

# Quels sont les risques juridiques liés à l'utilisation de l'IA générative en entreprise ?

## Réponse courte

L'utilisation de l'IA générative (ChatGPT, Copilot, Gemini) en entreprise au Luxembourg expose l'employeur à des risques juridiques dans quatre domaines principaux : la **confidentialité des données** (saisie d'informations sensibles dans des outils externes), la **propriété intellectuelle** (statut incertain des contenus générés), la **conformité obligations RGPD** (traitement de données personnelles par des tiers) et la **fiabilité des résultats** (hallucinations et contenus inexacts).

L'employeur est responsable des contenus produits et diffusés par ses salariés, même lorsqu'ils sont générés par l'IA. L'absence de **charte d'utilisation** et de **formation** expose l'entreprise à des fuites de données, des violations de droits d'auteur, des **sanctions CNPD** et des atteintes à sa réputation.

## Définition

L'**IA générative** désigne les systèmes d'intelligence artificielle capables de créer du contenu original (texte, image, code, audio, vidéo) à partir de modèles entraînés sur de vastes corpus de données. En entreprise, ces outils sont utilisés pour la rédaction de documents, la programmation, l'analyse de données, la création de contenus marketing et l'assistance aux processus décisionnels.

Les risques juridiques spécifiques à l'IA générative découlent de sa nature même : les données saisies peuvent être **stockées et réutilisées** par le fournisseur, les contenus générés peuvent contenir des éléments **protégés par le droit d'auteur**, et les résultats peuvent être **factuellement inexacts** (hallucinations).

## Questions fréquentes

### Comment encadrer l'IA générative plutôt que l'interdire en entreprise ?

Déployer des solutions entreprise avec garanties contractuelles (non-réutilisation des données, localisation UE, conformité RGPD), adopter une charte d'utilisation, classifier les données autorisées, former les salariés et imposer une relecture humaine de tout contenu avant diffusion.

### Qu'est-ce que le shadow AI et quels risques pose-t-il pour l'entreprise ?

Le shadow AI désigne l'utilisation clandestine d'outils d'IA générative par les salariés sans cadre ni autorisation. Il expose à des fuites de données, violations RGPD et risques de contrefaçon. Une charte IA structurée et une formation préviennent ce phénomène.

### Que sont les hallucinations de l'IA générative ?

Les hallucinations sont des productions factuellement fausses générées avec un haut degré d'apparente crédibilité : références juridiques inexistantes, données chiffrées erronées, citations inventées. Toute information produite par l'IA générative doit être vérifiée avant diffusion ou utilisation professionnelle.

### Quelles données ne jamais saisir dans un outil d'IA générative public ?

Les données personnelles de salariés ou clients, les secrets d'affaires, les données financières non publiées, les stratégies commerciales et tout document classifié confidentiel. Les versions grand public stockent et peuvent réutiliser ces données pour entraîner leurs modèles.

### Quelles obligations l'AI Act impose-t-il aux modèles d'IA générative ?

L'article 52 impose des obligations de transparence pour les systèmes générant du contenu (étiquetage, identification IA). Les articles 53 à 56 fixent les obligations pour les modèles d'IA à usage général (GPAI), avec des exigences renforcées pour les modèles à risque systémique.

### Quels sont les principaux risques juridiques de l'IA générative en entreprise ?

Quatre domaines : la confidentialité des données saisies, la propriété intellectuelle des contenus générés, la conformité RGPD (transferts hors UE) et la fiabilité des résultats (hallucinations). L'employeur reste responsable des contenus produits et diffusés par ses salariés via ces outils.

## Conditions d'exercice

Les risques juridiques de l'IA générative se répartissent en plusieurs catégories.

