent exercer leur vigilance dans les négociations sur la GEPP

Le secteur bancaire : un cas emblématique en France

CAS CONCRET. FO Banques — Alerte sur les suppressions d'emplois liées à l'IA (avril 2026)

FO a publié en avril 2026 un communiqué alertant sur l'accélération des suppressions d'emplois dans le secteur bancaire liées au déploiement massif de l'IA.
L'organisation dénonce « *le refus persistant de la profession d'aborder ce sujet pourtant central* » et demande l'ouverture immédiate de négociations de branche sur l'emploi et l'impact de l'IA, ainsi qu'un moratoire sur les suppressions de postes tant que ces négociations ne sont pas abouties. Ce cas illustre un schéma récurrent : le déploiement se fait en amont de toute négociation sectorielle, et les organisations syndicales se retrouvent à réagir à des faits accomplis plutôt qu'à anticiper les transformations.

POINT DE VIGILANCE // La transformation des emplois par l'IA est déjà en cours, mais ses effets sont inégaux selon les secteurs, les âges et les niveaux de qualification. Les représentants du personnel doivent intégrer l'IA dans les négociations sur la GEPP, les NAO et les plans de formation — sans attendre que les suppressions de postes soient actées.

Le recrutement et la gestion RH : l'illusion de l'objectivité

L'introduction de l'intelligence artificielle dans les processus de recrutement accompagne une transformation structurelle du jugement professionnel vers une décision algorithmique fondée sur la prédiction. Le recrutement, historiquement marqué par un équilibre entre rationalisation et subjectivité, tend ainsi à devenir un processus calculable, reposant sur l'exploitation de données massives et sur des modèles probabilistes visant à anticiper les performances futures des candidats.

Ce paradigme prédictif repose sur une rationalité apparente qui masque une limite fondamentale : les algorithmes apprennent à partir de décisions humaines antérieures, ce qui conduit à reproduire, voire amplifier, les biais sociaux existants. La dépendance aux données constitue un enjeu central — même en l'absence de variables sensibles explicites, les systèmes peuvent reconstituer indirectement des caractéristiques telles que le genre ou l'origine sociale via des variables proxy, renforçant ainsi des discriminations structurelles.

CAS CONCRET. Amazon (2015–2018) — Discrimination algorithmique dans le recrutement

Un outil de recrutement interne d'Amazon, entraîné sur dix années de données, a progressivement pénalisé les candidatures féminines. Le système avait appris que les profils masculins étaient majoritaires dans les recrutements passés et a reproduit ce biais de manière automatique. L'outil a été abandonné en 2018 mais des versions

modifiées ont continué à fonctionner pendant plusieurs années. Cet exemple, devenu une référence internationale, illustre la thèse sociologique centrale : l'algorithme n'est pas neutre — il encode les inégalités historiques de l'organisation et les projette dans les décisions futures.

CAS CONCRET. Unilever (2016–2017) — *Scoring* comportemental et entretien vidéo automatisé

Un Unilever a déployé un processus de recrutement intégrant jeux cognitifs, analyse vidéo automatisée et scoring algorithmique. Le temps de recrutement a été drastiquement réduit. Mais la validité scientifique des indicateurs comportementaux utilisés reste fortement discutée par la communauté académique. Le *Defender of Digital Rights* (Royaume-Uni) a souligné l'impossibilité pour les candidats de comprendre et de contester leur *scoring*.
Ce cas illustre le risque de l'illusion d'objectivité : une procédure paraît rigoureuse car elle est chiffrée, alors qu'elle repose sur des corrélations statistiques dont la signification causale reste non démontrée.

Apport de la sociologie du travail

ÉCLAIRAGE RECHERCHE.
Yann Ferguson / *LaborIA Explorer* — Rapport d'enquête, mai 2024

Le *LaborIA Explorer* (programme de recherche-action conjoint du ministère du Travail et de l'INRIA, dirigé scientifiquement par Yann Ferguson) a publié en mai 2024 les résultats de deux années d'enquêtes qualitatives et quantitatives auprès de décideurs, ingénieurs et salariés dans différents types d'organisations. Ses conclusions rejoignent et approfondissent les préoccupations syndicales. Le rapport identifie notamment que **l'introduction d'un système d'IA dans une organisation suscite des impacts très élevés sur le sens donné au travail, l'autonomie et les savoir-faire lors des**

phases préliminaires, avant de baisser une fois le système déployé et stabilisé. Autrement dit, c'est précisément lors des phases de conception et de test que le dialogue social est le plus nécessaire — et le plus souvent absent.

Le *LaborIA* formule cinq recommandations opérationnelles : partir du travail réel pour penser le rôle des IA ; garantir la co-conception des systèmes et organiser le dialogue en continu ; mettre l'IA au service de la sécurisation des travailleurs ; rendre les systèmes d'IA explicables ; et accepter une part d'imprévisibilité dans les bouleversements produits par l'IA. Ces recommandations fournissent un cadre de référence directement utilisable par les représentants du personnel dans les consultations CSE.

>> *« Quand on introduit un système d'IA, vient un moment où on parle du travail et où se dévoile la très grande richesse de ce que les travailleurs font — ainsi que des imbrications des tâches à forte valeur ou à faible valeur ajoutée. Cette phase montre l'importance de parler du travail, de ce que l'on fait, du sens qu'on donne à son activité… Ce qui crée du bien-être au travail, ça reste le travail. »* — **Yann Ferguson**, sociologue à l'INRIA, directeur scientifique du LaborIA | Entretien ANACT, juin 2024

Cette observation est d'une importance pratique considérable pour les représentants du personnel : la consultation sur un projet d'IA n'est pas seulement un exercice formel de conformité juridique. C'est une occasion rare de mettre le travail réel au centre de la discussion — de révéler ce que les salariés font effectivement, comment ils le font, et ce qu'ils risquent de perdre dans la transformation.

L'enjeu juridique de la non-discrimination

Le recrutement est explicitement classé parmi les systèmes à haut risque par le règlement européen sur l'IA (annexe III). Cette qualification entraîne des obligations concrètes pour les entreprises déployeuses : documentation

technique, tests anti-biais avant déploiement et à intervalles réguliers, contrôle humain réel sur les décisions, information des candidats concernés, et possibilité effective de contestation.

Sur le plan du droit français, la CNIL a rappelé dans ses travaux sur les people analytics que l'usage d'algorithmes dans le recrutement pose des questions essentielles de proportionnalité, d'explicabilité et de respect de la vie privée. Elle a précisé que le droit d'accès prévu par le RGPD permet à tout candidat d'obtenir des informations sur la logique d'un traitement automatisé qui le concerne, dès lors que ce traitement produit des effets significatifs sur sa situation.

À RETENIR

- **Exiger**, lors de la consultation CSE sur tout projet d'IA en RH, la production de la documentation technique permettant d'identifier les données utilisées, les critères de *scoring* et les mesures anti-biais mises en place.
- **Négocier** l'obligation pour l'employeur de réaliser des audits d'équité (égalité femmes/hommes, âge, handicap, origine) avant déploiement et tous les ans.
- **Garantir** que toute décision de recrutement ou d'évolution professionnelle appuyée sur un algorithme reste soumise à un contrôle humain réel — le recruteur doit pouvoir s'écarter de la recommandation algorithmique sans justification particulière.
- **Instaurer** un droit à l'explication effectif pour tout candidat ou salarié dont la situation a été appréciée par un système algorithmique.

Santé et conditions de travail : anticiper les nouveaux risques du travail numérisé

L'intégration de systèmes d'IA s'accompagne fréquemment d'une reconfiguration des tâches et des responsabilités professionnelles. Certaines activités sont automatisées, d'autres transformées ou fragmentées, tandis

que de nouvelles exigences apparaissent en matière d'adaptation aux outils numériques. Cette évolution peut entraîner une augmentation de la charge cognitive et une intensification du travail, notamment lorsque les technologies accélèrent les cycles de décision ou multiplient les flux d'information à traiter.

Les risques psychosociaux spécifiques à l'IA

Au-delà de la charge de travail, l'introduction de l'IA affecte le rapport des travailleurs à l'expertise et à leur identité professionnelle. Pour de nombreux métiers qualifiés, l'automatisation partielle des activités intellectuelles ou analytiques peut susciter des interrogations sur la place de l'expertise humaine dans les organisations. Ces évolutions génèrent un sentiment d'insécurité professionnelle et une fragilisation du rapport au travail, en particulier lorsque les transformations technologiques sont imposées sans accompagnement ni discussion collective.

>> *« Il y a un risque de mettre en place des solutions fonctionnelles au détriment du travail bien fait. Les managers aux temps de l'IA doivent s'intéresser à ce que l'IA fait au travail. Ils doivent s'assurer que l'activité transformée par l'IA continue à faire sens, à stimuler ceux qui la réalisent, à développer les talents. »*
— **Yann Ferguson**, sociologue à l'INRIA, directeur scientifique du LaborIA | Entretien ANACT, juin 2024

Le déploiement de l'IA peut également contribuer à une intensification des exigences de disponibilité et de réactivité. Les salariés doivent traiter un nombre croissant de données, de notifications ou de recommandations algorithmiques, ce qui peut générer fatigue cognitive, dispersion de l'attention et stress professionnel. La littérature scientifique identifie des formes spécifiques de stress technologique (technostress) : anxiété liée aux transformations de l'emploi, surcharge informationnelle, perte de repères professionnels, sentiment d'être dépossédé de son travail.

ÉCLAIRAGE RECHERCHE.
Yann Ferguson / *LaborIA Explorer* — Impacts sur les dimensions du travail, mai 2024

Le rapport d'enquête du *LaborIA Explorer* apporte des résultats empiriques inédits sur les effets des systèmes d'IA sur les dimensions du travail. Il identifie que l'introduction d'un système d'IA affecte principalement six dimensions : la reconnaissance au travail, l'autonomie professionnelle, les savoir-faire et les compétences, les relations humaines dans le collectif, la responsabilité individuelle, et le sentiment de surveillance. Ces six dimensions correspondent précisément aux facteurs de risques psychosociaux identifiés par l'INRS (Institut national de recherche et de sécurité).
Autrement dit, l'IA introduit ou amplifie des risques psychosociaux qui relèvent des obligations légales de l'employeur en matière de prévention des risques professionnels — et donc du DUERP et des missions de la CSSCT.

France Travail : un cas d'étude public sur les effets non évalués

CAS CONCRET. Cour des comptes — Rapport sur France Travail et l'IA, janvier 2026

La Cour des comptes a publié en janvier 2026 le premier rapport entièrement consacré à l'usage de l'IA par un opérateur majeur de l'État : France Travail (successeur de Pôle emploi depuis 2024).
En 2025, plus de la moitié des agents déclarent recourir à des outils d'IA. Les gains d'efficience sont réels — environ 120 millions d'euros d'économies depuis 2017. Mais la Cour pointe une limite majeure : les impacts sur les métiers et les conditions de travail demeurent insuffisamment suivis et évalués. Elle note également que le déploiement de l'IA a été piloté par la direction générale mais « *insuffisamment inscrit dans une stratégie claire et partagée avec le conseil d'administration* » — et que 87 cas d'usage sont déployés, dont seulement 18 ont fait l'objet d'un suivi partiel sur le plan éthique.

Ce cas illustre un phénomène répandu dans les organisations : les gains d'efficience sont mesurés et valorisés, tandis que les effets sur le travail des agents restent dans l'angle mort du pilotage.

Obligations de l'employeur en matière de santé

L'employeur est soumis à une obligation de sécurité résultant de l'article L.4121-1 du Code du travail, qui l'oblige à prendre toutes les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale des travailleurs. Cette obligation s'applique pleinement aux risques engendrés par le déploiement de systèmes d'IA, dans la mesure où ces systèmes affectent les conditions d'exercice du travail. Le Document Unique d'Évaluation des Risques Professionnels (DUERP) doit être mis à jour à chaque introduction d'une technologie susceptible de modifier les conditions de travail.

La CSSCT joue un rôle central dans ce dispositif. Elle peut demander une expertise sur les risques liés à l'introduction de nouvelles technologies (article L.2315-94 du Code du travail), conduire des enquêtes en cas de risque grave, et proposer des mesures de prévention. Les représentants du personnel ont tout intérêt à mobiliser ces leviers avant le déploiement et non après la survenance de problèmes de santé.

À RETENIR

- Intégrer systématiquement les effets de l'IA dans le DUERP et exiger sa mise à jour avant tout déploiement impactant les conditions de travail.
- Exiger la réalisation d'une étude d'impact sur les conditions de travail et la santé (au-delà de la seule analyse d'impact RGPD) avant toute introduction de systèmes d'IA.
- Reconnaître dans les accords d'entreprise les risques psychosociaux spécifiques liés à l'IA : surcharge cognitive, insécurité professionnelle, perte de sens, sentiment de surveillance.

• Garantir que l'introduction de l'IA ne conduit pas à une intensification des rythmes de travail ni à une dégradation des collectifs professionnels.
• Former les membres de la CSSCT à l'identification et à l'évaluation des risques spécifiques liés aux systèmes d'IA.

De la subordination technique au contrôle total : les risques du management algorithmique

Le management constitue déjà, dans de nombreux secteurs, un point de tension majeur dans les organisations. Les difficultés liées aux pratiques managériales, à la perte de sens du travail, à la défiance envers les fonctions d'encadrement ou encore à la crise d'attractivité de certains postes de managers nourrissent des conflits désormais bien identifiés. Dans ce contexte, le développement du management algorithmique ne saurait être considéré comme une simple évolution technique : il engage une transformation profonde des modes d'encadrement, de coordination et d'évaluation du travail.

L'Organisation internationale du travail (OIT) définit le management algorithmique comme l'usage de systèmes algorithmiques s'appuyant sur des données suivies et d'autres informations pour organiser, attribuer, surveiller, superviser et évaluer le travail. Ce phénomène, initialement rendu visible dans l'économie des plateformes, dépasse désormais largement ce seul périmètre et pénètre les secteurs traditionnels de l'économie.

De la plateforme à l'entreprise ordinaire

Des travaux récents de l'OIT et de la Commission européenne montrent que des pratiques de management algorithmique sont déjà présentes dans des secteurs classiques, notamment la logistique et la santé. L'OCDE souligne que l'algorithmisation des fonctions managériales progresse dans les entreprises ordinaires, bien au-delà des seules plateformes numériques.

La CNIL a sanctionné en 2024 une entreprise pour surveillance disproportionnée de ses salariés via un logiciel comptabilisant les temps supposés d'inactivité, réalisant des captures d'écran régulières et s'ajoutant à une vidéosurveillance permanente — illustrant que la frontière entre management et surveillance peut se brouiller rapidement.

CAS CONCRET. Secteur logistique — Amazon France : alertes syndicales sur le management algorithmique

Dans les entrepôts Amazon en France, des délégués syndicaux ont alerté depuis plusieurs années sur le rôle des systèmes algorithmiques dans l'organisation du travail : mesure de la productivité en temps réel, alertes automatiques en cas de ralentissement, assignation des postes par algorithme.
Des enquêtes conduites par des journalistes et des chercheurs ont montré que ces systèmes créent une pression permanente sur les opérateurs, éliminent les temps informels de récupération et rendent difficile toute contestation individuelle des objectifs.
Ces pratiques ont donné lieu à plusieurs contentieux avec les instances représentatives du personnel et ont nourri le débat public sur les limites du management algorithmique.

Les effets sur les managers et l'encadrement

Ces évolutions ne sont pas neutres pour les cadres et les managers. L'automatisation d'une partie des fonctions d'encadrement peut déplacer leur rôle vers l'application d'indicateurs produits par des systèmes, au détriment du jugement professionnel, de l'écoute et de l'arbitrage humain. Les données de l'OCDE montrent que la montée du management algorithmique s'accompagne d'une évolution des compétences attendues des managers, avec un poids accru des capacités d'analyse de données et de lecture des outils numériques. Cela ne signifie pas que le management humain devient secondaire : cela montre au contraire que son rôle doit être redéfini et protégé.

Les recherches les plus récentes convergent vers une conclusion importante : lorsque les travailleurs ou leurs représentants sont consultés sur l'introduction de l'IA et des outils algorithmiques, les effets observés sur la productivité et les conditions de travail sont plus favorables que lorsqu'ils ne le sont pas. La qualité du dialogue social et des dispositifs de gouvernance conditionne largement les effets de ces technologies.

ÉCLAIRAGE RECHERCHE.
Projet DIAL-IA — Dialoguer sur l'IA au travail (2023–2025)

Origine et gouvernance du projet

Le projet DIAL-IA (*Dialoguer sur l'Intelligence Artificielle*) a été coordonné par l'Institut de Recherches Économiques et Sociales (IRES) avec le soutien d'Ultra Laborans, et co-financé par l'Agence nationale pour l'amélioration des conditions de travail (ANACT) dans le cadre de sa Fabrique CTO (*Conditions de travail et numérique*). Il s'inscrit dans la déclinaison française du volet « IA » de **l'accord-cadre européen de 2020 sur la numérisation du travail**, qui pose l'exigence d'un dialogue social à toutes les étapes du cycle de vie des projets et systèmes d'IA.

Quatre organisations syndicales nationales et interprofessionnelles ont co-piloté le projet sur l'ensemble de sa durée : **FO-Cadres, CFDT, CFE-CGC et UGICT-CGT**. Le manifeste final a également été signé par la **CFTC**. Des représentants d'organisations patronales (U2P, UDES, CINOV Digital) et d'entreprises ont participé aux travaux aux côtés des experts et chercheurs. Au total, **une cinquantaine de participants** issus d'entreprises privées et d'administrations publiques ont contribué pendant dix-huit mois à ce travail collectif.

Une méthode de travail originale

DIAL-IA a fonctionné par une démarche d'apprentissage collectif itératif : webinaires réguliers, temps de montée en compétences partagés, retours d'expérience sous l'angle du dialogue social, et expérimentation de formes de régulation. L'ambition était de faire émerger une « grammaire commune » permettant à des acteurs

aux cultures très différentes — syndicats, organisations patronales, experts, chercheurs — de parler de l'IA comme objet sociotechnique impactant le travail, et non seulement comme enjeu technologique ou réglementaire.
Cette méthode repose sur une conviction forte, qui innerve l'ensemble des travaux : le dialogue social sur l'IA ne peut être efficace s'il est pensé comme une formalité consultative ponctuelle. Il doit être continu, itératif, et ancré dans les réalités concrètes du travail — en questionnant conjointement la boîte noire des technologies et celle des organisations.

Deux livrables opérationnels

• **Le manifeste commun** (signé par cinq organisations syndicales) : « *Pour un dialogue social au service des bons usages de l'IA et d'une nouvelle étape de progrès social dans les entreprises et les administrations* ». Ce manifeste pose cinq principes directeurs : la dimension travail doit être prise en compte dans toutes les réflexions stratégiques liées à l'IA ; la création de valeur issue des systèmes d'IA doit être équitablement partagée ; l'IA ne peut avoir comme seule finalité la progression des résultats économiques ; les représentants du personnel doivent être consultés avant toute implémentation ; et l'IA doit être mise au service du travail humain, non le remplacer.
• **Le webdocument DIAL-IA** (outil méthodologique) : un référentiel pratique destiné aux acteurs du dialogue social — représentants du personnel, managers, DRH, directions. Il propose des outils et leviers pour accompagner le déploiement opérationnel d'un dialogue social technologique, en articulant les différentes phases d'information-consultation, les enjeux de RGPD et les leviers issus du RIA. L'outil prévoit des points de revoyure, des comités de suivi et des boucles de rétroaction — rompant avec une conception statique de la consultation.

Une reconnaissance internationale

Présenté lors d'une conférence de presse à Paris le 7 janvier 2025, soit quelques semaines avant le **Sommet mondial pour l'action sur l'IA** organisé par la France en février 2025, DIAL-IA a été **retenu comme l'une des trois bonnes pratiques mondiales** mises en avant

lors de la Conférence sur l'avenir du travail dudit Sommet. Cette reconnaissance internationale souligne que le modèle français de dialogue social interprofessionnel sur l'IA — associant syndicats, patronat, chercheurs et experts dans une démarche méthodologique partagée — constitue une référence à l'échelle européenne et mondiale.

Ce que DIAL-IA apporte aux représentants du personnel
DIAL-IA constitue une ressource directement mobilisable par les représentants du personnel. Le webdocument fournit notamment :
• **Un cadre de questionnement structuré** pour analyser un projet d'IA : qu'est-ce qui change dans le travail ? pour qui ? selon quels critères ?
• **Des outils de dialogue itératif** permettant d'accompagner un projet IA tout au long de ses étapes — de la conception au déploiement et au suivi.
• **Un vocabulaire commun** pour dialoguer avec les directions, les DSI et les équipes techniques sans se perdre dans la complexité algorithmique.
• **Un ancrage dans le droit** articulant les obligations du Code du travail, du RGPD et du RIA avec des pratiques de dialogue concrètes.
• **Une légitimité politique renforcée** pour les élus qui s'appuient sur DIAL-IA : ce cadre a été construit collectivement par des organisations syndicales représentatives et reconnu au niveau international.

