Un salarié peut-il utiliser des outils d'IA générative sans autorisation de l'employeur ?

Réponse courte

Un salarié ne peut pas utiliser des outils d'IA générative sans **autorisation de l'employeur** dans le cadre de son activité professionnelle. Le contrat de travail impose une obligation de **loyauté** et de respect des **instructions de l'employeur**. L'utilisation non autorisée d'outils d'IA, notamment d'IA générative externe, peut constituer une **faute disciplinaire** sanctionnable.

L'utilisation clandestine d'outils d'IA non approuvés (**shadow AI**) expose l'entreprise à des risques de **fuite de données confidentielles**, de violation du obligations RGPD et d'atteinte à la propriété intellectuelle. L'employeur doit encadrer les usages par une **charte IA** claire et des formations, plutôt que de se limiter à une interdiction qui risque d'être contournée.

Définition

Le **shadow AI** (ou IA clandestine) désigne l'utilisation par les salariés d'outils d'intelligence artificielle non approuvés par l'employeur, sans connaissance ni autorisation de la direction ou du service informatique. Ce phénomène concerne principalement les outils d'IA générative gratuits ou en accès libre (ChatGPT version gratuite, outils en ligne) utilisés pour des tâches professionnelles.

Cette pratique pose des problèmes juridiques multiples : violation de l'obligation de **loyauté contractuelle**, atteinte à la **confidentialité des données**, non-respect de la **politique de sécurité informatique** et transfert non autorisé de données vers des serveurs hors UE.

Conditions d’exercice

L'utilisation d'outils d'IA par le salarié est encadrée par le contrat de travail et les obligations légales.

Obligation	Détail
Loyauté contractuelle	Le salarié doit respecter les instructions de l'employeur et ne pas agir contre les intérêts de l'entreprise (obligation issue du contrat de travail)
Règlement intérieur	Le salarié est tenu de respecter les règles d'utilisation des outils informatiques et la charte IA lorsqu'elle existe
Confidentialité	Obligation de ne pas divulguer les informations confidentielles de l'entreprise, y compris en les saisissant dans des outils d'IA externes
Politique de sécurité	Obligation de respecter la politique de sécurité informatique, qui peut interdire l'installation ou l'utilisation de logiciels non approuvés
RGPD	Le salarié qui saisit des données personnelles dans un outil d'IA non autorisé engage potentiellement la responsabilité de l'employeur en tant que responsable de traitement
Propriété intellectuelle	Les contenus produits avec l'IA dans le cadre professionnel appartiennent à l'entreprise ; l'utilisation d'outils non approuvés peut compromettre ces droits

Modalités pratiques

La gestion du risque de shadow AI nécessite une approche combinant encadrement et sensibilisation.

Action	Détail
Charte IA	Adopter une charte définissant clairement les outils autorisés, les usages permis et interdits, et les sanctions applicables
Solutions approuvées	Mettre à disposition des salariés des outils d'IA approuvés et sécurisés répondant à leurs besoins opérationnels
Formation	Sensibiliser les salariés aux risques du shadow AI et les former à l'utilisation responsable des outils approuvés
Détection	Mettre en place des mécanismes techniques de détection de l'utilisation d'outils non autorisés (filtrage réseau, logs)
Procédure disciplinaire	Définir les sanctions graduelles en cas de non-respect (avertissement, blâme, sanction disciplinaire)
Canal de remontée	Créer un processus permettant aux salariés de demander l'approbation de nouveaux outils d'IA pour leurs besoins

Pratiques et recommandations

Proposer des alternatives approuvées couvrant les principaux besoins des salariés en matière d'IA générative, car l'interdiction pure sans alternative conduit inévitablement au shadow AI et à des risques non maîtrisés.

Communiquer clairement sur les risques concrets du shadow AI en utilisant des exemples illustrant les conséquences possibles (fuite de données clients, violation de secret d'affaires, sanctions disciplinaires) pour responsabiliser les salariés.

Graduer les sanctions en fonction de la gravité du manquement, en distinguant l'utilisation ponctuelle d'un outil grand public sans données sensibles de l'utilisation systématique avec saisie de données confidentielles.

Évaluer régulièrement les besoins des équipes en matière d'IA pour adapter l'offre d'outils approuvés et réduire l'incitation au shadow AI.

Cadre juridique

Référence	Objet
Art. L.121-1	Contrat de travail, obligations réciproques employeur-salarié
Art. L.121-4	Règlement intérieur, cadre des obligations du salarié
Art. L.124-10	Faute grave justifiant le licenciement immédiat
RGPD - Article 5	Principes de traitement des données personnelles
RGPD - Articles 44-49	Transferts de données hors UE
Art. L.261-1	Traitement de données à caractère personnel en milieu professionnel
Loi du 26 juin 2019	Protection du secret des affaires (transposition directive 2016/943/UE)

Le shadow AI constitue l'un des risques les plus concrets et les plus immédiats de l'IA en entreprise. La majorité des salariés qui utilisent des outils d'IA non autorisés le font par commodité et sans intention de nuire, mais les conséquences juridiques sont identiques.

L'employeur doit adopter une approche de **responsabilisation** plutôt que d'interdiction, en mettant à disposition des outils sécurisés et en formant les salariés aux enjeux. L'expérience montre que les entreprises qui proposent des alternatives approuvées réduisent significativement le recours au shadow AI.