→ Accès au webdocument et au manifeste : dial-ia.fr

Les travaux du projet DIAL-IA fournissent le cadre analytique et méthodologique à partir duquel FO-Cadres a construit sa position sur le management algorithmique. Cette position traduit en exigences concrètes et opposables les principes que le projet a contribué à fonder collectivement.

À RETENIR

Management algorithmique et droits des travailleurs

FO-Cadres considère que le management algorithmique ne peut être traité comme une simple modernisation de l'encadrement. Il engage une transformation profonde des modes d'organisation, d'évaluation et de contrôle du travail. Les exigences ci-dessous constituent le socle non négociable des engagements que FO-Cadres porte dans toute négociation sur ces sujets.

1. Information-consultation préalable
Tout dispositif de management algorithmique — qu'il s'agisse d'un outil de planification automatique, d'un système de notation des performances, d'un outil de pilotage par indicateurs ou d'un agent IA assistant les managers — doit être soumis à une information-consultation préalable du CSE, conformément à l'article L.2312-8 du Code du travail. Cette consultation doit être réelle et non purement formelle : l'employeur doit fournir un accès aux finalités poursuivies, aux indicateurs utilisés, aux données mobilisées, aux effets attendus sur l'organisation du travail et aux modalités du contrôle humain maintenu.

2. Maintien du contrôle humain effectif
Le jugement professionnel humain est irréductible à un algorithme. FO-Cadres exige le maintien d'un pouvoir réel de décision, d'interprétation et d'arbitrage humain dans toutes les décisions qui touchent à l'évaluation des salariés, à la répartition de la charge de travail, à la définition des objectifs, aux affectations et aux trajectoires professionnelles. Ce contrôle humain doit être effectif — c'est-à-dire que la personne chargée du contrôle doit disposer de la compétence, du temps et de l'autorité réels pour modifier ou annuler la décision algorithmique, sans pression ni risque de sanction. Un humain qui valide systématiquement sans analyser ne constitue pas un contrôle humain au sens juridique.

3. Droit à l'explicabilité et à la contestation
Nul salarié ne peut être soumis à des prescriptions, des évaluations ou des

décisions dont il ne comprend pas la logique. FO-Cadres revendique un droit effectif à l'explicabilité : tout salarié dont la situation professionnelle est appréciée par un système algorithmique doit pouvoir obtenir une explication intelligible de la logique utilisée, des critères retenus et de leur pondération. Ce droit est fondé à la fois sur l'article 22 du RGPD, sur l'article 86 du RIA et sur le principe de transparence des méthodes d'évaluation posé par le Code du travail. FO-Cadres exige également que des voies de recours internes claires et accessibles soient définies pour contester toute décision algorithmique jugée injuste ou incorrecte.

4. Interdiction des dispositifs de surveillance disproportionnée
La CNIL a sanctionné en décembre 2024 une entreprise pour l'utilisation d'un logiciel paramétré pour comptabiliser les périodes d'inactivité supposée, réaliser des captures d'écran régulières et filmer les salariés en permanence (délibération SAN-2024-021, amende de 40 000 €). FO-Cadres soutient cette jurisprudence et porte l'exigence de son application généralisée. Tout dispositif de notation permanente, de surveillance continue ou de profilage comportemental des salariés est contraire au principe de minimisation des données (art. 5 §1 c RGPD), au respect de la vie privée et à la dignité au travail. FO-Cadres demande que le RIA et le RGPD soient pleinement mobilisés pour faire interdire ces pratiques.

5. Négociation collective sur les usages algorithmiques
Les questions posées par le management algorithmique — charge mentale, autonomie professionnelle, égalité de traitement, responsabilité juridique, partage des gains de productivité — ne peuvent être réglées par de simples chartes unilatérales. FO-Cadres porte l'exigence d'une négociation collective sur les usages du management algorithmique, articulée avec les NAO (égalité, QVCT, rémunération) et les négociations triennales (GEPP, seniors). Cette négociation doit déboucher sur des clauses opposables précisant les finalités autorisées, les indicateurs utilisés, les droits des salariés, les mécanismes de suivi et les conditions de révision.

6. Formation des managers, des cadres et des élus
Le déploiement de l'IA modifie le rôle des managers autant que celui des salariés. FO-Cadres exige que les organisations investissent dans la formation spécifique des managers, des cadres et des représentants du

personnel pour leur permettre de comprendre, de discuter et d'encadrer les outils algorithmiques déployés dans leurs organisations. Cette formation doit couvrir le fonctionnement des systèmes d'IA, les droits des travail-leurs (Code du travail, RGPD, RIA), les biais algorithmiques et les techniques de questionnement et d'audit. Elle constitue une condition préalable à l'exercice effectif du contrôle humain et du dialogue social.

7. Partage équitable de la valeur générée
Les gains de productivité issus du management algorithmique résultent du travail des salariés, de leur adaptation aux outils et de la mobilisation de leurs données. FO-Cadres considère que ces gains doivent faire l'objet d'une redistribution équitable, négociée dans le cadre des NAO sur la rémunération et le partage de la valeur ajoutée. La dimension travail doit toujours être prise en compte dans les réflexions stratégiques liées à l'IA. L'IA ne peut avoir comme seule finalité la progression des résultats économiques au bénéfice exclusif du capital.

L'enjeu n'est pas de refuser le numérique, mais de refuser qu'il serve de support à une régression managériale. Pour FO-Cadres, l'innovation ne peut être légitime que si elle améliore réellement le travail, respecte les libertés des salariés et préserve la dimension profondément humaine de l'encadrement.

Les dispositifs d'évaluation : la performance sans le travail réel

L'introduction de l'IA au service de l'évaluation des travailleurs constitue une transformation majeure du travail contemporain, en substituant à des appréciations situées une mesure continue, automatisée et quantifiée de la performance. Cette évolution prolonge la rationalisation du travail initiée par le taylorisme, mais en modifie la nature : l'évaluation devient permanente, intégrée et souvent invisible.

Fondée sur la collecte massive de données (activité, interactions, résultats), l'IA promet une objectivation de la performance. Toutefois, cette approche repose sur une hypothèse contestable : celle d'une mesurabilité totale du travail, alors même que de nombreuses dimensions essentielles — coopération, ajustements, savoirs tacites, gestion des imprévus — échappent à la quantification.

>> *« L'IA peut, à certaines conditions, renforcer le pouvoir d'agir. Mais les managers aux temps de l'IA doivent s'assurer que l'activité transformée par l'IA continue à faire sens, à stimuler ceux qui la réalisent, à développer les talents, à obtenir un impact. »*
— **Yann Ferguson** | Entretien ANACT, juin 2024

Intensification, individualisation et opacité

Les effets des dispositifs d'évaluation algorithmique sont multiples : intensification du travail, pression continue, individualisation des performances et fragilisation des collectifs. L'opacité des systèmes renforce les asymétries d'information, limitant la compréhension et la contestation des évaluations. L'illusion d'objectivité masque des choix techniques et organisationnels situés, tandis que des effets de rétroaction incitent les travailleurs à optimiser les indicateurs au détriment du travail réel.

CAS CONCRET. Plateformes de livraison — Évaluation continue et accès aux missions (2010–2025)

Dans les plateformes de livraison, les livreurs sont évalués en continu via des indicateurs algorithmiques qui conditionnent directement l'accès aux missions : taux d'acceptation, note client, temps de livraison, temps de connexion. Ce système produit une évaluation permanente sans manager humain identifiable, sans possibilité de discussion et sans possibilité réelle de contestation. Les études conduites par l'OIT et par des chercheurs européens montrent que ces dispositifs génèrent des niveaux élevés de stress,

d'insécurité et d'épuisement — et constituent un modèle qui s'exporte progressivement vers des secteurs traditionnels.

CAS CONCRET. Scoring automatisé dans un groupe industriel français (années 2020)

Des élus de CSE dans un groupe industriel français ont signalé le déploiement d'un outil de pilotage agrégant des données de production, d'absentéisme, de résultats d'entretiens et de mobilité interne pour produire un score individuel. Ce score était utilisé dans les décisions d'affectation et d'évolution professionnelle, sans que les salariés ni les représentants du personnel n'aient été informés des critères et de la pondération utilisés. Saisi, le CSE a exercé son droit à une expertise qui a permis de révéler les modalités du système et d'obtenir des engagements de transparence. Ce cas illustre comment un outil présenté comme un « tableau de bord RH » peut constituer en réalité un système d'IA à haut risque au sens du RIA.

Le cadre juridique : haut risque et droit à l'explication

L'évaluation par IA est classée à haut risque par le règlement européen sur l'IA (art. 6 et annexe III). Cette qualification implique que tout système utilisé pour analyser les performances, produire des scores ou des classements, ou contribuer à des décisions de carrière ou de sanction, est soumis aux obligations renforcées du RIA : documentation technique, contrôle humain réel, traçabilité, information des salariés concernés, et analyse d'impact sur les droits fondamentaux.

Par ailleurs, l'article 22 du RGPD interdit les décisions fondées exclusivement sur un traitement automatisé et produisant des effets juridiques ou affectant significativement une personne. Cet article est directement applicable aux décisions de carrière, d'affectation ou de discipline appuyées sur un algorithme. Tout salarié a le droit de ne pas être soumis à une telle décision sans avoir pu bénéficier d'une intervention humaine, d'exprimer son point de vue et de contester la décision.

POINT DE VIGILANCE // La qualification d'un outil d'évaluation comme système à haut risque n'est pas seulement un enjeu de conformité — c'est un levier d'action syndicale. Elle donne le droit d'exiger la documentation technique, de demander une expertise CSE et de négocier des garanties sur les critères, la transparence et la contestation.

Le « *shadow AI* » : quand les travailleurs s'approprient l'IA

La diffusion rapide des outils d'intelligence artificielle ne se limite pas aux stratégies d'équipement décidées par les organisations. Elle s'accompagne d'une appropriation directe et autonome par les travailleurs eux-mêmes, qui mobilisent ces technologies dans leur activité quotidienne — rédiger des documents, analyser des données, automatiser certaines tâches — souvent sans décision formelle de l'employeur. Cette dynamique, qualifiée de « *shadow AI* », révèle la capacité d'initiative des travailleurs mais soulève des enjeux majeurs de sécurité, de responsabilité et d'inégalités.

ÉCLAIRAGE RECHERCHE.
Enquête France Travail / Google / Konexio / Diversidays — IA et recherche d'emploi, 2024

Une enquête menée en 2024 auprès des demandeurs d'emploi suivis par France Travail révèle que **77 % déclarent avoir utilisé au moins une fois l'IA pour optimiser leur recherche d'emploi**.
Parmi eux, 83 % des moins de 25 ans l'intègrent dans leur stratégie de recherche. Ces chiffres illustrent une réalité désormais structurelle : l'IA n'est pas seulement un outil déployé par les organisations — elle est un outil que les individus mobilisent eux-mêmes dans leur rapport au travail et à l'emploi. Ce « *shadow AI* » des travailleurs pose la question de la formation, des usages acceptables et des inégalités d'accès : 50 % des moins diplômés utilisent l'IA régulièrement, contre 73 % des bac+5.

La zone grise organisationnelle et juridique

L'usage informel soulève des enjeux majeurs en matière de protection des données et de confidentialité. La CNIL a alerté sur les risques liés à l'utilisation d'outils externes d'IA générative dans les environnements professionnels : l'introduction de données internes (informations sur des clients, données stratégiques, données personnelles de collègues) dans des systèmes hébergés à l'extérieur peut entraîner une divulgation d'informations sensibles et exposer l'organisation à des risques juridiques significatifs.

Ces pratiques peuvent également accentuer les écarts entre travailleurs selon leur niveau de maîtrise technologique. Lorsque certains salariés mobilisent des outils d'IA pour accroître leur productivité, les attentes collectives peuvent progressivement s'élever, générant des formes d'intensification du travail et de pression sur les collectifs professionnels — y compris pour ceux qui n'utilisent pas ces outils ou qui ne sont pas à l'aise avec eux.

Une réalité à encadrer collectivement

Pour FO-Cadres, ces évolutions montrent que l'IA ne peut être pensée uniquement comme un outil déployé par les entreprises : elle est désormais un élément structurant de l'activité professionnelle, approprié par les travailleurs eux-mêmes. Cette réalité appelle une reconnaissance et une régulation collective du phénomène de *shadow AI*, afin d'éviter que ces pratiques ne se développent dans un cadre incertain et potentiellement risqué pour les salariés.

À RETENIR

- Reconnaître le phénomène du *shadow AI* comme un enjeu de dialogue social, et non comme une simple question disciplinaire.
- Élaborer, dans le cadre des négociations d'entreprise, des cadres d'usage clairs et négociés : outils autorisés, conditions d'utilisation, règles de protection des données.
- Assurer une information et une formation des salariés aux enjeux juridiques, éthiques et sécuritaires liés à l'usage de l'IA.

• Garantir que l'usage d'outils d'IA ne conduise pas à une intensification implicite des normes de performance ou à une mise en concurrence accrue entre travailleurs.
• Clarifier les règles relatives à la responsabilité et à la propriété des productions réalisées avec l'appui de systèmes d'IA.

Libertés et vie privée : vers une surveillance étendue ?

Le développement des systèmes d'intelligence artificielle s'accompagne d'une capacité inédite de collecte, d'analyse et de croisement des données. Cette puissance technologique ouvre la voie à de nouveaux modes de pilotage du travail, mais soulève également des enjeux majeurs en matière de protection de la vie privée, de dignité et de droits fondamentaux des salariés. Sans cadre clair et régulation effective, ces technologies peuvent contribuer à l'instauration de formes de surveillance renforcée dans les environnements de travail.

La CNIL comme autorité de référence

La CNIL souligne régulièrement que l'usage de dispositifs d'IA dans le monde du travail doit être examiné avec une vigilance particulière. Dans ses guides pratiques et ses décisions de contrôle, elle rappelle que ces systèmes peuvent conduire à une collecte extensive et continue de données relatives aux comportements, aux interactions ou aux performances des travailleurs, parfois au-delà de ce qui est strictement nécessaire à l'activité professionnelle. Elle alerte sur les risques liés à la profilisation et à la catégorisation automatisée des individus, susceptibles d'entraîner des décisions ayant des effets significatifs sur la situation professionnelle des salariés.

En 2024, la CNIL a sanctionné une entreprise pour surveillance disproportionnée de ses salariés via un logiciel comptabilisant les temps supposés d'inactivité, réalisant des captures d'écran à intervalles réguliers et s'ajoutant à une vidéosurveillance permanente. Cette sanction établit un précédent important : le contrôle numérique du travail a des limites juridiques qui

s'imposent aux employeurs, indépendamment des justifications techniques ou économiques avancées.

La dimension collective de la surveillance algorithmique

Au-delà des enjeux techniques et juridiques, la multiplication des dispositifs de mesure et d'analyse peut instaurer un climat de surveillance permanente, susceptible d'altérer la confiance, l'autonomie et la qualité des relations collectives au sein des organisations. La sociologie du travail souligne que ce climat de surveillance généralisée modifie le comportement des travailleurs au-delà du seul espace de travail : il affecte le rapport à l'initiative, à la prise de risque professionnelle et à la coopération informelle — des dimensions essentielles de la qualité du travail que les indicateurs algorithmiques ne mesurent pas.

CAS CONCRET. Projet de vidéosurveillance algorithmique dans un hôpital public français (2023–2024)

Un établissement hospitalier public a envisagé le déploiement d'un système de vidéosurveillance algorithmique dans ses couloirs, présenté comme un outil de sécurité. Les représentants du personnel, informés lors d'une consultation CSE, ont relevé que le système était capable d'analyser les comportements et les mouvements du personnel soignant. Après saisine de la CNIL et expertise, il a été établi que le système collectait des données disproportionnées et que les agents n'avaient pas été correctement informés. Le projet a été modifié pour exclure les zones où travaillent les personnels soignants.
Ce cas illustre comment la consultation CSE, articulée avec le RGPD et les recommandations de la CNIL, peut constituer un contre-pouvoir efficace face aux déploiements disproportionnés.

À RETENIR

• Exiger une transparence renforcée sur les systèmes d'IA utilisés dans les organisations : données collectées, finalités poursuivies, critères des algorithmes.
• Obtenir un encadrement strict des dispositifs de surveillance et de profilage, fondé sur les principes de nécessité, de proportionnalité et de respect de la vie privée.
• Maintenir un contrôle humain effectif sur toute décision ayant un impact sur la situation professionnelle des salariés.
• Intégrer systématiquement ces enjeux dans le dialogue social et la négociation collective, afin de définir des règles claires de gouvernance des données au travail.
• Renforcer les moyens des représentants des salariés pour contrôler les usages de l'IA, notamment en sollicitant l'expertise de la CNIL et en développant la coopération avec le DPO de l'entreprise.

Le partage de la valeur : qui bénéficie réellement des gains ?

Le développement de l'intelligence artificielle est susceptible de générer des gains de productivité considérables. Cependant, l'expérience des précédentes vagues de numérisation montre que les bénéfices économiques tendent à se concentrer entre les mains d'un nombre limité d'acteurs, notamment les grandes plateformes technologiques, les fournisseurs d'infrastructures et les détenteurs de volumes importants de données. Cette dynamique contribue à accentuer les déséquilibres existants dans la répartition de la richesse.

Les salariés, producteurs invisibles de la valeur IA

Pour FO-Cadres, il est impératif que l'essor de l'IA ne conduise pas à une nouvelle phase de concentration de la valeur au détriment des travailleurs. Les salariés participent pleinement à la création de cette richesse, que ce soit par la production et la qualification des données, par l'adaptation des organisations du

travail ou par la mobilisation de leurs compétences pour intégrer et superviser ces technologies. Cette contribution est structurante mais rarement reconnue ni rémunérée.

ÉCLAIRAGE RECHERCHE.
PwC, *Jobs Barometer 2025* — Salaires et compétences IA

L'étude PwC révèle un écart salarial significatif lié à la maîtrise de l'IA : à poste équivalent, les collaborateurs disposant de compétences en IA perçoivent en moyenne **un salaire supérieur de 56 % à celui de leurs pairs** ne maîtrisant pas ces outils. Ce constat a une double implication syndicale. D'une part, il confirme que la formation aux compétences IA est devenue un enjeu de rémunération et d'évolution professionnelle que les NAO doivent intégrer. D'autre part, il soulève la question de l'accès équitable à cette formation : si les compétences IA conditionnent l'évolution salariale, leur inégale distribution entre les salariés constitue un facteur aggravant des inégalités existantes.

L'expérience internationale : négocier les gains

CAS CONCRET. SAG-AFTRA (Hollywood) — La première grève syndicale mondiale pour protéger les droits face à l'IA (2023–2024)

En juillet 2023, le syndicat des acteurs américains SAG-AFTRA a déclenché une grève historique de 118 jours contre les grands studios hollywoodiens. L'un des enjeux centraux était la protection contre l'utilisation de l'IA : les studios entendaient utiliser des reproductions numériques des acteurs, cloner leurs voix et leurs images, sans consentement ni rémunération. La grève a abouti en novembre 2023 à un accord d'un milliard de dollars, incluant des protections sans précédent sur le consentement et la rémunération liés à l'utilisation de l'IA. En juillet 2024, une nouvelle grève a été déclenchée dans le secteur du jeu vidéo, avec les mêmes revendications.

Ces mobilisations constituent la première manifestation internationale du fait que la protection des droits face à l'IA peut devenir un enjeu central de la conflictualité sociale.

Cet exemple n'est pas anecdotique. Il illustre la thèse selon laquelle les technologies ne déterminent pas mécaniquement leur propre régulation : celle-ci résulte de rapports de force sociaux. Le mouvement syndical, en France comme à l'étranger, a la capacité de poser les termes de la négociation sur le partage des gains de l'IA — à condition de s'en saisir avant que les pratiques ne soient établies et les rapports de force figés.

Le cadre de revendication

À RETENIR

- Intégrer la question du partage de la valeur liée à l'IA dans les NAO : si l'IA génère des gains de productivité, une part de ces gains doit être redistribuée aux salariés sous forme de salaires, d'intéressement ou de réduction du temps de travail.
- Exiger une association des représentants des salariés aux décisions relatives à l'introduction et aux usages de l'IA, afin d'évaluer ses effets économiques et sociaux.
- Revendiquer que les données professionnelles produites par les travailleurs soient reconnues comme un actif collectif et non comme une ressource exclusivement mobilisée à des fins de contrôle ou d'optimisation.
- Soutenir une adaptation des cadres fiscaux et économiques afin de mieux capter la valeur produite par les actifs immatériels et les données.
- Promouvoir l'affectation d'une part des gains issus de l'IA au financement de biens collectifs : formation des travailleurs, investissement productif, transition écologique.

Un cadre syndical : partir du travail réel

Les systèmes d'IA ne peuvent et ne doivent pas être traités comme de simples innovations dépourvues d'externalités du seul fait d'une neutralité apparente liée à une conception purement technique. Le positionnement syndical invite à dépasser la dimension de la technologie en tant que telle, pour replacer la question du travail et des droits des salariés au centre.

>> *« Affirmer qu'on est dans une problématique de gouvernance des systèmes d'information ; écouter les professionnels actifs ; ne pas céder aux sirènes du* quick and dirty *; questionner les évidences ; s'organiser pour piloter continûment. L'éthique est trop souvent convoquée comme cerise sur le gâteau, alors que c'est le principe actif de toute la réaction chimique ! »*
— **Yann Ferguson**, LaborIA | Entretien ANACT, juin 2024

Trop souvent, l'IA est encore pensée à partir d'une lecture strictement économique, qui réduit le travail à une somme de tâches individuelles à automatiser ou à optimiser. C'est pourquoi l'action syndicale doit se fonder sur l'observation du terrain pour mettre en relief les transformations en cours sur les activités collectives, les interactions sociales et sur la nature même du travail.

Ce travail syndical est de nature à révéler les conflits de rationalité associés à des dispositifs d'IA conçue uniquement à partir du travail prescrit, alors que le travail réel repose plus largement sur l'ajustement, la coopération et l'intelligence des situations. Les écarts observés entre le travail réel et les dispositifs d'IA sont de nature à nourrir de profonde tensions.

Des risques cognitifs et sociaux peuvent émerger avec force dès lors que l'IA se déploie dans les lieux de travail sans cadre de discussion, de négociation et de formation. Ces risques peuvent être de plusieurs nature allant de la dette cognitive (performance sans apprentissage) au délestage cognitif (abandon de l'esprit et du jugement critiques) en passant par une substitution des interactions humaines par des interactions techniques.

À terme, les travailleurs peuvent faire face à un risque d'isolement et d'ubérisation insidieuse de leur travail.

Partir du travail réel c'est aussi s'interroger sur la transformation des compétences dont l'enjeu dépasse la simple maîtrise technique. Elle pose l'urgence de réponses concrètes sur le développement d'une littératie IA au travail, l'émergence de profils hybrides métier/IA et la nécessité d'une capacité réflexive, notamment pour les plus jeunes.

L'action syndicale en matière d'IA doit porter non seulement sur les conditions de nouvelles formes de production mais également sur l'enjeu de l'utilisation de l'IA pour apprendre sur les lieu de travail.

Cette démarche est indissociable de l'urgence d'un cadre collectif pour encadrer et réguler le déploiement des IA dans les lieux de travail notamment pour faire face intelligemment à la montée des usages spontanés comme ledit « *Shadow IA* ».

Il devient alors indispensable de construire :
- une gouvernance claire ;
- un dialogue social structuré ;
- un alignement entre technologie, travail réel et finalités des organisations.

QUESTIONS À POSER EN CSE

Les questions essentielles ne sont pas « l'outil est-il innovant ? performant ? moderne ? » mais :
- **Qui décide réellement** des usages et des effets de l'outil ?
- L'outil **accroît-il la pression, la cadence, la standardisation** du travail ?
- Les salariés **perdent-ils des marges de manœuvre** et de l'autonomie ?
- Les décisions deviennent-elles **plus opaques**, moins contestables ?
- Les risques de **discrimination** sont-ils accrus ?
- Le professionnel garde-t-il la **maîtrise de son métier** ?
- La responsabilité est-elle transférée à un système **« boîte noire »** ?

POINT DE VIGILANCE //
Transparence et contrôle humain : deux principes directeurs

1. Pas de décision sans contrôle humain effectif. Un outil peut assister, mais ne peut se substituer à la responsabilité humaine, surtout lorsqu'il s'agit d'accès à l'emploi, d'évaluation, de carrière, d'affectation ou de discipline.
2. Pas d'outil structurant sans transparence. Une organisation ne peut exiger des salariés qu'ils se soumettent à un système dont les règles d'usage, les finalités, les effets et les modalités de contrôle ne sont pas clairement établis.

À RETENIR

Maîtriser. Négocier. Protéger

- **Maîtriser :** comprendre les usages, exiger la documentation, rendre visibles les effets réels des outils.
- **Négocier :** transformer les obligations légales (RIA, RGPD, Code du travail) en garanties concrètes sur le travail : contrôle humain, formation, prévention des risques, non-discrimination, qualité du travail.
- **Protéger :** éviter que l'IA devienne un levier d'intensification du travail, de surveillance disproportionnée ou de déresponsabilisation managériale.

PARTIE #4

3 leviers juridiques pour bâtir une vigilance syndicale

4 Les 3 leviers juridiques pour bâtir une vigilance syndicale

L'essor de l'intelligence artificielle dans le monde du travail ne s'opère pas dans un vide normatif. Il s'inscrit dans un ensemble de règles juridiques qui encadrent depuis longtemps la relation de travail — et sur lesquelles les représentants du personnel peuvent s'appuyer dès aujourd'hui. Trois textes forment un triple levier dont la combinaison donne aux organisations syndicales des droits effectifs, concrets et sanctionnés.

Loin d'instaurer un régime d'exception, l'IA vient ainsi se confronter à des principes fondamentaux, issus du droit social et du droit de la non-discrimination, qui conservent toute leur pertinence à l'ère numérique.

Ces principes reposent sur une exigence constante : celle de préserver la dignité des travailleurs, de garantir l'égalité de traitement et d'encadrer l'exercice du pouvoir de direction de l'employeur. En ce sens, les outils algorithmiques ne sauraient être considérés comme neutres ou autonomes ; ils s'inscrivent dans la responsabilité de l'employeur, qui demeure tenu de justifier ses décisions et d'en assumer les conséquences juridiques.

L'introduction de systèmes d'IA ne modifie donc pas la nature des obligations fondamentales, mais en renouvelle les conditions d'application. Elle en révèle aussi les tensions, en particulier lorsque des décisions sont médiatisées par des dispositifs techniques opaques ou fondées sur des corrélations statistiques difficilement interprétables. Dans ce contexte, le droit apparaît moins comme un frein à l'innovation que comme un cadre structurant, destiné à en orienter les usages et à en prévenir les dérives.

Ainsi, l'analyse des règles issues du droit social et du droit de la non-discrimination constitue un préalable indispensable pour comprendre les conditions dans lesquelles l'intelligence artificielle peut être mobilisée dans le monde du travail, sans porter atteinte aux droits fondamentaux des travailleurs.

LES TROIS LEVIERS

1. Le Code du travail : le levier social fondamental, celui qui s'applique depuis toujours à l'introduction de nouvelles technologies.
2. Le Règlement sur l'IA (RIA / AI Act) : le premier cadre juridique européen spécifique à l'IA. En vigueur progressivement depuis 2025. Il rend visible ce qui était opaque, impose des obligations opposables, et prévoit des sanctions lourdes.
3. Le RGPD : encadre le traitement des données personnelles par les systèmes d'IA. Cumul avec le RIA : la conformité à l'un ne dispense pas de la conformité à l'autre.

Le Code du travail, le premier levier juridique immédiatement applicable

Le droit social constitue le socle normatif à partir duquel doit être appréhendée l'introduction de l'IA dans la relation de travail. Structuré autour de la protection du salarié dans un lien de subordination, il organise un équilibre entre le pouvoir de direction de l'employeur et les droits fondamentaux des travailleurs. Cet équilibre ne disparaît pas avec l'usage de technologies algorithmiques — il en conditionne, au contraire, la légitimité.

Les systèmes d'IA, parce qu'ils participent de l'exercice du pouvoir de direction, doivent être soumis aux mêmes exigences de justification, de proportionnalité et de contrôle que toute autre décision managériale. L'employeur qui déploie un outil d'IA ne délègue pas sa responsabilité à un algorithme : il en assume pleinement les effets juridiques.

Les articles clés : tableau de référence

ARTICLE	CONTENU	APPLICABILITÉ À L'IA
L.2312-8	Information-consultation du CSE sur les questions intéressant la marche générale de l'entreprise, notamment l'introduction de nouvelles technologies	Clé de voûte : toute IA impactant l'organisation du travail déclenche la consultation obligatoire
L.2312-14	La consultation doit intervenir avant toute décision définitive de l'employeur	Interdit tout déploiement anticipé — même en phase pilote — avant l'avis du CSE

ARTICLE	CONTENU	APPLICABILITÉ À L'IA
L.2312-17	Trois consultations récurrentes obligatoires : orientations stratégiques, situation économique, politique sociale	Permet d'aborder l'IA dans les grandes consultations annuelles
L.2312-38	Information préalable sur les méthodes de recrutement, les traitements automatisés de gestion du personnel et les moyens de contrôle de l'activité	Obligation spécifique pour tout outil IA en RH, recrutement, évaluation ou surveillance
L.2315-94	Droit à expertise en cas d'introduction de nouvelles technologies ou de projet important modifiant les conditions de travail	Expertise financée à 80 % par l'employeur ; délai de consultation porté à 2 mois
L.2315-80	Financement de l'expertise : 80 % employeur, 20 % CSE	Applicable à l'expertise IA
L.4121-1	Obligation de sécurité de l'employeur : protéger la santé physique et mentale des travailleurs	Impose l'évaluation des risques liés à l'IA dans le DUERP
L.1221-8	Le candidat à un emploi est informé des méthodes et techniques de recrutement utilisées à son égard	Droit individuel du candidat face aux outils IA de recrutement
L.2317-1	Délit d'entrave au fonctionnement du CSE : amende de 7 500 € (pers. physique) ou 37 500 € (pers. morale)	Sanction pénale applicable en cas de déploiement d'IA sans consultation

POINT DE VIGILANCE // Le droit du travail français ne comporte pas encore de régime spécifique pour l'IA. Mais plusieurs dispositions existantes s'appliquent pleinement dès lors que ces technologies affectent l'organisation du travail, les conditions d'emploi, la santé ou les méthodes de gestion.
Ces articles sont tous vérifiés et en vigueur.

La consultation du CSE : mode d'emploi en 4 étapes

Étape 1 — En amont du projet : l'information-consultation préalable

BASE LÉGALE — Art. L.1221-8 + Art. L.1221-9 Code du travail + Art. 6 RGPD
Le CSE est informé et consulté sur l'introduction de nouvelles technologies et tout aménagement important modifiant les conditions de santé et de sécurité ou les conditions de travail. La consultation doit intervenir avant toute décision définitive de l'employeur.

C'est l'article central pour les élus. Il impose à l'employeur de soumettre son projet au CSE avant de le déployer — y compris en phase pilote, y compris pour une « mise à jour » d'un outil existant si cette mise à jour constitue une nouvelle technologie. L'employeur doit remettre au CSE les informations permettant un avis éclairé : description du projet, objectifs poursuivis, impacts sur l'organisation du travail, l'emploi et les compétences, effets possibles sur la santé et les conditions de travail.

À RETENIR. Phase pilote : pas d'exception La jurisprudence est claire : la consultation doit intervenir dès le stade du projet. Une phase pilote ou une expérimentation n'exonère pas l'employeur de l'obligation de consultation préalable (TJ Nanterre, 14 février 2025 ; TJ Paris, 2 septembre 2025). Tout déploiement anticipé — même partiel, même expérimental — constitue un trouble manifestement illicite.

BASE LÉGALE — Art. L.2312-38 du Code du travail — Spécifique aux outils RH et de contrôle
Le CSE est informé préalablement à leur utilisation sur les méthodes ou techniques d'aide au recrutement ainsi que sur tout traitement automatisé de gestion du personnel. Il est informé et consulté sur les moyens ou techniques permettant un contrôle de l'activité des salariés.

Cet article est souvent méconnu et pourtant fondamental.
Il s'applique à trois catégories d'outils particulièrement répandus : les IA de recrutement (tri de CV, scoring de candidats), les traitements automatisés de gestion RH (SIRH avec fonctionnalités IA), et les systèmes de contrôle ou de surveillance de l'activité. Pour ces systèmes, la consultation du CSE est obligatoire même en dehors de tout « projet important ».
L'article L.1221-8 du même code prévoit par ailleurs que tout candidat à l'emploi doit être informé individuellement des méthodes de recrutement utilisées à son égard.

Étape 2 — Pendant la phase d'étude : l'expertise CSE

BASE LÉGALE — Art. L.2315-94 + Art. L.2315-80 du Code du travail
Le CSE peut se faire assister par un expert habilité en cas d'introduction de nouvelles technologies ou de projet important modifiant les conditions de travail. L'expertise est financée à 80 % par l'employeur et 20 % par le CSE. Le recours à l'expertise porte le délai de consultation à 2 mois.

Le recours à l'expertise est un droit et un outil puissant. Un expert technique peut analyser le fonctionnement réel du système (données utilisées, logique de décision, biais potentiels), évaluer l'impact sur l'organisation du travail et la santé des salariés, identifier les risques juridiques (discrimination, surveillance disproportionnée) et aider le CSE à formuler un avis éclairé ou à négocier des garanties.

CE QUE L'EXPERT PEUT ANALYSER

- **Le fonctionnement technique :** données d'entrée, logique de décision, opacité du modèle, risques de biais.
- **L'impact sur l'organisation du travail :** modification des tâches, des qualifications, de l'autonomie, de la charge.
- **Les effets sur la santé et la sécurité :** risques psychosociaux, surveillance, intensification, pression.
- **Les risques juridiques :** conformité RGPD, qualification RIA, risques de discrimination directe ou indirecte.
- **Le contrat fournisseur :** garanties, documentation de conformité, clauses sur les données.

Étape 3 — Pendant le déploiement : suivi et prévention

BASE LÉGALE — Art. L.2312-9, L.2312-26 + Art. L.4121-1 du Code du travail
Le CSE contribue à la prévention des risques professionnels. L'employeur est tenu d'une obligation générale de sécurité : prendre toutes les mesures nécessaires pour protéger la santé physique et mentale des travailleurs.

Une fois le projet déployé, le rôle du CSE ne s'arrête pas. Les élus peuvent demander l'actualisation du Document Unique d'Évaluation des Risques Professionnels (DUERP) pour intégrer les risques liés à l'IA, proposer des mesures de prévention, suivre les effets du système sur la charge de travail et les compétences, et déclencher des enquêtes en cas de risque avéré pour la santé ou les conditions de travail. La CSSCT joue ici un rôle essentiel dans l'identification et le suivi des risques psychosociaux spécifiques liés à l'IA.

Étape 4 — En cas de manquement : le recours judiciaire

BASE LÉGALE — Art. L.2317-1 du Code du travail + Art. 835 du Code de procédure civile
L'entrave au fonctionnement du CSE est constitutive d'un délit pénal (amende de 7 500 € pour une personne physique, 37 500 € pour une personne morale).
Le trouble manifestement illicite peut être constaté par le juge des référés, qui peut ordonner la suspension immédiate du dispositif.

Si l'employeur déploie un système d'IA sans consultation préalable, ou poursuit le déploiement avant que le CSE ait rendu son avis, les représentants du personnel disposent de deux voies de recours : le juge des référés pour obtenir la suspension immédiate du dispositif, et le tribunal correctionnel pour le délit d'entrave.

JURISPRUDENCE — TJ Nanterre
14 février 2025 (n°24/01457)

Une entreprise avait déployé de nouvelles applications d'IA sans attendre la fin de la consultation du CSE. Le tribunal a considéré que ce déploiement anticipé constituait un trouble manifestement illicite et a ordonné la suspension du dispositif. Décision confirmant que la consultation du CSE est une exigence incontournable pour les projets d'IA en entreprise.

JURISPRUDENCE — TJ Paris
2 septembre 2025 (n°25/53278) - France Télévisions

Le CSE de France Télévisions avait demandé la consultation sur le déploiement d'une plateforme d'accès aux outils d'IA générative. Le tribunal a ordonné la consultation en qualifiant la plateforme de « technologie nouvelle » *au sens de l'article L.2312-8, précisant que l'outil* « dépasse la simple mise à disposition d'un outil informatique »*. En revanche, la montée de version d'un chatbot RH existant n'a pas été considérée comme une nouvelle technologie, faute de modification substantielle.*

JURISPRUDENCE — TJ Créteil
15 juillet 2025 (n°25/00851) - Secteur Presse

Le tribunal a confirmé le droit à consultation du CSE pour l'implantation d'outils d'IA dans l'intranet d'un groupe de presse, permettant la génération automatique de contenu. Ces outils ont été qualifiés de « nouvelle technologie susceptible d'affecter les conditions de travail » *des journalistes.*

POINT DE VIGILANCE // La consultation du CSE n'est pas qu'une formalité : c'est une arme. Si l'employeur passe outre, le juge peut suspendre immédiatement le déploiement, même si des milliers de salariés utilisent déjà l'outil depuis des mois. Et si des risques psychosociaux sont documentés, le Conseil de prud'hommes peut également ordonner la suspension (CPH Lyon, 22 janvier 2025).

Les consultations récurrentes : intégrer l'IA dans l'agenda social permanent

BASE LÉGALE — Art. L.2312-17 du Code du travail
Le CSE est consulté chaque année sur : les orientations stratégiques de l'entreprise ; la situation économique et financière de l'entreprise ; la politique sociale de l'entreprise, les conditions de travail et l'emploi.

Ces trois consultations constituent des points d'entrée permanents pour aborder l'IA dans le dialogue social. Elles permettent d'agir en amont des projets, avant même que des décisions de déploiement soient annoncées.
Voici comment les utiliser :

Comment intégrer l'IA dans les trois consultations récurrentes

Orientations stratégiques (L.2312-17, 1°) : aborder les projets futurs de déploiement de SIA, leurs conséquences sur l'activité, l'emploi, les métiers, les compétences, la GPEC et les orientations de formation. Exiger que le plan stratégique IA de l'entreprise soit présenté au CSE.
Situation économique et financière (L.2312-17, 2°) : aborder les investissements réalisés ou prévus en IA, les économies attendues (ex. : gains de productivité), la répartition des gains entre capital et travail, les effets sur la politique de R&D.
Politique sociale, conditions de travail et emploi (L.2312-17, 3°) : aborder les effets de l'IA sur l'emploi, les qualifications, la formation, la prévention des risques professionnels, les conditions de travail et le temps de travail. Exiger la mise à jour du DUERP.

La négociation collective : transformer les droits en clauses opposables

Les délégués syndicaux peuvent aborder les problématiques d'IA dans le cadre des négociations obligatoires, et transformer ainsi des protections légales en garanties contractuelles plus exigeantes.

Les quatre négociations obligatoires à mobiliser

- **NAO rémunération et partage de la valeur :** impacts de l'IA sur le temps de travail, répartition des gains de productivité entre capital et travail, négociation sur les primes liées aux compétences IA.
- **NAO égalité professionnelle et QVCT :** impacts différenciés selon le genre, politique de prévention des risques liés à l'IA, qualité du management et droit à la déconnexion.
- **NTO sur la GEPP :** catégories d'emplois affectées par les évolutions technologiques, politique de formation et de reconversion, emploi des jeunes.
- **NTO emploi et conditions de travail des salariés expérimentés** : effets des transformations technologiques sur les seniors, politique de formation et de transmission des compétences.

Le droit de la non-discrimination : un levier souvent sous-utilisé

Le droit de la non-discrimination constitue un pilier essentiel de l'encadrement des usages de l'IA dans le monde du travail. Fondé sur le principe d'égalité de traitement, il interdit toute différenciation injustifiée entre les individus, directe ou indirecte, à toutes les étapes de la relation de travail.

L'introduction de systèmes algorithmiques complexifie les modalités d'application de ce principe, sans en remettre en cause l'exigence. Les discriminations peuvent désormais émerger de mécanismes statistiques, de corrélations ou de biais présents dans les données d'apprentissage — sans intention consciente, et pourtant avec des effets réels et juridiquement condamnables. La responsabilité de l'employeur demeure pleinement engagée : le recours à un outil algorithmique, qu'il soit développé en interne ou fourni par un prestataire, ne saurait exonérer de l'obligation de garantir l'égalité de traitement.

POINT DE VIGILANCE // La discrimination indirecte produite par un algorithme est aussi illégale que la discrimination directe intentionnelle. L'employeur qui déploie un outil de recrutement ou d'évaluation biaisé engage sa responsabilité civile et pénale, même s'il ignorait l'existence du biais.

Le règlement européen sur l'IA (RIA/*AI Act*), un levier juridique européen inédit avec des sanctions directes

Le règlement européen sur l'intelligence artificielle (Règlement UE 2024/1689, dit « *AI Act* » ou « RIA ») est la première initiative de l'Union européenne établissant un cadre réglementaire global et contraignant pour l'IA. Il est entré en vigueur le 1er août 2024 et s'applique progressivement.

Pour les représentants du personnel, ce règlement est d'une importance stratégique majeure : il rend visible ce qui était opaque, il impose aux employeurs des obligations documentaires opposables, et il prévoit des sanctions financières très significatives pour les manquements.

La logique fondamentale : une approche par les risques

L'architecture du RIA repose sur une idée simple mais structurante : tous les systèmes d'IA ne présentent pas le même niveau de risque pour les droits fondamentaux. Le règlement ne réglemente donc pas uniformément tous les systèmes, mais en fonction de leur dangerosité potentielle. Plus le système peut affecter les droits des personnes, plus les obligations sont lourdes.

Le « déployeur » au sens du RIA est la personne physique ou morale qui utilise un système d'IA dans un contexte professionnel, sous sa propre autorité. Dans la quasi-totalité des situations en entreprise, l'employeur est le déployeur. C'est lui qui supporte les obligations découlant du règlement — et non le fournisseur qui a développé l'outil. Cette qualification est fondamentale : elle signifie que même si l'outil est un logiciel acheté à un éditeur, c'est l'employeur qui en assume la responsabilité réglementaire dans l'usage qu'il en fait.

La pyramide des risques : ce que chaque niveau signifie concrètement

Le RIA distingue quatre niveaux de risque, auxquels correspondent des obligations différentes. Le tableau suivant présente cette échelle avec les exemples concrets du monde du travail et les sanctions applicables.

Niveau / Catégorie	Exemples dans le monde du travail	Sanction max.	En vigueur
NIVEAU 4 — RISQUE INACCEPTABLE *SYSTÈMES INTERDITS* Obligation : Interdiction totale — contester la légalité, pas négocier	Manipulation comportementale, notation sociale, inférence d'émotions au travail, catégorisation biométrique (affiliation syndicale, religion…), identification biométrique en temps réel dans l'espace public	**35 M€ ou 7 % CA mondial**	2 fév. 2025
NIVEAU 3 — HAUT RISQUE *Obligations renforcées —* Obligation : Documentation, contrôle humain, traçabilité, information des salariés, audit	Manipulation comportementale, notation sociale, inférence d'émotions au travail, catégorisation biométrique (affiliation syndicale, religion…), identification biométrique en temps réel dans l'espace public	**15 M€ ou 3 % CA mondial**	2 août 2026
NIVEAU 2 — RISQUE LIMITÉ *Obligations de transparence —* Obligation : Informer les utilisateurs qu'ils interagissent avec une IA ou que le contenu est généré par IA	Chatbots, assistants de rédaction, IA générative, deepfakes, systèmes d'interaction avec des humains, contenus synthétiques	**7, 5 M€ ou 1, 5 % CA mondial**	2 août 2025
NIVEAU 1 — RISQUE MINIMAL *Libre d'usage — Codes de bonne pratique encouragés* Obligation : Aucune obligation réglementaire spécifique (codes de bonnes pratiques volontaires)	Filtres anti-spam, jeux vidéo, IA de recommandation non critique, outils de productivité sans impact décisionnel	—	Immédiat

POINT DE VIGILANCE // Pour identifier le niveau de risque d'un système déployé dans l'entreprise, les représentants du personnel peuvent demander à l'employeur de justifier la qualification retenue et les documents qui l'étayent. En cas de qualification incorrecte, l'employeur engage sa responsabilité réglementaire.

Les systèmes interdits (risque inacceptable) : ce qui est interdit dès maintenant

Depuis le 2 février 2025, les systèmes d'IA relevant de la catégorie « *risque inacceptable* » sont totalement interdits dans l'Union européenne. Cette interdiction s'impose à tous les acteurs — fournisseurs, importateurs, distributeurs et déployeurs. Les systèmes concernés font l'objet d'une interdiction pure et simple de mise sur le marché, de mise en service et d'utilisation.

Dans le monde du travail, les pratiques interdites les plus directement pertinentes sont :

- **L'inférence des émotions sur le lieu de travail** en dehors de toute raison médicale ou de sécurité expressément définie. Tout système qui prétend analyser l'état émotionnel des salariés (via la voix, le visage, la posture ou d'autres signaux) est interdit.
- **La catégorisation biométrique** pour déduire l'affiliation à une organisation syndicale, les convictions religieuses ou philosophiques, les opinions politiques, la vie sexuelle ou l'orientation sexuelle d'une personne.
- **La manipulation comportementale subliminale** susceptible d'altérer le comportement d'une personne sans qu'elle en soit consciente, au détriment de ses intérêts.
- **L'exploitation des vulnérabilités** d'une personne (âge, handicap, situation économique ou sociale difficile) pour l'amener à des décisions contraires à ses intérêts.

À RETENIR. Ces systèmes ne se négocient pas
Si un outil IA déployé dans l'entreprise relève de ces pratiques interdites, la réponse syndicale n'est pas la négociation — c'est la contestation de sa légalité. Ces pratiques sont prohibées par la loi, indépendamment de tout bénéfice économique ou organisationnel avancé par l'employeur. Non-respect : sanctions pouvant atteindre 35 millions d'euros ou 7 % du chiffre d'affaires mondial.

Les systèmes à haut risque : le cœur du sujet pour les représentants du personnel

Les systèmes à haut risque constituent la catégorie la plus importante pour les représentants du personnel. Ces systèmes ne sont pas interdits, mais soumis à un régime juridique exigeant.
Leurs obligations entrent en vigueur le 2 août 2026.

Quels systèmes sont à haut risque dans le monde du travail ?

Le RIA identifie explicitement, dans son annexe III, les systèmes utilisés dans le domaine de l'emploi, la gestion des travailleurs et l'accès au travail indépendant comme relevant du haut risque. Sont concernés :

- **Les systèmes de recrutement :** tri automatique de CV, *scoring* de candidats, classement des candidats, pré-sélection algorithmique.
- **Les systèmes d'évaluation et de notation des salariés :** mesure de la performance, attribution de scores, classements individuels. Incluent les systèmes utilisés dans les centres d'appels, la logistique, l'industrie.
- **Les systèmes d'affectation des tâches et d'organisation du travail :** planification automatique, tournées, répartition des missions lorsqu'ils influencent directement les conditions de travail.
- **Les systèmes contribuant aux décisions de gestion des carrières :** promotion, formation, mobilité interne, rupture du contrat.

POINT DE VIGILANCE // Conséquence pratique : dès lors qu'un système d'IA est utilisé dans l'entreprise pour une de ces finalités, l'employeur est soumis aux obligations renforcées de l'article 26 du RIA. Ces obligations constituent autant de droits pour les représentants du personnel.

Les obligations de l'article 26 RIA : ce que le CSE peut exiger

L'article 26 du RIA fixe les obligations principales des déployeurs de systèmes à haut risque. Le tableau suivant traduit chaque obligation en droit d'action pour les représentants du personnel.

Obligation (Art. 26 RIA)	Ce que l'employeur doit faire concrètement	Ce que le CSE/DS peut exiger
Utiliser le système conformément aux instructions (§1)	Respecter la notice d'utilisation du fournisseur. Ne pas modifier les paramètres au-delà des usages prévus.	Obtenir la notice d'utilisation du système. Vérifier que les usages réels correspondent aux usages prévus.
Assurer un contrôle humain effectif (§2)	Nommer des personnes compétentes capables de comprendre, surveiller et corriger les décisions du système.	Demander : qui sont les responsables du contrôle humain ? Quelle formation ont-ils reçue ? Peuvent-ils réellement corriger ou annuler les décisions ?
Assurer un contrôle humain effectif (§2)	Nommer des personnes compétentes capables de comprendre, surveiller et corriger les décisions du système.	Demander : qui sont les responsables du contrôle humain ? Quelle formation ont-ils reçue ? Peuvent-ils réellement corriger ou annuler les décisions ?
Vérifier la pertinence des données d'entrée (§4)	S'assurer que les données utilisées sont représentatives, exactes et à jour. Identifier les données biaisées.	Demander la liste des données utilisées. Exiger des tests anti-biais avant déploiement et à intervalles réguliers.
Surveiller le fonctionnement et signaler les incidents (§5)	Mettre en place une procédure de détection des anomalies et d'alerte au fournisseur et aux autorités.	Demander le plan de surveillance et la procédure d'incident. Exiger d'être informés de tout incident ou dysfonctionnement.

Obligation (Art. 26 RIA)	Ce que l'employeur doit faire concrètement	Ce que le CSE/DS peut exiger
Conserver les journaux (logs) pendant au moins 6 mois (§6)	Tenir des journaux automatiques des décisions et actions du système. Les conserver 6 mois minimum.	Exiger l'accès aux logs en cas de contestation d'une décision. Vérifier que les logs permettent de retracer les décisions individuelles.
Informer les travailleurs avant déploiement (§7)	Avant d'utiliser un système d'IA à haut risque sur le lieu de travail, informer les travailleurs et leurs représentants.	Droit à l'information préalable opposable. Peut être articulé avec la consultation du CSE (art. L.2312-8 C. trav.).
Informer les personnes soumises au système (§11)	Informer chaque personne physique concernée qu'elle est soumise à un système d'IA à haut risque.	Chaque salarié doit être informé personnellement. Ce droit est individuel et opposable à l'employeur.
Coopérer avec les autorités de contrôle	Fournir toute documentation demandée par l'autorité nationale compétente.	Les représentants du personnel peuvent signaler des manquements aux autorités (CNIL, autorité nationale IA).

L'analyse d'impact sur les droits fondamentaux (FRIA) — Article 27 RIA

BASE LÉGALE — Art. 27 du RIA — Analyse d'impact sur les droits fondamentaux

Avant le déploiement d'un système d'IA à haut risque, les déployeurs qui sont des organismes de droit public ou des entités privées fournissant des services publics (et certains systèmes en annexe III §5) effectuent une analyse de l'impact sur les droits fondamentaux.

Attention : l'obligation formelle de FRIA (article 27) ne s'impose, pour les entreprises privées de droit commun, qu'à celles qui gèrent des services essentiels ou opèrent dans des domaines spécifiques. Les entreprises privées « *ordinaires* » ne sont pas soumises à la FRIA formelle, mais restent tenues aux obligations de l'article 26 (contrôle humain, logs, information des personnes). Pour les organismes publics et les entreprises de services essentiels, la FRIA doit être réalisée avant le déploiement et ses résultats enregistrés auprès de l'autorité nationale compétente.

Ce que les représentants du personnel peuvent demander : même pour les entreprises non soumises à la FRIA formelle, les élus peuvent exiger que l'employeur documente les impacts du système sur les droits fondamentaux des travailleurs dans le cadre de la consultation CSE. Cette documentation peut être négociée comme condition préalable à tout déploiement.

Les systèmes à risque limité : transparence obligatoire

BASE LÉGALE — Art. 50 du RIA — Obligations de transparence
Les déployeurs de systèmes d'IA qui interagissent avec des personnes physiques (chatbots, assistants de rédaction, systèmes générant des contenus synthétiques) doivent informer les personnes qu'elles interagissent avec une IA ou que le contenu a été généré par une IA.

Cette catégorie concerne directement les outils d'IA générative désormais très répandus en entreprise. Même si l'outil n'est pas classé « haut risque », l'entreprise est tenue :

- d'informer les salariés lorsqu'ils interagissent avec un *chatbot* ou un agent IA ;
- d'indiquer que des contenus (textes, images, synthèses, comptes-rendus) ont été générés ou modifiés par une IA ;
- pour les contenus susceptibles d'influencer le public sur des questions d'intérêt général, d'indiquer explicitement la génération algorithmique.

POINT DE VIGILANCE // Même hors « haut risque », l'entreprise doit informer les salariés lorsque l'IA est utilisée dans leurs outils de travail. Cette obligation de transparence est opposable à l'employeur et peut être intégrée dans les accords d'entreprise.

Le calendrier de mise en application : ce qui est en vigueur maintenant

Calendrier ria — ce qui s'applique et quand

- **2 février 2025 — En vigueur :** Interdiction totale des systèmes à risque inacceptable (art. 5). Sanctions : jusqu'à 35 M€ ou 7 % du CA mondial.
- **2 août 2025 — En vigueur :** Obligations pour les fournisseurs de modèles d'IA à usage général (LLM type GPT, Claude, Gemini…). Obligations de transparence de l'art. 50 (*chatbots*, contenus synthétiques).
- **2 février 2026 — En vigueur :** Acte sur la surveillance post-commercialisation des systèmes d'intelligence artificielle.
- **2 août 2026 — En vigueur :** Obligations complètes pour les systèmes à haut risque (annexe III). Les États membres doivent avoir mis en place leurs sanctions. ATTENTION : c'est à cette date que les droits des travailleurs et des CSE face aux systèmes à haut risque RH deviennent pleinement opposables avec toutes leurs sanctions.
- **2 août 2027 — En vigueur :** Systèmes à haut risque utilisés comme composants de sécurité d'un produit.
- **D'ici fin 2030 :** Systèmes intégrés dans des systèmes d'information à grande échelle dans les domaines liberté, sécurité, justice.

À RETENIR.
2026 : Les employeurs doivent se préparer maintenant

Les obligations des systèmes à haut risque en matière de travail entrent en vigueur le 2 août 2026. Mais la documentation, les audits anti-biais, la formation du personnel et l'information des salariés demandent du temps. Les entreprises qui attendent 2026 pour commencer leur mise en conformité s'exposent à des sanctions immédiates dès la date d'entrée en vigueur. Les représentants du personnel ont intérêt à anticiper cette échéance dès maintenant dans les consultations CSE et les négociations.

Les sanctions : un outil de pression

Tableau des sanctions du RIA (article 99)

Infraction	Montant maximum	Art.RIA
Utilisation d'un système à risque inacceptable (interdit)	**35 millions € ou 7 % du CA annuel mondial (le plus élevé)**	Art. 99 §3
Non-respect des obligations pour systèmes à haut risque (art. 26 RIA)	**15 millions € ou 3 % du CA annuel mondial (le plus élevé)**	Art. 99 §4
Fourniture d'informations inexactes ou trompeuses aux autorités	**7, 5 millions € ou 1, 5 % du CA annuel mondial (le plus élevé)**	Art. 99 §5

À ces sanctions administratives s'ajoutent les sanctions pénales du Code du travail (délit d'entrave : 7 500 € à 37 500 €) et les recours civils des salariés discriminés par un système d'IA biaisé.

Les documents que les élus peuvent exiger

Checklist — Documents à demander à l'employeur

Documents obligatoires pour les systèmes à haut risque (art. 26 RIA) :

- La notice d'utilisation fournie par le fournisseur (art. 13 RIA) : finalités, capacités, limites, risques identifiés par le fournisseur
- La documentation technique de conformité du fournisseur (marquage CE pour les systèmes à haut risque)
- La preuve d'enregistrement dans la base de données UE des systèmes à haut risque (art. 71 RIA) — pour les organismes publics
- La politique de contrôle humain : qui, comment, avec quelle compétence ?
- Les journaux (logs) du système conservés pendant 6 mois minimum (art. 26 §6 RIA)
- Le résultat des tests anti-biais réalisés avant le déploiement

Documents à exiger dans le cadre de la consultation CSE :

- Description complète du projet : finalité, périmètre, populations concernées, niveau d'automatisation

Checklist — Documents à demander à l'employeur

- Qualification RIA retenue par l'employeur et justification
- Impact sur l'organisation du travail, les compétences et l'emploi
- Effets possibles sur la santé et les conditions de travail
- Plan de formation et d'information des salariés
- Contrat avec le fournisseur : clauses de confidentialité des données, droits d'audit, engagements de conformité

Documents supplémentaires pour les droits individuels des salariés :

- En vertu de l'art. 26 §11 RIA : information individuelle à chaque personne soumise à un système à haut risque
- En vertu de l'art. 86 RIA : droit à l'explication de toute décision individuelle prise ou assistée par un système d'IA à haut risque
- En vertu de l'art. 22 RGPD : droit de ne pas être soumis à une décision fondée exclusivement sur un traitement automatisé

RIA et RGPD : deux obligations cumulatives, non alternatives

Un point essentiel souvent mal compris : conformité au RGPD et conformité au RIA sont deux exigences distinctes et cumulatives. Un système d'IA peut être parfaitement conforme au RGPD — avoir une base légale valide, respecter la minimisation des données, informer les personnes concernées — et pourtant être non conforme au RIA, par exemple parce qu'il est à haut risque et déployé sans contrôle humain ni documentation.

RGPD — Traitements de données personnelles

- Base légale du traitement
- Minimisation des données
- Droits des personnes (accès, rectification, opposition)
- Analyse d'impact sur les données (AIPD — art. 35 RGPD)
- Droit de ne pas être soumis à une décision automatisée (art. 22 RGPD)

RIA — systèmes d'intelligence artificielle

- Classification du niveau de risque
- Contrôle humain effectif (art. 26 §2)
- Documentation et traçabilité (logs 6 mois)
- Information des travailleurs avant déploiement (art. 26 §7)
- Droit à l'explication des décisions IA (art. 86 RIA)

QUESTIONS À POSER EN CSE

La question pour l'employeur n'est plus seulement :
« Avons-nous une base légale RGPD ? » *mais aussi* ***« Avons-nous qualifié correctement notre système d'IA selon le RIA et rempli les obligations qui s'y attachent ? »***

À RETENIR. Ce que le triple levier permet d'obtenir

• **Via le Code du travail :** consultation préalable obligatoire (art. L.2312-8), expertise financée (art. L.2315-94), information sur les méthodes de recrutement et contrôle (art. L.2312-38), suspension judiciaire en cas de manquement, délit d'entrave (art. L.2317-1).
• **Via le RIA (applicable au monde du travail) :** documentation technique obligatoire, contrôle humain effectif, logs conservés 6 mois, information individuelle des personnes soumises au système, droit à l'explication des décisions, sanctions jusqu'à 15 M€ ou 3 % du CA pour les systèmes à haut risque.
• **Via le RGPD :** droit d'accès aux données traitées, droit de ne pas être soumis à une décision exclusivement automatisée (art. 22), analyse d'impact obligatoire pour les traitements à haut risque, sanctions jusqu'à 20 M€ ou 4 % du CA mondial.

Ce qui n'est pas documenté ne peut pas être contrôlé. Ce qui n'est pas contrôlé ne protège pas. L'exigence de documentation est le premier acte syndical face à l'IA.

Le RGPD : la protection des données personnelles, un levier juridique plus que jamais d'actualité face à l'IA

Le Règlement général sur la protection des données (RGPD, Règlement UE 2016/679, applicable depuis le 25 mai 2018) constitue le troisième pilier du dispositif juridique encadrant l'usage de l'intelligence artificielle dans le monde du travail. Il s'applique à tout traitement de données personnelles — et les systèmes d'IA déployés dans les organisations traitent massivement de telles données, qu'il s'agisse des dossiers des candidats, des évaluations des salariés, des données comportementales collectées sur les postes de travail, des communications professionnelles ou des données de géolocalisation.

Contrairement à ce que l'on entend parfois, le RGPD n'est pas un obstacle à l'IA. C'est un cadre qui impose que l'IA soit conçue et utilisée dans le respect des droits fondamentaux des personnes. Pour les représentants du personnel, il constitue un levier d'action immédiatement opérationnel : ses principes sont directement opposables à l'employeur, ses droits sont exercés individuellement par chaque salarié, et son non-respect est sanctionné par une autorité indépendante — la Commission nationale de l'informatique et des libertés (CNIL) — dont l'activité de contrôle dans le domaine du travail s'intensifie fortement.

RGPD et RIA : deux obligations cumulatives, non alternatives

Un système d'IA peut être conforme au RGPD et pourtant non conforme au RIA — et inversement. Ces deux règlements ne régulent pas la même chose. Le RGPD encadre les traitements de données personnelles. Le RIA encadre les systèmes d'IA eux-mêmes. La conformité à l'un ne dispense pas de la conformité à l'autre. Les responsables de traitement qui pensent s'en tenir à leur politique RGPD pour couvrir leurs obligations IA sont dans l'erreur — et les représentants du personnel doivent connaître cette distinction pour l'utiliser.

	RGPD (Règlement UE 2016/679)	RIA / AI Act (Règlement UE 2024/1689)
Objet	Protéger les personnes physiques à l'égard du traitement de leurs données personnelles	Encadrer le développement, la mise sur le marché et l'utilisation des systèmes d'IA

	RGPD (Règlement UE 2016/679)	RIA / AI Act (Règlement UE 2024/1689)
Question centrale	Le traitement de données est-il licite et proportionné ?	Le système d'IA est-il acceptable, et à quel niveau de risque ?
Acteur visé	Le responsable de traitement (et son sous-traitant)	Le fournisseur (développeur) et le déployeur (utilisateur professionnel)
Droits accordés	Droits d'accès, rectification, opposition, effacement, portabilité, explication, refus des décisions automatisées (art. 22)	Droit à l'information avant déploiement (art. 26 §7 et 11), droit à l'explication des décisions IA (art. 86)
Obligations clés	Base légale, finalité, minimisation, sécurité, information, DPIA pour risques élevés	Documentation, contrôle humain, traçabilité (logs 6 mois), information des travailleurs, gestion des risques
Sanctions max.	20 M€ ou 4 % du CA mondial (art. 83 §5 RGPD)	35 M€ ou 7 % du CA (IA interdite) / 15 M€ ou 3 % (haut risque)
Autorité de contrôle en France	CNIL	Autorité nationale IA (en cours de désignation) + CNIL pour le volet données
Articulation	Cumul obligatoire : RGPD + RIA s'appliquent simultanément. L'AIPD (RGPD art. 35) et la FRIA (RIA art. 27) sont deux analyses distinctes et complémentaires.	Idem

Le RGPD dans le contexte professionnel : pourquoi s'applique-t-il à l'IA ?

Le RGPD s'applique à tout traitement de données à caractère personnel, c'est-à-dire à toute information permettant d'identifier directement ou indirectement une personne physique.

Dans le contexte de l'IA au travail, cela couvre un périmètre extrêmement large : les données RH utilisées pour entraîner des algorithmes de recrutement ou d'évaluation, les données comportementales collectées par des outils de suivi (mouvement de souris, temps d'activité, géolocalisation), les données issues des communications professionnelles analysées par des systèmes d'IA, et tout résultat produit par un algorithme concernant une personne identifiable.

La CNIL face à l'IA : un régulateur en première ligne

La CNIL joue un rôle central dans l'articulation entre RGPD et IA. Depuis le lancement de son plan d'action sur l'IA en mai 2023, elle a publié un corpus de plus de treize fiches pratiques (entre 2024 et juillet 2025) détaillant l'application du RGPD au développement et au déploiement des systèmes d'IA. Elle a également défini les conditions dans lesquelles un modèle d'IA peut être considéré comme anonyme — et donc soustrait au RGPD — ou doit au contraire être traité comme relevant de ce règlement.

CNIL / JURISPRUDENCE — CNIL, recommandations IA
Fiches pratiques, juillet 2025

La CNIL a confirmé que les modèles d'IA entraînés sur des données personnelles doivent, dans la plupart des cas, être considérés comme relevant du RGPD. La complexité des systèmes d'IA ne doit pas empêcher la bonne compréhension des droits par les personnes concernées. La CNIL recommande aux responsables de traitement de documenter la manière dont les données sont utilisées lors de l'apprentissage, le fonctionnement du système d'IA et la distinction entre la base de données d'apprentissage, le modèle et ses sorties.

Au-delà de ses travaux normatifs, la CNIL exerce un contrôle actif dans le monde du travail. La surveillance des salariés et la gestion des données RH constituent le troisième motif de plainte reçu par la CNIL (13 % des 17 772 plaintes reçues en 2024), et les sanctions liées à la surveillance des salariés représentaient la majorité des sanctions simplifiées prononcées en 2025. Ces données reflètent une réalité de terrain : le déploiement de technologies de suivi et d'évaluation des salariés génère des atteintes systémiques aux droits des personnes, souvent non identifiées comme telles par les organisations qui les commettent.

CNIL / JURISPRUDENCE — CNIL, Bilan des sanctions 2025
Rapport annuel 2024

Cookies, surveillance des salariés et sécurité des données constituent les principaux motifs des 83 sanctions prononcées en 2025, pour un montant cumulé de 486 839 500 euros. Six des dix sanctions simplifiées de début 2025 concernaient la surveillance des salariés. Le manquement au principe de minimisation est majoritairement en cause : surveillance vidéo permanente, captures d'écran systématiques, géolocalisation continue. Le rapport annuel 2024 de la CNIL précise que l'essor des usages de l'IA en entreprise devrait entraîner une sollicitation croissante de la CNIL sur ces questions.

Le cas emblématique de la surveillance algorithmique

CNIL / JURISPRUDENCE — CNIL, Délibération SAN-2024-021,
19 décembre 2024
Surveillance disproportionnée de salariés (40 000 €)

Une agence immobilière avait installé sur les ordinateurs de ses salariés en télétravail un logiciel paramétré pour comptabiliser des périodes d'inactivité supposée via les mouvements de souris et l'activité clavier, réaliser des captures d'écran régulières, et filmer les salariés en permanence par vidéosurveillance. La CNIL a retenu plusieurs manquements : violation du principe de minimisation des données (art. 5 §1 c RGPD), absence de base légale valide pour le traitement (art. 6 RGPD), défaut d'information des salariés (art. 13 RGPD). Ce dispositif, qui peut conduire à la captation de courriels personnels, conversations instantanées et mots de passe, a été qualifié de surveillance particulièrement intrusive et disproportionnée.

Cette décision est emblématique à plusieurs titres. Elle confirme que les outils de « *people analytics* » et de suivi de productivité basés sur l'IA sont directement dans le viseur de la CNIL, qui les examine sous l'angle du RGPD indépendamment de toute qualification au titre du RIA. Elle établit qu'une surveillance continue des postes

de travail ne repose sur aucune base légale valide, que les salariés doivent être informés individuellement de tout traitement les concernant, et que l'employeur est tenu de démontrer la proportionnalité de son dispositif.

POINT DE VIGILANCE // Un employeur qui déploie un outil de suivi de l'activité des salariés — même présenté comme un outil de gestion de la productivité — engage sa responsabilité au titre du RGPD. Les représentants du personnel peuvent signaler tout dispositif suspect à la CNIL et demander qu'un contrôle soit diligenté.

Les sept principes fondamentaux du RGPD : ce qu'ils imposent concrètement face à l'IA

L'article 5 du RGPD pose les principes fondamentaux applicables à tout traitement de données personnelles. Ces principes constituent autant de garanties opposables à l'employeur qui déploie un système d'IA traitant des données de salariés ou de candidats. Le tableau suivant les traduit en questions pratiques pour les élus du personnel et les délégués syndicaux.

Principe RGPD	Article	Application aux systèmes d'IA dans le travail	Questions pour le CSE/DS
Licéité, loyauté, transparence	Art. 5 §1 a)	L'employeur doit avoir une base légale valide pour chaque traitement de données opéré par le système d'IA. Les salariés doivent être informés loyalement de l'existence et des finalités du système.	Sur quelle base légale le traitement repose-t-il ? Les salariés ont-ils été informés ? L'information est-elle réellement intelligible ?
Limitation des finalités	Art. 5 §1 b)	Les données collectées par le système d'IA ne peuvent être réutilisées à d'autres fins que celles pour lesquelles elles ont été collectées. Un outil de suivi de la performance ne peut alimenter une procédure disciplinaire sans base légale spécifique.	Les données collectées sont-elles utilisées à d'autres fins que celles déclarées ? Le registre des traitements reflète-t-il la réalité des usages ?

Principe RGPD	Article	Application aux systèmes d'IA dans le travail	Questions pour le CSE/DS
Minimisation des données	Art. 5 §1 c)	Le système d'IA ne doit traiter que les données strictement nécessaires à sa finalité. La CNIL a sanctionné en 2024-2025 plusieurs employeurs pour violation de ce principe (surveillance vidéo continue, captures d'écran systématiques, géolocalisation excessive).	Le système collecte-t-il plus de données que nécessaire ? Le principe de minimisation a-t-il été respecté lors de la conception ?
Exactitude	Art. 5 §1 d)	Les données utilisées comme entrées du système d'IA doivent être exactes et tenues à jour. Des données inexactes ou obsolètes peuvent produire des décisions biaisées ou injustes, avec un impact direct sur les salariés.	Comment les données d'entrée sont-elles vérifiées ? Quelle procédure existe pour corriger des données inexactes utilisées par le système ?
Limitation de la conservation	Art. 5 §1 e)	Les données personnelles traitées par le système d'IA ne peuvent être conservées au-delà de la durée nécessaire. Les journaux (logs) doivent eux aussi respecter des durées de conservation définies.	Quelle est la durée de conservation des données traitées par le système ? Celle des journaux automatiques ? Des procédures d'archivage ou de suppression sont-elles définies ?
Intégrité et confidentialité	Art. 5 §1 f)	Le système d'IA doit être sécurisé contre les accès non autorisés, les violations de données et les risques de réidentification. L'employeur doit avoir mis en place des mesures techniques et organisationnelles appropriées.	Quelles mesures de sécurité protègent les données traitées par le système ? Des tests de sécurité ont-ils été réalisés ? Qui a accès aux résultats et aux logs ?
Responsabilité (*Accountability*)	Art. 5 §2	L'employeur est responsable du respect de tous ces principes et doit être en mesure de le démontrer. Il doit tenir un registre des traitements incluant le système d'IA.	L'employeur peut-il produire le registre des traitements incluant ce système ? A-t-il réalisé une AIPD si le traitement présente un risque élevé ?

POINT DE VIGILANCE // Le principe d'*accountability* (art. 5 §2) est particulièrement stratégique : l'employeur doit pouvoir prouver sa conformité à tout moment. Il n'est pas seulement tenu de respecter ces principes — il doit être capable de le démontrer, par des documents, des procédures et des analyses d'impact. C'est cette obligation documentaire qui donne son contenu concret au droit d'exiger des preuves.

Les bases légales : ce qui autorise l'employeur à traiter les données personnelles

Tout traitement de données personnelles exige une base légale valide (art. 6 RGPD). Dans le contexte de l'emploi, six bases légales sont prévues par le règlement, mais seules certaines sont applicables aux traitements liés à l'IA en entreprise. Comprendre les bases légales permet aux représentants du personnel d'exiger que l'employeur justifie chaque traitement et de contester les traitements dont la base légale est fragile ou inexistante.

Les bases légales dans le contexte du travail

Bases légales applicables aux traitements IA dans l'entreprise
Exécution du contrat de travail (art. 6 §1 b) : justifie les traitements strictement nécessaires à l'exécution du contrat (pointage, gestion des congés, accès aux outils numériques). Ne peut pas justifier une surveillance généralisée ou un profilage comportemental.
Obligation légale (art. 6 §1 c) : justifie les traitements imposés par la loi (déclarations sociales, registre du personnel, prévention des accidents). Utilisable pour certains traitements de sécurité au travail.
Intérêt légitime (art. 6 §1 f) : base la plus souvent invoquée pour les systèmes d'IA (optimisation des processus, sécurité informatique, détection de fraude). Impose une mise en balance avec les droits des salariés et la réalisation d'un test en trois étapes. Un salarié peut s'y opposer (droit d'opposition de l'art. 21).
Consentement (art. 6 §1 a) : rarement applicable dans le contexte du travail. La CNIL et la jurisprudence soulignent que le consentement d'un salarié n'est généralement pas libre en raison du lien de subordination. Invoqué abusivement, il peut être contesté.

Bases légales applicables aux traitements IA dans l'entreprise

Point d'attention pour les données sensibles (art. 9 RGPD) : la race, l'origine ethnique, les opinions politiques, l'appartenance syndicale, les données de santé, la vie sexuelle ou l'orientation sexuelle bénéficient d'une protection renforcée. Leur traitement est en principe interdit, sauf exceptions strictement énumérées. Un système d'IA qui infère ces caractéristiques à partir d'autres données viole l'article 9 du RGPD — et relève également des pratiques interdites par le RIA (art. 5 §1 g).

Le cas particulier du recrutement

Dans le cadre du recrutement, le RGPD se combine avec le Code du travail pour encadrer strictement l'usage des outils d'IA. L'employeur ne peut collecter que les données strictement nécessaires à l'appréciation de la candidature (principe de minimisation). Les données sensibles — notamment la nationalité, la situation de famille, ou les informations permettant d'inférer l'origine — ne peuvent être collectées. Le traitement doit être fondé sur une base légale valide et le candidat doit être informé de l'existence d'un traitement automatisé et de son droit à une intervention humaine.

BASE LÉGALE — Art. L.1221-8 + Art. L.1221-9 Code du travail + Art. 6 RGPD

Le candidat à un emploi est expressément informé, préalablement à leur mise en œuvre, des méthodes et techniques d'aide au recrutement utilisées à son égard. Les résultats obtenus sont confidentiels.
Les informations demandées au candidat doivent avoir un lien direct et nécessaire avec l'emploi proposé.

CNIL / JURISPRUDENCE — CNIL, Rapport 2024
Recrutement et collecte excessive de données

En mai 2024, la CNIL a été saisie d'une plainte à l'encontre d'une société collectant un volume important de données personnelles auprès des candidats à un poste : lieu de naissance, nationalité, situation familiale. Cette pratique a été jugée contraire au principe de minimisation. La CNIL rappelle que la collecte doit rester proportionnée à la finalité du recrutement et ne peut pas inclure des données permettant une discrimination indirecte.

L'article 22 RGPD : le droit fondamental face aux décisions algorithmiques

L'article 22 du RGPD constitue l'une des protections les plus importantes accordées par le droit européen aux personnes soumises à des décisions algorithmiques. Il est au cœur des enjeux posés par l'IA dans le monde du travail et mérite une attention particulière de la part des représentants du personnel.

BASE LÉGALE — Art. 22 §1 RGPD
Décision individuelle automatisée et profilage
La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

Qu'est-ce qu'une décision entièrement automatisée ?

Une décision est « entièrement automatisée » lorsqu'elle a été prise par un algorithme, sans aucune intervention humaine réelle. Le Comité européen de la protection des données (CEPD) a précisé que l'intervention humaine doit être réelle et effective : un opérateur qui valide systématiquement les décisions algorithmiques sans analyse indépendante ne constitue pas une intervention humaine au sens de l'article 22. L'intervenant doit avoir l'autorité et la compétence pour modifier la décision, et doit disposer de toutes les informations nécessaires.

Dans le monde du travail, les décisions visées par l'article 22 peuvent inclure : le rejet automatique d'une candidature par un algorithme de présélection, la réduction automatique d'objectifs ou de primes sur la base d'un score de performance, une décision d'affectation ou de mutation produite exclusivement par un système de planification algorithmique, ou encore une décision disciplinaire fondée sur des alertes automatiques issues d'un outil de surveillance de l'activité.

Les effets juridiques ou significatifs

L'article 22 s'applique dès lors que la décision produit des effets juridiques ou affecte significativement la personne. La CNIL et le CEPD ont clarifié ces notions. Un effet juridique est toute décision qui impacte les droits légaux de la personne (accès à

l'emploi, modification du contrat, sanction, rupture). Un effet significatif inclut toute décision qui désavantage financièrement la personne, la ferme à des opportunités professionnelles, ou influence de manière importante ses conditions de travail.

CNIL / JURISPRUDENCE — CJUE, arrêt du 27 février 2025, C-203/22 Droit à l'explication

La Cour de justice de l'Union européenne a statué qu'une personne soumise à une décision automatisée peut exiger une explication de la procédure et des principes concrètement appliqués pour exploiter ses données personnelles. La seule communication d'un algorithme ou de formules mathématiques n'est pas une explication intelligible au sens de l'article 15 §1 h) RGPD. Si le responsable de traitement considère que les informations à fournir relèvent du secret des affaires, il doit les communiquer à l'autorité de contrôle ou à la juridiction compétente — non les refuser à la personne concernée

Les trois exceptions et leurs limites

L'article 22 pose une interdiction de principe, assortie de trois exceptions strictement encadrées. Ces exceptions ne dispensent pas l'employeur de mettre en place des garanties appropriées : information de la personne, droit à l'intervention humaine, droit d'exprimer son point de vue et de contester la décision.

Les trois exceptions à l'interdiction des décisions automatisées (art. 22 §2)

Exception 1 : nécessité contractuelle - la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne et le responsable. Dans le contexte du travail, cette exception est d'interprétation stricte.
Exception 2 : autorisation légale - un texte de l'UE ou national autorise explicitement la décision automatisée. Elle doit comprendre des mesures de protection des droits de la personne.
Exception 3 : consentement explicite - la personne a donné son consentement explicite. Dans le contexte du travail, cette exception est très fragile : le CEPD rappelle que le consentement d'un salarié n'est généralement pas libre en raison du lien de subordination.

Dans tous les cas, la personne a le droit : d'obtenir une intervention humaine réelle (pas formelle), d'exprimer son point de vue, et de contester la décision — même lorsqu'une exception s'applique.

POINT DE VIGILANCE // Le fait qu'un manager valide formellement une décision produite par un algorithme ne suffit pas à satisfaire l'exigence d'intervention humaine de l'article 22. La validation doit être réelle et fondée sur une analyse indépendante. Exiger de l'employeur qu'il démontre concrètement en quoi l'intervention humaine est réelle et non purement formelle est un droit syndical.

L'AIPD (Analyse d'Impact relative à la Protection des Données)

L'AIPD est obligatoire pour les traitements présentant un risque élevé pour les droits des personnes. La CNIL a établi une liste des types de traitements qui nécessitent systématiquement une AIPD — cette liste comprend notamment le profilage à grande échelle et l'évaluation systématique d'aspects personnels par traitement automatisé.
Tout système d'IA utilisé pour évaluer les performances des salariés, classer des candidats ou analyser des comportements professionnels entre dans cette catégorie.

BASE LÉGALE — Art. 35 RGPD — Analyse d'impact relative à la protection des données (AIPD / DPIA)
Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

L'AIPD doit être réalisée avant le déploiement et comprend : une description systématique des traitements envisagés et de leurs finalités, une évaluation de la nécessité et de la proportionnalité du traitement, une évaluation des risques pour les droits des personnes, et les mesures envisagées pour y remédier.

Articulation aipd (rgpd art. 35) et fria (ria art. 27)

AIPD (RGPD) : obligatoire pour tout traitement d'IA à risque élevé traitant des données personnelles. S'applique à toutes les entreprises. Porte sur les risques pour la vie privée et la protection des données.
FRIA (RIA) : obligatoire avant le déploiement de systèmes d'IA à haut risque uniquement pour les organismes publics, les opérateurs de services essentiels et certains établissements d'enseignement. Porte sur l'ensemble des droits fondamentaux, au-delà de la seule protection des données.
Articulation : la CNIL confirme que l'AIPD et la FRIA sont deux analyses complémentaires. Le déployeur peut s'appuyer sur l'AIPD déjà réalisée pour nourrir son analyse d'impact au titre du RIA (art. 26 §9 RIA). Pour les entreprises privées ordinaires, l'AIPD est obligatoire (RGPD) ; la FRIA formelle est optionnelle mais recommandée.

POINT DE VIGILANCE // Exiger de l'employeur qu'il produise l'AIPD réalisée avant le déploiement d'un système d'IA est un droit. Cette analyse doit être préalable, documentée et mise à jour dès que le traitement évolue. En l'absence d'AIPD pour un traitement à risque élevé, l'employeur commet une infraction au RGPD susceptible d'être signalée à la CNIL.

Les droits individuels des salariés : un arsenal à mobiliser

Le RGPD accorde à chaque personne physique un ensemble de droits directement opposables à l'employeur qui traite ses données personnelles via un système d'IA. Ces droits sont individuels — ils appartiennent à chaque salarié ou candidat — mais les représentants du personnel jouent un rôle essentiel dans leur mise en œuvre collective : information des salariés, accompagnement dans l'exercice de leurs droits, négociation de garanties renforcées.

Droit RGPD	Article	Application aux systèmes d'IA dans le travail	Comment l'exercer ?
Droit d'accès	Art. 5 §1 c)	Tout salarié ou candidat peut demander quelles données personnelles sont traitées à son sujet par un système d'IA, à quelles fins, et les résultats produits par ce système à son égard.	Demande écrite à l'employeur (ou au DPO). Réponse dans le délai légal d'un mois (prorogeable à 2 mois). Le refus ou l'absence de réponse peut être signalé à la CNIL.
Droit de rectification	Art. 16	Le salarié peut exiger la correction de données inexactes qui alimentent le système d'IA et qui ont pu conduire à une décision erronée le concernant.	Demande écrite avec justificatif. L'employeur est tenu de rectifier dans un délai raisonnable.
Droit d'opposition	Art. 21	Le salarié peut s'opposer au traitement de ses données personnelles par un système d'IA dès lors que ce traitement est fondé sur l'intérêt légitime. L'opposition est de droit sauf motifs légitimes impérieux de l'employeur.	Demande écrite motivée. L'employeur doit soit cesser le traitement, soit démontrer ses motifs légitimes impérieux.
Droit à l'explication des décisions automatisées	Art. 22 + Art. 15 §1 h)	Toute personne soumise à une décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques ou significatifs a le droit d'obtenir une explication intelligible de la logique utilisée. La CJUE (27 fév. 2025, C-203/22) a précisé que la communication du seul algorithme ou de formules mathématiques ne constitue pas une explication intelligible.	Demande écrite au responsable de traitement ou au DPO. En cas d'absence de réponse satisfaisante, saisine de la CNIL ou recours judiciaire.
Droit d'intervention humaine	Art. 22	Toute personne a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques ou l'affectant de manière significative. Elle a le droit d'obtenir une intervention humaine réelle et effective.	Demande écrite à l'employeur. L'intervention humaine doit être réelle et non formelle : le CEPD a précisé qu'un humain qui valide systématiquement sans analyse n'est pas une « intervention humaine » au sens du RGPD.
Droit à la limitation du traitement	Art. 18	Permet de suspendre le traitement pendant une contestation sur l'exactitude des données ou la licéité du traitement.	Demande écrite à l'employeur, qui doit suspendre l'utilisation des données contestées jusqu'à résolution.
Droit à la portabilité	Art. 20	Dans certains cas, le salarié peut demander à recevoir ses données personnelles dans un format structuré et lisible par machine. S'applique aux traitements fondés sur le consentement ou le contrat.	Demande écrite au responsable de traitement ou DPO.

Le rôle du Délégué à la Protection des Données (DPO) : un interlocuteur stratégique

Le Délégué à la Protection des Données (DPO) est obligatoire dans les entreprises qui traitent des données à grande échelle, ou dont le traitement des données constitue l'activité principale (art. 37 RGPD).
Dans les entreprises qui disposent d'un DPO, les représentants du personnel ont tout intérêt à nouer avec lui une relation de travail active, car il est un interlocuteur privilégié sur les questions liées à l'IA et aux données.

Ce que les élus peuvent obtenir via le DPO

- Accéder au registre des traitements de l'entreprise (art. 30 RGPD), qui doit lister tous les traitements de données, y compris ceux opérés par des systèmes d'IA.
- Demander que l'AIPD réalisée pour un projet d'IA soit partagée avec le CSE, au moins dans ses grandes lignes.
- Signaler au DPO tout traitement qui semble disproportionné, non déclaré ou non conforme au RGPD.
- Demander que le DPO soit associé aux travaux du CSE sur les projets d'IA, notamment lors de la consultation obligatoire.
- Interroger le DPO sur la conformité d'un système d'IA déjà déployé et dont l'impact sur les salariés n'a pas été évalué.

Les sanctions : une autorité de contrôle active et des montants significatifs

Le RGPD est assorti d'un régime de sanctions administratives parmi les plus dissuasifs du droit européen. La CNIL dispose d'un pouvoir de contrôle (sur plainte ou d'office) et de sanction. En 2025, elle a prononcé 83 sanctions pour un montant total de 486 millions d'euros — un record. Cette activité de contrôle s'intensifie précisément dans le domaine qui nous occupe : surveillance des salariés et traitement des données RH.

Tableau des sanctions rgpd (art. 83)		
Type de manquement	**Amende max.**	**Articles RGPD**
Violations graves des principes fondamentaux et des droits des personnes (y compris art. 5, 6, 9, 22, 35)	**20 M€ ou 4 % du CA mondial**	Art. 83 §5
Violations des obligations du responsable et du sous-traitant (y compris art. 13, 14, 25, 30, 32)	**10 M€ ou 2 % du CA mondial**	Art. 83 §4
Surveillance disproportionnée des salariés (violation art. 5 §1 c — minimisation)	**Sanctions simplifiées : jusqu'à 20 000 € — Formation restreinte : jusqu'à 20 M€**	Pratique CNIL 2024-2025
Absence d'AIPD pour un traitement à risque élevé	**10 M€ ou 2 % du CA mondial**	Art. 83 §4 + art. 35

*À ces sanctions administratives s'ajoutent les **sanctions pénales du Code du travail** (délit d'entrave : 7 500 € à 37 500 €) et les **recours civils** ouverts à chaque salarié lésé par une décision illicite.*

La CNIL peut être saisie directement

Tout salarié, candidat ou représentant du personnel peut adresser une plainte à la CNIL lorsqu'il rencontre une difficulté dans l'exercice de ses droits ou pour signaler une atteinte aux règles de protection des données.

La démarche est préalablement d'essayer de faire valoir ses droits auprès du responsable de traitement (le Conseil d'État a confirmé cette condition préalable en janvier 2025). Ce n'est qu'en cas d'échec ou d'absence de réponse que la saisine de la CNIL devient possible.

Comment saisir la CNIL

- Via le formulaire en ligne sur le site cnil.fr (rubrique « Plaintes »)
- Par courrier postal à la CNIL : 3 Place de Fontenoy, 75007 Paris
- La CNIL peut déclencher un contrôle sur pièces ou sur place, y compris à la suite d'une plainte syndicale
- En cas de violation grave et urgente, la CNIL peut ordonner des mesures provisoires immédiates
- La CNIL peut également être saisie collectivement par des organisations syndicales pour des manquements systémiques

RGPD et IA générative : les risques spécifiques dans l'entreprise

Le développement rapide des outils d'IA générative dans les entreprises (assistants de rédaction, *chatbots* internes, outils de synthèse, génération de code) soulève des risques spécifiques au regard du RGPD, qui s'ajoutent aux enjeux déjà identifiés pour les autres types de systèmes d'IA.

Le risque de divulgation de données personnelles

Lorsqu'un salarié utilise un outil d'IA générative externe (comme ChatGPT, Claude ou Gemini) pour traiter des documents internes, il peut introduire dans le système des données personnelles de clients, de collègues ou de candidats. Ces données peuvent potentiellement être mémorisées par le modèle et restituées lors d'interactions ultérieures avec d'autres utilisateurs — ou utilisées pour entraîner de futures versions du modèle.

CNIL / JURISPRUDENCE — CNIL,
Recommandations sur l'IA générative dans les organisations (2024 - 2025)

La CNIL a publié des recommandations spécifiques sur l'utilisation des outils d'IA générative dans les environnements professionnels. Elle alerte sur les risques liés à l'introduction de données personnelles dans des systèmes hébergés à l'extérieur, sur la nécessité de vérifier les conditions d'utilisation des outils (notamment si les données soumises sont utilisées

pour l'entraînement), et sur l'obligation pour l'employeur de définir une politique d'usage claire. La CNIL rappelle également que l'usage d'un outil d'IA générative peut constituer un traitement de données personnelles au sens du RGPD, qui doit être déclaré dans le registre des traitements.

L'obligation de politique d'usage négociée

L'absence de politique d'usage claire crée une situation de risque partagé entre l'employeur et les salariés. L'employeur qui tolère implicitement l'usage d'outils d'IA générative sans définir de cadre engage sa responsabilité au titre du RGPD si des données personnelles sont exposées. Les salariés, de leur côté, peuvent être exposés à des sanctions disciplinaires si leur usage non encadré conduit à une fuite de données.

POINT DE VIGILANCE // La politique d'usage de l'IA générative doit être un sujet de négociation collective, non une décision unilatérale de la direction informatique. Les représentants du personnel doivent exiger d'être associés à la définition de cette politique, qui engage directement la protection des données personnelles des salariés et des tiers.

Checklist RGPD pour les représentants du personnel face à un projet d'IA

Le tableau suivant récapitule les vérifications essentielles à réaliser au regard du RGPD avant et pendant le déploiement d'un système d'IA dans l'entreprise. Ces vérifications peuvent être conduites dans le cadre de la consultation CSE, en demandant à l'employeur de justifier chaque point par un document.

Checklist RGPD — Ce que le CSE peut demander à l'employeur

Sur la licéité du traitement :

- **Base légale :** quelle est la base légale retenue pour chaque traitement opéré par le système d'IA ? Elle est documentée dans le registre des traitements ?
- **Données sensibles :** le système traite-t-il ou infère-t-il des données relevant de l'article 9 RGPD (santé, appartenance syndicale, opinions politiques, origine, etc.) ? Si oui, quelle exception de l'article 9 §2 est invoquée ?
- **Décision automatisée :** le système produit-il des décisions affectant significativement des personnes ? Si oui, comment l'art. 22 RGPD est-il respecté ?

Checklist RGPD — Ce que le CSE peut demander à l'employeur

- **Minimisation :** quelles données sont collectées ? Sont-elles toutes nécessaires à la finalité déclarée ? Comment la proportionnalité est-elle justifiée ?
- **Données sensibles :** pour quelles finalités le système traite-t-il les données ? Ces finalités sont-elles documentées ? Les données sont-elles utilisées à d'autres fins que celles déclarées ?
- **Conservation :** quelle est la durée de conservation des données ? Des procédures d'effacement ou d'anonymisation ont-elles été mises en place ?

Sur l'information et les droits :

- **Information des salariés :** les salariés ont-ils été informés individuellement de l'existence du traitement, de ses finalités, de leurs droits ? Cette information est-elle accessible et intelligible ?
- **Droits des personnes :** quelle procédure existe pour exercer les droits d'accès, de rectification, d'opposition, d'explication et d'intervention humaine ? Les délais légaux sont-ils respectés ?
- **DPO :** un délégué à la protection des données a-t-il été désigné ? Est-il associé au projet ?

Sur l'analyse d'impact et la documentation :

- **AIPD :** une Analyse d'Impact relative à la Protection des Données a-t-elle été réalisée avant le déploiement ? Pour quels traitements ? Peut-elle être communiquée au CSE ?
- **Registre des traitements :** ce système figure-t-il dans le registre des traitements de l'entreprise (art. 30 RGPD) ? Le registre est-il accessible au DPO et à la CNIL ?
- **Sous-traitants :** les prestataires et éditeurs qui traitent des données personnelles pour le compte de l'entreprise ont-ils signé un contrat de sous-traitance conforme à l'art. 28 RGPD ? Ce contrat interdit-il la réutilisation des données à d'autres fins ?

Synthèse RGPD, une ressource à actionner dès aujourd'hui

Contrairement au RIA dont les obligations les plus importantes (haut risque) n'entrent en vigueur qu'en août 2026, le RGPD est pleinement applicable et ses droits sont exerçables dès maintenant. C'est l'un de ses avantages stratégiques majeurs pour les représentants du personnel.

CE QUE LE RGPD PERMET D'OBTENIR IMMÉDIATEMENT

- **Accès au registre des traitements** de l'entreprise pour identifier tous les systèmes d'IA qui traitent des données personnelles.
- **Exiger la preuve de l'AIPD** réalisée avant le déploiement de tout système à risque élevé.
- **Obtenir l'information des salariés** sur l'existence et les finalités de tout traitement les concernant.
- **Contester toute décision automatisée** affectant significativement un salarié sans intervention humaine réelle.
- **Demander une explication intelligible** de la logique d'un algorithme ayant produit une décision défavorable.
- **Signaler à la CNIL** tout dispositif de surveillance disproportionné ou tout traitement non conforme.
- **Négocier une politique d'usage de l'IA générative** en s'appuyant sur l'obligation de l'employeur de définir un cadre conforme au RGPD.

Ce que le RGPD ne fait pas : il n'impose pas de consultation du CSE par lui-même (c'est le Code du travail qui le fait). Il ne prévoit pas de contrôle humain sur les décisions algorithmiques au même niveau de précision que le RIA. Il ne classe pas les systèmes par niveau de risque. C'est précisément pourquoi les trois leviers — Code du travail, RIA et RGPD — doivent être mobilisés ensemble.

À RETENIR.
Le triple levier en action

Code du travail, RIA et RGPD constituent trois éclairages complémentaires sur la même réalité : l'introduction d'un système d'IA dans une organisation est un acte de gouvernance, pas un simple choix technique. Chacun de ces textes confère des droits et impose des obligations qui se renforcent mutuellement.

- **Le Code du travail :** donne le droit à la consultation préalable, à l'expertise, et à la suspension judiciaire. C'est le levier collectif immédiat.
- **Le RIA :** impose la documentation, le contrôle humain et la traçabilité pour les systèmes à haut risque. C'est le levier de la preuve et de la qualification.
- **Le RGPD :** garantit les droits individuels face aux algorithmes, l'obligation de l'AIPD, et la protection contre la surveillance disproportionnée. C'est le levier de la dignité et de la vie privée.

La question centrale reste inchangée : cet outil influence-t-il l'organisation du travail ou des décisions concernant des personnes ? Si oui, les trois textes s'activent, et les représentants du personnel ont des droits concrets, documentés et sanctionnés pour l'encadrer.

PARTIE #5

Annexes

5 Annexes

ANNEXE N° 01.
10 principes pour une IA éthique

Les observations soulignent le risque qui tient à la confiance excessive dans les décisions prises par les « machines » jugées comme infaillibles et plus « objectives » que l'humain au risque que ce dernier finisse par se déresponsabiliser. Pour faire face à ces risques, FO-Cadres a dégagé 10 principes majeurs permettant de déboucher sur 20 propositions opérationnelles.

À la lecture de ces derniers, nous retrouvons d'une part en toile de fond la logique de responsabilisation des entreprises prévue par le Règlement général sur la protection des données (RGPD) et, plus concrètement, l'obligation de mettre en œuvre toutes les mesures appropriées pour garantir ab initio une protection optimale des données et une minimisation de leur collecte, tout en assurant que cette protection perdure. Un engagement nécessaire pour lutter contre l'effet « boîtes noires » des IA et rendre les systèmes algorithmiques compréhensibles pour plus de transparence.

D'autre part, ces principes préconisent une approche réglementaire qui ne se limite pas à l'encadrement juridique de la collecte de données, mais mettent en doute également la conception des IA, la légitimité et la transparence des processus algorithmiques eux-mêmes. Cette approche souligne l'importance de la capacité critique des travailleurs, des IRP et des organisations syndicales à comprendre, questionner et contester les logiques sous-jacentes aux systèmes automatisés qui influencent au-delà de la vie sociale et politique, de plus en plus le monde de l'entreprise et des administrations publiques. Dans le sillage du progrès technologique, l'élaboration de systèmes algorithmiques exige l'adhésion à des principes fondamentaux pour établir un cadre permettant un équilibre entre innovation et intégrité humaine. Ces principes ne sont pas

seulement des guides pour l'action, mais aussi des gardiens de notre intégrité sociale et voire même une meilleure efficacité de l'IA.

Cela signifierait que toute régulation devrait tenir compte de la nature et de l'évolution des technologies elles-mêmes, de leur rôle dans la société et de leur interaction avec l'humain. Plutôt que d'imposer des règles strictes, il convient de préconiser un cadre favorisant une co-évolution harmonieuse entre la technologie et l'humain, en permettant une adaptation continue de la technologie aux besoins sociaux et vice versa des travailleurs.

La technologie n'est pas un destin inévitable ; c'est l'humain qui doit diriger cette transition.

1 — La finalité

Tout déploiement de l'IA doit servir un objectif clair, répondant aux besoins réels de la société, en veillant à améliorer la condition humaine sans compromettre nos valeurs démocratiques. Avant tout déploiement d'un SIA, il est fondamental d'établir une finalité explicite respectueuse des droits des salariés. Que l'IA soit utilisée pour l'analyse de performances, le recrutement ou même la détection de fraudes, elle doit toujours respecter l'intégrité des individus. Aucune donnée ne doit être collectée sans une justification solide et en garantissant toujours la confidentialité des informations personnelles.

Les algorithmes d'apprentissage automatique, particulièrement pertinents pour les services RH, ne doivent pas y déroger bien qu'ils génèrent leurs propres règles à partir de jeux de données. Cette caractéristique peut paraître en contradiction avec le principe de finalité, notamment lorsque l'innovation est vue comme une priorité absolue. Toutefois, même si le « *machine learning* » vise à découvrir des corrélations insoupçonnées, son utilisation doit s'ancrer dans un objectif défini, et légitime même si celui-ci est formulé de manière générale.

2 — La proportionnalité

La proportionnalité en droit s'assure que toute mesure prise, spécifiquement dans le domaine du numérique, est adéquate, pertinente, et limitée à ce qui

est nécessaire. Cela implique une évaluation constante des bénéfices et des inconvénients potentiels de chaque décision, notamment lorsqu'il s'agit en matière RH pour les entreprises d'une certaine taille d'alimenter l'IA avec les données de l'entreprise.

Alors que le principe de minimisation se réfère spécifiquement à la collecte, au stockage et à l'utilisation de données, en insistant sur le fait que seules celles qui sont strictement nécessaires à un objectif précis doivent être traitées, le principe de proportionnalité est plus large. Il englobe l'équilibre entre les moyens utilisés et les fins poursuivies. Le principe de proportionnalité demeure crucial pour garantir un équilibre entre les impératifs technologiques et réglementaires ainsi que la protection des droits individuels et l'essor d'une innovation responsable.

3 — La loyauté

La fidélité aux engagements pris, la loyauté envers les utilisateurs, doivent imprégner l'IA, dans le cadre d'une conception qui respecte équitablement tous les acteurs concernés, sans tromperie ni partialité. Le principe de loyauté incarne l'essence même d'une éthique technologique dans le contexte de l'IA. Il met l'accent sur les obligations des concepteurs d'algorithmes plutôt que sur les droits des utilisateurs.

Ayant ses racines dans la loi Informatique et Libertés de 1978, ce principe exige que l'algorithme soit transparent, préalable nécessaire à l'exercice des droits des personnes (droit d'accès), en leur fournissant sur son fonctionnement, exemptes de biais cachés ou d'agendas opaques. Il restreint également la manière dont celui-ci est conçu et utilisé.

L'adoption du principe de loyauté signifie aussi que les entreprises s'engagent à protéger les données des travailleurs, non seulement en termes de sécurité, mais aussi en garantissant qu'elles sont utilisées de manière cohérente au regard des finalités définies. La clé de la mise en œuvre réussie de ce principe de loyauté réside dans la combinaison d'une conception éthique, d'une communication transparente et d'une volonté constante d'ajuster les systèmes en fonction des retours et des évolutions.

4 — La vigilance

Le développement des SIA et de l'apprentissage automatique suscite une imprévisibilité croissante quant à leurs impacts. Leur nature mouvante, renforcée par l'étendue de leur champ d'application rend complexe leur encadrement. Face à ces défis, le principe de vigilance émerge comme une réponse méthodologique. Il vise à prévenir les risques et à anticiper les effets inattendus des algorithmes.

Elle entend aussi remédier à la confiance excessive envers l'IA, souvent perçue comme infaillible, et à la déresponsabilisation due à son opacité. Plus que de simples outils, l'IA est insérée dans de vastes chaînes algorithmiques impliquant de nombreux acteurs, du développeur à l'utilisateur final. Cette multiplicité peut engendrer une dilution de la responsabilité.

La vigilance, en tant que devoir collectif, cherche donc à garantir une éthique et une responsabilité tout au long de cette chaîne, garantissant que cette technologie soit développée et déployée avec précaution, en tenant compte de l'intérêt général et des droits des individus et de l'évaluation des études d'impact.

5 — La transparence

Une clarté absolue dans les processus algorithmiques est essentielle pour obtenir et conserver la confiance du public ainsi que pour assurer la compréhension des décisions prises par ou avec l'aide de l'IA. Un SIA auquel une personne recourt ou est soumise doit être transparent c'est-à-dire que l'individu doit être en état de comprendre ses mécanismes fondamentaux, les motivations des concepteurs et celles des utilisateurs. Et, le cas échéant avoir le droit et les moyens concrets de les contester.

Si des détails techniques peuvent rester confidentiels, notamment pour des raisons de propriété intellectuelle, les critères utilisés, les données collectées et traitées par l'IA doivent être accessibles et explicites. Lorsqu'un algorithme est utilisé pour le recrutement ou l'évaluation des performances, les employés doivent connaître la nature des données qui sont collectée, à quelle fin et comment elles affectent les décisions. Cette transparence est essentielle pour garantir l'équilibre entre innovation et protection.

6 — La justice

Le recours à un cadre réglementaire fort est nécessaire pour poser des « lignes rouges » et bloquer le cas échéant, des SIA qui iraient à l'encontre du principe démocratique, de la justice sociale ou environnementale. La loi informatique et libertés et l'entrée en application du RGPD en 2018 participent pleinement à cet objectif. Or le seul consentement ne saurait faire reposer le choix d'une technologie sur l'individu d'autant qu'il sera inopérant dans de nombreux cas, par exemple dans le cadre d'un lien de subordination au travail. Si le recours à l'IA dans le domaine RH ou par les administrations publiques peut poursuivre des finalités légitimes, il ne doit pas conduire à automatiser des missions, des ressources, des jugements et à réduire la dépense. Dans les chartes et outils de régulation, le sens de ces activités est souvent évincé au profit de cette rationalité économique.

Le développement de technologies « justes » favorisant l'autonomie, individuelle et collective, au service d'organisations sociales dans lesquelles les personnes auraient le contrôle de l'outil serait de nature à élargir le pouvoir de l'action collective. L'objectif ? Rectifier les biais qu'ils soient le fruit d'intentions malveillantes ou de négligences et promouvoir une technologie qui viendrait servir la solidarité.

PERMETTRE UNE ADAPTATION DE LA TECHNOLOGIE AUX BESOINS SOCIAUX ET VICE VERSA

7 — L'innocuité

Les SIA doivent être conçus pour être sûrs, ne pas nuire aux personnes, à leurs biens et à leurs droits. Ce principe obligerait les développeurs d'algorithmes à s'assurer que toutes les précautions ont bien été prises pour éviter d'infliger des dommages matériels ou moraux aux personnes et aux collectivités. Cette démarche induit également de ne faire appel à l'IA que lorsque sa contribution nette est positive pour l'Humanité. Cela implique que dans la relation humains-machines les rôles soient strictement définis. Techniquement, cela implique des systèmes conçus pour éviter toute nuisance, que ce soit en termes de sécurité physique ou de protection des données personnelles. La mise en place

de protocoles de sécurité robustes et la conformité avec la réglementation notamment le RGPD constituent des mesures préventives essentielles.

Juridiquement, l'innocuité exige une législation encadrant strictement l'utilisation de l'IA, avec des directives claires pour prévenir les dérives potentielles telles que la surveillance excessive ou le profilage discriminatoire. La création de normes internationales pour les algorithmes et l'obligation de leur conformité à des critères d'équité et de transparence sont également des mesures cruciales pour obtenir un alignement des valeurs.

8 — La responsabilité

Tout déploiement d'un SIA doit engager la responsabilité pleine et entière des personnes et organismes impliqués dans la conception, sa diffusion et son déploiement, en particulier en cas de mauvais fonctionnement ou de conséquences adverses imprévues.

Sur le plan technique, cela implique la mise en place de processus d'évaluation et de suivi rigoureux, le développement de SIA transparents et explicables, ainsi que l'intégration de mécanismes permettant de les désactiver ou de les modifier en cas de détection de comportements inattendus ou dangereux. La responsabilité en matière d'IA doit être encadrée par des normes et standards qui définissent les exigences en termes de sécurité, d'éthique et de conformité.

Elle oblige à une clarification des rôles et des responsabilités des parties prenantes dans le cycle de vie de l'IA, de la conception à sa mise en œuvre et au-delà.

POUR UNE CLARIFICATION DES RÔLES ET DES RESPONSABILITÉS DES PARTIES PRENANTES DANS LE CYCLE DE VIE DES SIA

9 — Le progrès

Il est important de poursuivre les avancées technologiques non seulement pour leur valeur intrinsèque, mais également pour leur contribution au progrès social et humain. Cependant, ces nouveaux outils ne doivent être déployés que

lorsqu'ils apportent une amélioration des conditions d'existence des personnes et des collectivités. Leur objectif sera de contribuer à l'organisation des activités professionnelles et à l'amélioration d'exercice.

Par ailleurs, le principe de finalité doit également s'appliquer à la décision des suppressions de postes. Il est nécessaire d'interdire strictement de telles manœuvres dès lors que l'utilité pour l'intérêt général n'a pas été démontrée. En France, plusieurs instances de dialogue social peuvent être mobilisées pour traiter des enjeux liés à l'intelligence artificielle. Elles jouent un rôle essentiel pour veiller à ce que le développement et l'implémentation de SIA se fassent dans le respect des droits, de manière équitable et responsable.

10 - La vie privée

L'essor fulgurant des SIA conjugué à leur sophistication continue les rend progressivement plus intrusifs pour l'intimité de chacun. Un risque réel dans l'entreprise où la collecte et le traitement massif des données notamment personnelles sont à la source de l'émergence ou de l'évolution de nombreux modèles économiques. Dans un univers panoptique, soumis au contrôle permanent et « intelligent » de la machine et encadré par des algorithmes qui disent quoi faire, comment (mieux) le faire et avec qui le faire, le risque de voir le salarié devenir l'assistant, le serviteur, le supplétif d'une technologie est tout sauf une fiction. La gestion algorithmique se déploie progressivement dans les moindres faits et gestes des travailleurs : du recrutement, à la gestion des emplois et des compétences en passant par la surveillance, l'évaluation et la géolocalisation des salariés. Sans contrôle, ni information, la vie privée des travailleurs s'en trouve alors menacée : surveillance de masse, fichage, profilage... Or le respect de la vie privée est un des piliers de la démocratie sociale. Elle doit être impérativement une pierre angulaire du déploiement de l'IA dans l'entreprise et les administrations publiques.

ANNEXE N° 02.

Faire du RIA une méthode d'action syndicale

Détecter l'IA dans l'entreprise

La première étape consiste à identifier les outils susceptibles de relever du RIA. Certains termes doivent alerter les représentants du personnel : « optimisation », « *scoring* », « pilotage par la donnée », « assistant », « automatisation », « prédiction », « recommandation ». Ces termes peuvent désigner des systèmes d'IA sans que ce mot soit jamais prononcé.

Conduire une enquête syndicale sur un projet d'IA

Étape 1 — Comprendre le fonctionnement de l'outil

Les élus doivent d'abord comprendre quel type d'IA est utilisé, à quoi elle sert, et quelles décisions elle influence. Questions essentielles : quel est l'objectif du système ? S'agit-il d'un outil d'aide à la décision ou d'une décision automatisée ? Quels services de l'entreprise sont concernés ? Qui développe ou fournit la technologie ?

Étape 2 — Identifier les données utilisées

Les systèmes d'IA reposent sur l'analyse de données. Les élus doivent identifier la nature des données utilisées, leur origine, leur mode de traitement et leur durée de conservation. Questions à poser : quelles données alimentent l'algorithme ? Concernent-elles les salariés ? Sont-elles anonymisées ? Où sont-elles hébergées ?

Étape 3 — Analyser les effets sur le travail

Un projet d'IA transforme souvent le contenu concret du travail. Les élus doivent analyser les tâches supprimées, les tâches créées et les nouvelles contraintes. Points d'attention : intensification du travail, standardisation des procédures, réduction de l'autonomie, nouvelles formes de surveillance, modification des qualifications.

Étape 4 — Évaluer les effets sur les métiers et les qualifications

Les technologies d'IA peuvent transformer les métiers de plusieurs façons : disparition de certaines tâches, création de nouvelles compétences, polarisation des qualifications. Questions à poser : quels métiers sont concernés ?
Des suppressions de postes sont-elles envisagées ? Des formations sont-elles prévues ? Les classifications professionnelles doivent-elles évoluer ?

Étape 5 — Examiner les risques sociaux et organisationnels

Risques possibles : intensification du travail, perte de sens du travail, surveillance accrue, dépendance aux systèmes numériques, perte d'autonomie professionnelle. Questions à poser : une évaluation des risques a-t-elle été réalisée ? Le CSE peut-il consulter le Document Unique ? Les effets psychosociaux ont-ils été étudiés ?

La méthode FO-Cadres en 6 étapes

1. **Détection et cartographie :** identifier les systèmes d'IA déployés ou en projet dans l'entreprise.
2. **Demande des documents :** fiche RIA, éléments RGPD, données SST.
3. **Procédure CSE/CSSCT :** engager la procédure de consultation préalable.
4. **Expertise :** expertise technique, SST et juridique si nécessaire.
5. **Négociation :** élaborer et négocier un accord ou une charte IA.
6. **Suivi et audit :** mettre en place des indicateurs, des revues périodiques et un comité de suivi paritaire.

ANNEXE N° 03.

Négocier : du respect du RIA à la qualité du travail

Projet d'architecture d'un accord IA

Le RIA constitue le socle minimal des exigences. L'ambition de FO-Cadres est d'aller au-delà, en transformant ces obligations légales en garanties concrètes sur la qualité du travail, l'autonomie professionnelle et la protection des salariés.

Articles types d'un accord IA

Article 1 — Champ, définitions, registre des systèmes IA : liste tenue à jour, accessible aux IRP (version, finalité, périmètre, qualification RIA).
Article 2 — Gouvernance et comité de suivi paritaire : composition, périodicité, accès aux documents, droit d'alerte, revue annuelle.
Article 3 — Conditions préalables au déploiement : remise obligatoire d'une fiche d'identité RIA, pilote cadré, clause de généralisation sous conditions.
Article 4 — Contrôle humain et responsabilité : nomination des rôles, pouvoirs d'annulation, liste des décisions interdites sur la seule base d'un score.
Article 5 — Information des salariés et contestation : droit à la contestation avec délais, circuits et protections contre les représailles.
Article 6 — Traçabilité, logs et audit : politique de logs, conservation des versions, droit à l'audit interne et externe.
Article 7 — Données, non-discrimination, égalité : tests anti-biais, indicateurs de suivi et actions correctrices obligatoires.
Article 8 — Santé, sécurité, conditions de travail : évaluation des impacts, interdiction de la surveillance disproportionnée.
Article 9 — Formation et AI literacy : plan de formation salariés, managers et élus, budget et calendrier.
Article 10 — Sous-traitants et fournisseurs : exigences contractuelles de conformité, assistance incidents, encadrement de la réutilisation des données.
Article 11 — Réversibilité et amélioration continue : clause de retour arrière possible, conditions d'arrêt, revues périodiques.

ANNEXE N° 04.

Modèle FO-Cadres : fiche d'identité RIA d'un système d'IA

Le RIA constitue le socle minimal des exigences.
L'ambition de FO-Cadres est d'aller au-delà, en transformant ces obligations légales en garanties concrètes sur la qualité du travail, l'autonomie professionnelle et la protection des salariés.

En-tête de la fiche

Titre du système / nom commercial :

_____

Version / date / environnement : (pilote / production)
Direction porteuse : (DSI / RH / Opérations…)
Fournisseur(s) / intégrateur(s) : (coordonnées + contrat / DPA / SLA)
Référents internes : (DSI, RH, métier, DPO, SST, RSSI)

Finalité et périmètre

- Finalité(s) déclarée(s) (ce que l'entreprise cherche à faire) : _____
- Décisions / processus impactés : (recrutement, évaluation, affectation, disciplinaire, planning…)
- Population concernée : (salariés, candidats, intérimaires, prestataires, managers…)
- Caractère obligatoire/facultatif : l'outil est-il imposé ? des alternatives existent-elles ?
- Niveau d'automatisation : information/recommandation - classement/*scoring* - proposition de décision - exécution automatisée
- Impact individuel possible (carrière, rémunération, sanction, accès à l'emploi, charge, horaires, santé…) : _____

Qualification RIA

- Qualification proposée par l'employeur : pratique interdite - IA à haut risque - obligations de transparence - autre/hors champ (à justifier)

- Justification de la qualification : (critères utilisés, usages précis)
- Documentation de conformité fournie par le fournisseur : (références, notice, manuels, attestations)

Contrôle humain

- Qui contrôle ? (rôle, compétences, délégation)
- Quand intervient l'humain ? (avant / pendant / après)
- Pouvoir réel de l'humain : modifier/annuler/corriger - suspendre l'outil - décider sans tenir compte du score
- Procédure de contestation interne : délais, recours, interlocuteurs
- Interdits internes : décisions qui ne peuvent jamais être prises sur la seule base du système

Données et entrées

- Données d'entrée utilisées (catégories) et sources (SI RH, badgeuse, CRM, emails…)
- Données sensibles / inférences : oui - non — si oui, lesquelles ?
- Mesures anti-biais / anti-discrimination : (tests, audits, corrections)
- Mesures de qualité des données : (exactitude, mises à jour, minimisation)

Traçabilité et logs

- Le système génère-t-il des logs ? oui - non — Contenu : (entrées, sorties, horodatage, version du modèle…)
- Durée de conservation des logs et accès (qui, comment, traçabilité des accès)
- Archivage des versions (modèle, paramètres, règles) : oui/non — modalités

Incidents et sécurité

- Typologie d'erreurs connues (faux positifs/négatifs, hallucinations, dérives) :
- Procédure incident : déclaration, escalade, gel/suspension, correction
- Tests avant déploiement : (pilote, critères de réussite, retour d'expérience)

Transparence et information-consultation

- Information des salariés concernés (contenu, date, support) :
- Information/consultation des IRP : dates, documents remis, expertises
- Formation / *AI literacy* : publics, contenu, calendrier, évaluation

Impacts travail

- Impact charge et rythme (objectifs, intensification, astreintes) :
- Impact qualité du travail / autonomie :
- RPS / surveillance : indicateurs, garde-fous
- Mesures de prévention : (organisation, effectifs, formation, droit à la déconnexion)

ANNEXE N° 05.

35 questions et 8 thématiques pour l'examen d'un système d'IA en entreprise

Contexte et justification du projet

1. Quel problème cherchez-vous à résoudre ? Pourquoi une IA plutôt qu'une autre solution ?
2. Quels processus RH sont concernés (recrutement, carrière, planning, disciplinaire…) ?
3. Qui est concerné (salariés, candidats, prestataires) et à quelle échelle ?
4. L'outil est-il obligatoire ? Existe-t-il une alternative non algorithmique ?

Qualification RIA et responsabilités

5. L'outil produit-il des recommandations, scores ou décisions concernant des personnes ? Si oui, quelle qualification RIA est retenue (haut risque / transparence / autre) et sur quelle base ?
6. Ce système est-il enregistré dans la base de données UE des systèmes à haut risque (art. 49 et 71 RIA) ?
7. Dispose-t-on de la notice d'utilisation fournie par l'éditeur (art. 13 RIA) ? Quels sont les usages autorisés et interdits ?
8. Êtes-vous « déployeur » au sens du RIA ?
Quelles obligations assumez-vous ?
9. Qui est responsable en interne (métier / DSI / RH) ? Qui arbitre en cas de doute ?

Contrôle humain et décision

10. Qui exerce concrètement le contrôle humain sur les décisions du système ? Avec quelle compétence, quelle formation, quel temps réel disponible ?
11. L'humain peut-il réellement corriger ou annuler une décision du système sans contrainte ni pression ?
12. Quelles décisions ne peuvent jamais être prises sur la seule base du système, sans examen humain préalable ?
13. Comment évite-t-on l'automatisation de fait, où le manager suit

systématiquement la recommandation algorithmique sans examen critique ?
14. Quelle procédure pour contester une décision influencée par l'IA ? (délais, interlocuteurs)

Données, biais et discrimination

15. Quelles données sont utilisées comme entrées du système ? D'où viennent-elles ? Sur quelle période ?
16. Des données issues de surveillance sont-elles utilisées (productivité, emails, activité écran…) ?
17. Le système réalise-t-il des inférences sur des catégories sensibles (comportement, fiabilité, émotion, opinions syndicales, santé, origine, âge…) ?
18. Des tests anti-biais ont-ils été réalisés avant le déploiement ? Quels sont les résultats ? Sont-ils périodiquement répétés ?
19. Comment les discriminations indirectes sont-elles détectées et corrigées ? Quels indicateurs de suivi existent par genre, âge, origine, handicap ?
20. Quelles mesures correctrices sont prévues si un biais est détecté ?

Traçabilité, *logs* et audit

21. Le système génère-t-il des journaux automatiques (logs) ? Quel est leur contenu précis ?
22. Ces journaux sont-ils conservés pendant au moins 6 mois (art. 26 §6 RIA) ? Qui y accède, et comment, notamment en cas de contestation ?
23. Les versions du modèle (paramètres, règles, données d'entraînement) sont-elles archivées et accessibles pour comparaison dans le temps ?
24. Un audit interne ou externe est-il prévu ? Avec quel périmètre et quelles conditions d'accès ?

Incidents, sécurité et réversibilité

25. Quelles erreurs typiques sont connues et comment sont-elles gérées ?
26. Quelle procédure est prévue en cas d'incident ou d'effet indésirable ? Dans quelles conditions le système peut-il être suspendu ou arrêté ?
27. Des critères de réussite du déploiement ont-ils été définis ?

Que se passe-t-il si ces critères ne sont pas atteints ou si l'IA dégrade la qualité du service ou intensifie le travail ?
28. Une clause de réversibilité existe-t-elle, permettant de revenir à l'organisation antérieure ?

Information, consultation et formation

29. Les travailleurs concernés ont-ils été informés avant le déploiement (contenu, droits, modalités de contestation) — obligation art. 26 §7 RIA ?
30. Le CSE a-t-il été consulté conformément à l'art. L.2312-8 du Code du travail, suffisamment tôt pour pouvoir influencer le projet ? Dispose-t-il de tous les documents nécessaires (description du projet, impacts emploi, conditions de travail, effets santé) ?
31. Un plan de formation est-il prévu pour les salariés, managers et élus sur le fonctionnement et les limites du système ? Les managers sont-ils formés à ne pas déléguer automatiquement leur jugement à l'algorithme ?
32. Quel est le budget formation dédié ? Le temps de formation est-il reconnu comme temps de travail ?

Fournisseur et contrat

33. Quel est le rôle du fournisseur ? Quelles garanties contractuelles ont été obtenues : conformité RIA, documentation technique, assistance en cas d'incident, droit d'audit ?
34. Le contrat interdit-il la réutilisation des données des salariés pour entraîner d'autres modèles ?
35. Le fournisseur est-il en mesure de produire la documentation technique de conformité ? (marquage CE, déclaration de conformité UE)

POINT DE VIGILANCE // Astuce de conduite : demander que chaque réponse renvoie à un document précis (fiche outil, procédure, manuel, log, indicateur). Sans document = réponse non recevable.

ANNEXE N° 06.

20 propositions FO-Cadres pour une IA socialement responsable

Les débats autour de l'IA laissent placent à un sentiment partagé où l'ambivalence qui caractérise les évolutions technologiques se mêle à la fascination de la puissance de calculs des systèmes d'IA. Ce discours fait écho de manière forte au vécu des salariés et des agents publics. Ces derniers sont à la fois fascinés par les formidables potentialités offertes par l'usage de l'IA, et inquiets des risques d'un déploiement incontrôlé de l'IA sur les lieux de travail. Le potentiel de ces technologies est suffisamment important pour qu'on commence à les craindre, ou à trop en espérer. Car si la technologie peut avoir un caractère magique et fascinant, elle oppresse souvent les salariés et les agents publics lorsqu'elle est au cœur d'un univers professionnel dérégulé. Loin de céder aux sirènes d'un néo-luddisme fustigeant toutes innovations technologiques, c'est à l'appel d'un sursaut critique face au déploiement massif des SIA dans l'univers professionnel qu'il convient de répondre au plan syndical. Un sursaut critique pour interroger la technologie à l'aune des besoins sociaux et mettre à l'abri les travailleurs de toutes tentatives à les rendre translucides. Ce sursaut que nous appelons de nos vœux trouve une traduction opérationnelle dans les 20 propositions suivantes. Un travail modeste au service de la promotion d'un dialogue social technologique à même d'allier innovation et protection.

PROMOUVOIR UNE INTELLIGENCE ARTIFICIELLE GARANTE DES DROITS FONDAMENTAUX

1. Revendiquer un droit à l'opacité au travail

Dès lors que l'entreprise fait sien le secret des affaires pour protéger ses données, son intimité économique, les travailleurs ne pourraient-ils pas opposer dans le même esprit un droit à l'opacité ? Le secret tout comme l'opacité obligent à voir dans ces deux termes aussi bien une donnée, une valeur qu'un danger. Entre l'opacité absolue qui peut renvoyer à la dissimulation voire à un obstacle à la compréhension, et la transparence totale qui révèle et permet la connaissance de tout sur tout, l'opacité comme secret négocié serait le point d'équilibre entre ces deux contraires. En opposant l'opacité des travailleurs à

l'empire absolu de la transparence à l'ère numérique, c'est le pouvoir de dire non à toute forme d'emprise technologique sur l'intimité qui serait ici assuré. Dans tous les cas, tout en favorisant l'innovation et la croissance économique un droit des usages de l'IA au travail doit s'affirmer pour mieux protéger les travailleurs. Il faut s'assurer que la réglementation en cours sera suffisamment adaptée aux problèmes et inquiétudes dans le monde du travail.

2. Systématiser la prévention et la vigilance collectives

Sans contrainte légale, les discussions sur la mise en œuvre de critères soumis aux entreprises et aux administrations avant tout déploiement d'une technologie d'Intelligence Artificielle peuvent rencontrer des difficultés pour aboutir à des résultats tangibles.

C'est pourquoi il est nécessaire de traduire positivement dans le droit un principe de prévention en cas de risques identifiés de façon certaine et auquel il serait possible de se référer en cas de litiges pour contester le déploiement de tout système d'intelligence artificielle ou exiger la réalisation d'étude d'impacts complémentaires. Il existe une convergence sur ce point avec la proposition de règlement européen sur l'IA, dans laquelle certains SIA sont considérés « à haut risque » (article 6) et requièrent des obligations spécifiques.

FAIRE DES SYSTÈMES D'INTELLIGENCE ARTIFICIELLE UN OBJET DE DIALOGUE ET DE NÉGOCIATION COLLECTIVE

3. Adopter un principe de précaution responsable

En cas de risques identifiés, de façon certaine, sur le lieu de travail, il est important de pouvoir mobiliser, aux côtés du principe de prévention, un principe de précaution. Celui-ci rendu effectif doit permettre de stimuler la production de connaissance et conduire à des progrès notables dans le domaine du contrôle et de la protection des personnes face à l'IA. Ce principe ne doit pas s'opposer au développement technologique, mais se positionner dans l'action. Pourvu d'un contenu positif, il contribuera, dans le cadre d'un dialogue effectif et continu sur l'usage de l'IA à trouver les voies et moyens de l'innovation tout en écartant les risques pour les travailleurs.

Ainsi nous pourrions envisager un système de licence prohibant la création de SIA notamment dans le domaine des pratiques RH sans avoir obtenu au préalable un aval de l'autorité de régulation.

4. Adapter le code du travail aux enjeux de l'IA

Le peu de références au terme « algorithme » que contient le Code du Travail concerne des articles relatifs aux plateformes numériques. Bien que certaines de ses dispositions puissent être interprétées dans le contexte de l'IA, la santé, la sécurité, ou encore l'information-consultation des IRP, l'expansion de l'IA dans l'univers professionnel, nécessite une mise à jour ou une extension du Code du travail pour aborder spécifiquement ce sujet. Cela pourrait être des questions thématiques telles que la surveillance et le management algorithmiques, la prise de décision automatisée et ses impacts sur les salariés ou agents, ou encore la gestion des carrières liée à l'automatisation.

Avec le développement de l'IA, le droit du travail qui a réintroduit la personne humaine dans un cadre contractuel doit être est plus que jamais un instrument de protection de la dignité de l'Homme au travail.

5. Négocier des accords collectifs sur les usages de l'IA au travail

En l'absence de régulation et de contrôle collectif négocié, les usages de l'IA sur les lieux de travail peuvent ouvrir la voie à une surveillance intrusive et abusive des activités des travailleurs avec notamment des risques d'exploitation systématique, de discrimination, de problèmes de santé et de sécurité au travail. Ce constat exige d'associer les travailleurs et leurs représentants aux processus de prise de décision qui aboutissent au développement et au déploiement de l'IA. Le dialogue social doit ainsi prendre toute sa place pour que le recours à l'IA soit discuté et négocié à tous les niveaux de l'entreprise.

Un accord national interprofessionnel sur l'IA au travail apparait incontournable pour édicter des lignes directrices fortes en la matière et bâtir une régulation efficace au niveau des branches professionnelles et des entreprises. L'ensemble des instances de dialogue social doivent être mobilisées pour traiter des enjeux liés à l'intelligence artificielle (IA) dans le monde du travail. Leur rôle est crucial pour assurer que le développement et l'implémentation de l'IA concourent au progrès humain et au respect de la démocratie sociale.

6. Encourager les voies du dialogue et du débat collectif

Les Comités Stratégiques de Filière (CSF) en France, qui rassemblent des acteurs clés de secteurs industriels spécifiques (entreprises, syndicats, organismes de formation, etc.) définissant des stratégies de développement, peuvent jouer un rôle important face aux enjeux spécifiques de l'Intelligence Artificielle (IA). Leur rôle pourrait être d'élaborer des stratégies spécifiques pour intégrer l'IA dans leurs filières respectives, en tenant compte des particularités et des besoins de chacune. Ils joueraient alors un rôle crucial dans le soutien à l'industrie pour bâtir une souveraineté numérique et dans l'accompagnement des petites et moyennes entreprises (PME) ainsi que dans l'adoption et l'utilisation d'une IA éthique et respectueuse des droits fondamentaux.

Dans l'entreprise et les administrations, les parties prenantes ne sont pas seulement l'employeur et l'employé, ce sont aussi les partenaires, les co-producteurs et enfin les fournisseurs de services et de solutions. Les débats publics sur les enjeux technologiques doivent laisser de la place à l'ensemble de ces parties prenantes pour une meilleure défense et négociation des libertés collectives. La composition et le rôle du CESE sont de ce point de vue une richesse qu'il convient de solliciter pour nourrir les débats collectifs sur les enjeux de l'IA dans la société en général et dans le monde du travail en particulier.

7. Bâtir des référentiels sectoriels

Afin de renforcer la sécurité et d'encourager une innovation éthique et responsable, le recours à des référentiels de certification des SIA sur le modèle des normes ISO ou des analyses ABC utilisées pour la performance énergétique doit être encouragé. Ces référentiels viseront à établir les objectifs clairs que la certification cherche à atteindre autour de normes comme la qualité des données, la sécurité des systèmes, la transparence algorithmique, la robustesse, la résilience des dispositifs et le respect des droits fondamentaux. Il s'agit de déterminer les critères spécifiques que les systèmes d'IA doivent remplir pour être certifiés. Il s'agit également par ce biais de s'assurer, dès la conception des outils IA, l'humain demeure aux commandes.

La création de tels référentiels nécessite d'initier une collaboration entre les sciences cognitives, l'informatique, la philosophie et les sciences sociales.

Une approche interdisciplinaire qui veille à mettre en garde contre les excès d'optimisme concernant les capacités de l'IA par rapport à l'intelligence humaine.

8. Renforcer l'expertise et les moyens d'action des IRP*

Face aux risques qui pourraient être engendrés par le déploiement de l'intelligence artificielle, les IRP doivent être consultées et impliquées dans toutes les phases de conception, de développement et de déploiement des systèmes d'IA dans l'entreprise. Elles doivent être également associées aux décisions stratégiques concernant l'implémentation de l'IA, y compris le choix des technologies, des fournisseurs et des politiques de gestion des données. Dans cette perspective, les entreprises doivent fournir aux membres du CSE une formation spécialisée sur l'intelligence artificielle et ses implications dans le monde de travail. Cette formation doit leur permettre de comprendre et d'évaluer adéquatement les projets d'IA et leurs enjeux. Des ressources doivent être allouées pour permettre au CSE d'auditer les outils d'IA en amont de leur déploiement dans l'entreprise et réaliser une veille technologique et éthique continue sur leurs évolutions et leurs impacts potentiels sur l'organisation et les conditions de travail. La jurisprudence du Tribunal judicaire de Pontoise en 2022** a établit que l'introduction d'une nouvelle technologie justifie à elle seule le recours à une expertise par le CSE, sans même qu'il soit nécessaire de démontrer l'existence de répercussions sur les conditions de travail des salariés.

** Instances représentatives du personnel ** TJ Pontoise, 15 avr. 2022, n° RG 22/00134, S.A.S. Atos International c/ CSE de la société Atos International)*

DÉFENDRE UN DÉVELOPPEMENT DES SYSTÈMES D'INTELLIGENCE ARTIFICIELLE INTELLIGIBLES ET SOCIALEMENT RESPONSABLES

9. Promouvoir le « *Social by Design* »

Après l'ouverture des données l'enjeu est celui de la connaissance des savoirs et décisions prises à partir de ces data en vue de restaurer ou d'améliorer la confiance dans l'usage des outils d'IA.. Nous devons encourager les développeurs à intégrer les exigences de certification dès les premières étapes de conception

des produits et services IA afin d'y d'intégrer, nativement, des principes de transparence et de loyauté, d'intelligibilité des systèmes et des décisions. Il s'agit également de promouvoir un développement itératif, autorisant des améliorations continues visant à une certification ultérieure, notamment au sein des entreprises. L'objectif est ainsi de permettre aux organisations de pouvoir ouvrir le capot des systèmes qu'elles mobilisent pour en faire la source d'un nouveau dialogue social autour des enjeux de solidarité, de protection, d'accessibilité et d'inclusivité. En plus d'assurer la protection des données à caractère personnel dès la conception d'un outil IA (Privacy by Design) il est également nécessaire d'assurer la protection des droits fondamentaux (Social by Design) en encourageant la participation de toutes les parties prenantes dans ce processus de création.

10. Rendre effectif le droit à l'intelligibilité

Les systèmes d'intelligence artificielle fournissent des résultats sans donner les moyens de comprendre le processus logique dont ils procèdent. Véritables « boîtes noires » ils participent à la méfiance vis-à-vis de ces technologies. La transparence des algorithmes, de leurs emplois, de leurs usages et de leurs finalités est donc déterminante pour consolider la confiance et leur adoption.

Il s'agit d'exiger la complétude des informations auprès de l'employeur qui décide de les mettre en place et de leurs concepteurs des dispositifs. La transparence dans la manière dont les décisions sont prises est fondamentale et doit pouvoir être expliquée dans un langage clair et compréhensible en se concentrant sur les principes de base plutôt que sur les aspects techniques complexes.

DÉVELOPPER DES DISPOSITIFS DE VIGILANCE COLLECTIVE AU CŒUR DES ORGANISATIONS

11. Rendre systématiques les études d'impact

Au-delà de la conformité aux lois sur la protection des données, les entreprises doivent intégrer comme une phase obligatoire dans la réflexion et la réalisation de projets technologiques, dès les prémisses de la discussion et avant tout déploiement, une section dédiée à l'évaluation des impacts sociaux des

technologies d'IA, sur l'emploi, les métiers, les conditions de travail et les relations sociales.

Cela peut se traduire par des études, des enquêtes, des interviews et la constitution de groupes de discussion pour évaluer les implications potentielles. Les représentants du personnel doivent être associés dès le début du processus pour assurer un suivi continu et une révision des impacts collectifs sur les lieux de travail. A l'issue des résultats, les mesures prises pour prévenir et corriger les biais donneront lieu à la publication d'un rapport accessible aux IRP.

12. Permettre la réversibilité des systèmes IA

Les outils d'IA nécessitent d'être régulièrement ajustés, mis à jour ou modifiés pour s'adapter à de nouvelles données ou conditions. La réversibilité permettrait cette flexibilité afin de mieux gérer les risques associés à leur utilisation. Si un système s'avère défectueux, biaisé, ou cause des dommages imprévus, il doit pouvoir être désactivé ou ramené à une version antérieure plus stable. En pratique, la réversibilité peut être difficile à mettre en œuvre, en particulier pour les SIA complexes ou ceux intégrés dans des infrastructures critiques. Une planification minutieuse, des tests réguliers et une conception systématique permettant une déconnexion ou une régression sans faille pourraient inclure des fonctionnalités comme un « bouton d'arrêt d'urgence » ou « des clapets de sécurité », ainsi que des options de restauration, des sauvegardes de données et des protocoles de retrait sécurisés. En outre, les utilisateurs doivent avoir la possibilité de contester l'utilisation de tout outil qu'ils considèrent nuisible à leur vie professionnelle ou personnelle.

13. Favoriser les expérimentations

La confiance se fonde sur la réciprocité et se bâtit dans le temps. Elle ne se décrète pas. Il est donc primordial que le développement et le déploiement des systèmes d'IA sur les lieux de travail se réalisent « sans coups de force » et dans la plus grande transparence. L'entreprise doit faire la démonstration que l'emploi des outils IA concoure à la croissance de richesse dans une démarche de responsabilité sociale où les droits fondamentaux des salariés sont préservés. Le « bac à sable » (sandbox en anglais) réglementaire, gage d'innovation, peut contribuer à la réalisation de cet édifice. Il peut permettre

de tester et d'expérimenter des outils IA dans un cadre contrôlé, réduisant les risques et assurant la conformité avec la législation, notamment le RGPD. Cette démarche qui offre ainsi une certaine flexibilité ou des adaptations temporaires des normes réglementaires favorise l'innovation responsable, tout en étant encadrée par la CNIL pour veiller à ce que les droits fondamentaux des salariés soient protégés en matière de collecte, de traitement et d'utilisation des données personnelles.

14. Créer un comité de supervision

Dès lors que les SIA sont des technologies évolutives et apprenantes nécessitant d'être auditées en amont comme en aval, la création d'un comité de supervision permettrait d'assurer un suivi continu de des usages des outils IA. Composé des élus du personnel, du DPO, du DSI et du RSSI ce comité aurait pour rôle de superviser, avec le concours d'experts en éthique, en sciences sociales, en technologie, en droit et en gestion des risques dans la mesure du possible, l'utilisation des outils IA et s'assurer que ces derniers sont utilisés de manière responsable, sans risques pour les employés et sans produire d'externalités négatives pour l'entreprise. Ce comité proposerait des dispositifs de vigilance collective et de régulation adaptés lors de revues périodiques. Des checklists d'évaluation éthique et sociale pouvant être utilisées pour s'assurer à différentes étapes du cycle de développement des produits que les considérations éthiques sont prises en compte. Les recommandations et leurs motifs seront adressés au CODIR et au CSE et rendus accessibles selon des modalités appropriées, aux parties prenantes de l'entreprise afin des fins de consultation notamment en cas de contestation. Dans le cas des TPE, les missions du comité de supervision pourraient être intégrées à l'instance de dialogue social que constitue la commission paritaire régionale interprofessionnelle (CPRI).

15. Bâtir des chartes et codes de conduites contraignants

Les nombreuses chartes et codes de conduite rédigés pour infléchir des comportements au regard de règles ou de valeurs sont souvent des instruments volontaires d'autorégulation dépourvus de contrôle indépendant et de règles juridiques contraignantes. Pour encadrer efficacement le déploiement de l'IA sur les lieux de travail, ces chartes et codes, certifiés par la CNIL conformément aux dispositions prévues à l'article 40 du RGPD doivent introduire des

mécanismes d'évaluation et traiter des risques technologiques. Ce travail exige une coopération étroite avec les autorités de contrôle pour bénéficier de conseils susceptibles de développer des lignes d'orientation sur la protection des données et le respect de la vie privée sur les lieux de travail.

La validité de ces outils de régulation doit être subordonnée à l'existence d'une convention conforme à la réglementation encadrant notamment la durée de conservation des données, les modalités d'accès et les mesures de sécurité, les obligations de transparence et la procédure à suivre en cas de violation de donnée à caractère personnel.

16. Créer un registre des outils d'IA et de leurs usages

En prenant exemple sur certaines villes et administrations locales, comme Amsterdam et Helsinki, qui ont créé des registres publics d'algorithmes pour augmenter la transparence autour de l'utilisation des technologies d'IA et algorithmiques par les autorités publiques, il serait opportun de rendre obligatoire la tenue d'un registre recensant l'ensemble des usages de l'IA déployés dans l'entreprise. Ce registre à l'image de celui prévu à l'article 30 du RGPD pour les traitements des données à caractère personnel devra comporter les informations relatives à la nature des outils d'IA, des activités de traitements effectuées sous leur égide ainsi que la nature des données collectées et la finalité poursuivie par ces différents systèmes. Un tel registre porté à la connaissance des différentes parties prenantes formaliserait les obligations de transparence et de loyauté.

RENFORCER L'AUTONOMIE INFORMATIONNELLE DES ACTEURS PAR LA FORMATION ET L'INFORMATION

17. Bâtir un plan de formation spécifique à l'IA

Les professionnels des ressources humaines, de la direction des systèmes d'information (DSI) et les représentants du personnel doivent bénéficier de formations communes afin d'être sensibilisés ensemble aux conséquences liées à la mise en place de l'intelligence artificielle au sein de l'entreprise. Les entreprises et les administrations doivent établir un plan de formation spécifique à l'IA pour aux salariés et agents de mettre à jour leurs connaissances

sur les développements récents en IA et technologies numériques, ainsi que sur leurs implications sociales. Cette offre de formation régulière doit conduire à sensibiliser sur les enjeux et les conséquences sociales et éthiques des SIA.

Dans cette perspective, la formation des ingénieurs est essentielle afin de les sensibiliser de manière plus appuyée aux enjeux liés aux outils qu'ils conçoivent et les informez clairement sur les mesures prises pour garantir la sécurité des données et la protection de la vie privée dans le cadre de l'utilisation de l'IA.

18. Contribuer à la formation des managers

Le déploiement d'outils numériques tels que l'IA peut impacter les interactions entre le manager et les équipes. Certains logiciels peuvent même interférer au cœur de la fonction managériale, voire prendre eux-mêmes ou participer à la prise de décision. Les managers doivent donc être en mesure de comprendre les nouvelles formes d'expertise nécessaires pour travailler efficacement avec ces outils et aider leur équipe à s'approprier ces technologies.
Des modules de formation spécifiques sur les implications managériales des usages de l'IA doivent être intégrés dans le parcours professionnel des managers. Ces formations doivent leur offrir les moyens d'opter pour une organisation transparente et stable autour de discussion et de négociation des usages des SIA avec leurs collaborateurs.
Les managers ont dès lors un rôle clé pour veiller à l'articulation harmonieuse entre l'homme et la machine. et bannir toute forme de management algorithmique liberticide et promouvoir un management par la confiance et non par la surveillance notamment algorithmique.

19. Soutenir la mise en place d'un réseau « relais IA »

La mise d'un réseau de « relais de l'IA » au sein des entreprises composé généralement d'employés ayant diverses expertises techniques et opérationnelles dans le domaine de l'IA, des experts en données, et des utilisateurs clés dans différents départements. Elle participe de l'édification d'une compétence collective s'appuyant sur une grammaire commune de l'IA qui procède du travail de l'ensemble des salariés.
Cette compétence collective constitue une opportunité en matière d'ingénierie sociale, mais aussi une opportunité, dans tous les secteurs, pour faciliter

l'adoption et l'intégration des SIA dans l'entreprise en permettant le partage des connaissances, le soutien technique, et la promotion de l'utilisation efficace des outils IA.

En lien avec le comité de supervision et le DPO, il agit comme un catalyseur pour l'innovation et la transformation numérique, en offrant des formations, des ressources et un soutien opérationnel pour l'implémentation de l'IA.

Son action doit permettre de fournir des solutions techniques permettant aux salariés d'agir sur le paramétrage des solutions d'IA qui organisent et conditionnent leurs activités.

20. Protéger l'indépendance des DPO

Lorsque le DPO est salarié de l'entreprise celui-ci peut faire l'objet de pressions si fortes qu'il ne pourra rester réellement indépendant. Le RGPD prévoit que le DPO ne peut être sanctionné pour des raisons inhérentes à sa mission mais ce régime ne lui confère que peu de protection en cas de licenciement ou d'éventuelles sanctions. Cela justifie des garanties supérieures au RGPD parmi lesquelles l'octroi du statut de salarié protégé. La Cour de justice de l'Union Européenne a récemment rappelé qu'il est possible aux États membres de prévoir une protection plus importante en faveur des DPO, en limitant par exemple les possibilités de licenciement d'un DPO salarié à la commission d'une faute grave ou après autorisation de l'inspection du travail.

Dans tous les cas le législateur doit permettre que le CSE soit informé obligatoirement de la désignation de leur DPO afin de s'assurer de ses conditions d'exercice et de son indépendance. Les entreprises et les administrations doivent également s'engager formellement à assurer leur indépendance et le préciser à la CNIL lors de la désignation (exemple pouvoir s'adresser directement à la direction).

Il convient enfin que le règlement intérieur veille lorsque le poste de DPO est extérieur à l'entreprise que le contrat de prestations soit précis et détaillé pour éviter tout conflit d'intérêts.

ANNEXE N° 07.
Glossaire

Termes clés

Algorithme : Suite d'instructions définissant un processus de calcul ou de décision automatisé.
Biais algorithmique : Distorsion systématique dans les résultats d'un système d'IA, souvent due à des données d'entraînement non représentatives.
Contrôle humain (*human oversight*) : Capacité d'un individu ou d'une organisation à superviser, corriger ou annuler les décisions produites par un système d'IA.
Déployeur : Au sens du RIA, toute personne physique ou morale, autorité publique, agence ou autre organisme qui utilise un système d'IA sous sa responsabilité.
IA générative : Système capable de produire du contenu nouveau (texte, image, code, audio) à partir de données d'entraînement.
***Machine Learning* (apprentissage automatique) :** Technique d'IA permettant à un système d'apprendre à partir de données sans être explicitement programmé pour chaque tâche.
Management algorithmique : Usage de systèmes algorithmiques pour organiser, attribuer, surveiller, superviser et évaluer le travail (définition OIT).
RIA / AI Act : Règlement européen sur l'intelligence artificielle (2024), premier cadre juridique horizontal encadrant le développement, la mise sur le marché et l'utilisation des systèmes d'IA dans l'UE.
RGPD : Règlement général sur la protection des données (2018), encadrant le traitement des données personnelles dans l'UE.
***Shadow AI* :** Utilisation d'outils d'IA par les salariés en dehors des dispositifs officiellement déployés par l'organisation.
Système d'IA à haut risque : Au sens du RIA, système susceptible de porter une atteinte significative aux droits fondamentaux ou à la sécurité des personnes, soumis à des obligations renforcées.
Traçabilité : Capacité à retracer les décisions prises par un système d'IA, notamment grâce aux journaux (logs) conservant les entrées, sorties et conditions de fonctionnement.

Livre Blanc IA et dialogue social. Négocier l'IA pour une innovation responsable
Version 1.0 | Juin 2026
ÉDITION ET DIRECTION
Directeur de publication : Éric PÉRÈS
L'Union des Cadres et ingénieurs — FO
7, passage Tenaille - 75014 Paris
SIRET : 785 308 412 00036
RÉDACTION ET CONCEPTION
Auteur : Éric PÉRÈS
Maquettiste : Marion PALM
Illustrations : Magnific.com

FO-CADRES

L'UNION DES CADRES ET INGÉNIEURS - FO

www.fo-cadres.fr

7, passage Tenaille
75014 Paris

UCIFOCADRES FOCADRES FO-CADRES