Risque	Détail
<b>Confidentialité</b>	Saisie de données confidentielles (secrets d'affaires, données clients, stratégies) dans des outils d'IA générative dont les serveurs sont hors UE ; risque de fuite et de réutilisation des données par le fournisseur
<b>RGPD</b>	Traitement de données personnelles par un tiers sans base juridique, sans contrat de sous-traitance et potentiellement en violation des règles de transfert hors UE
<b>Propriété intellectuelle</b>	Statut juridique incertain des contenus générés (non protégeables par le droit d'auteur en l'état actuel) ; risque de contrefaçon si le contenu reproduit des œuvres protégées
<b>Fiabilité</b>	Hallucinations (informations factuellement fausses), références juridiques inexistantes, données chiffrées erronées ; responsabilité de l'employeur si ces contenus sont diffusés
<b>AI Act</b>	Les modèles d'IA générative (GPAI) sont soumis à des obligations de transparence spécifiques (article 52) et, pour les modèles à risque systémique, à des obligations renforcées
<b>Responsabilité employeur</b>	L'employeur est responsable des contenus diffusés par ses salariés, y compris ceux générés par l'IA, sur le fondement de la responsabilité du commettant

## Modalités pratiques

La gestion des risques de l'IA générative nécessite un cadre structuré.

Mesure	Détail
<b>Charte IA</b>	Adopter une charte d'utilisation définissant les outils autorisés, les cas d'usage permis et interdits, les données ne pouvant être saisies
<b>Classification des données</b>	Établir une classification des données de l'entreprise (public, interne, confidentiel, secret) et interdire la saisie des données classifiées au-delà du niveau autorisé
<b>Solutions approuvées</b>	Déployer des versions entreprise (API privée, garantie de non-réutilisation des données) plutôt que des versions grand public
<b>Vérification systématique</b>	Imposer une relecture humaine de tout contenu généré par l'IA avant diffusion ou utilisation
<b>Formation</b>	Former les salariés aux risques spécifiques de l'IA générative et aux bonnes pratiques d'utilisation
<b>Monitoring</b>	Surveiller les usages pour détecter les saisies de données sensibles et les utilisations non conformes

## Pratiques et recommandations

**Déployer** des solutions d'IA générative entreprise avec des garanties contractuelles de non-réutilisation des données saisies, de localisation du traitement dans l'UE et de conformité RGPD, plutôt que de laisser les salariés utiliser des versions grand public sans contrôle.

**Interdire** explicitement la saisie de données personnelles de salariés, de clients ou de partenaires, de secrets d'affaires, de données financières non publiées et de tout document classifié confidentiel dans les outils d'IA générative non approuvés.

**Instaurer** un processus de validation obligatoire pour tout contenu généré par l'IA destiné à être diffusé à l'extérieur de l'entreprise (communications clients, documents contractuels, publications), avec une vérification factuelle et juridique.

**Sensibiliser** les salariés au phénomène d'hallucination de l'IA générative et à la nécessité de vérifier systématiquement les informations, références juridiques et données chiffrées produites par ces outils.

## Cadre juridique

Référence	Objet
<b>RGPD - Article 5</b>	Principes de traitement des données (licéité, minimisation, sécurité)
<b>RGPD - Articles 44-49</b>	Transferts de données personnelles hors UE
<b>RGPD - Article 28</b>	Obligations en cas de sous-traitance du traitement
<b>AI Act - Article 52</b>	Obligations de transparence pour les systèmes d'IA générative (GPAI)
<b>AI Act - Articles 53-56</b>	Obligations pour les fournisseurs de modèles d'IA à usage général
<b>Directive (UE) 2019/790</b>	Directive droit d'auteur, exception de fouille de textes et données
<b>Loi luxembourgeoise du 18 avril 2001</b>	Droit d'auteur et droits voisins au Luxembourg

L'IA générative représente un défi juridique inédit car elle brouille les frontières entre création humaine et production algorithmique, entre données internes et données partagées avec des tiers. L'absence de cadre juridique stabilisé sur la **propriété intellectuelle** des contenus générés impose une approche de prudence.

L'employeur doit anticiper les risques en mettant en place un cadre d'utilisation structuré plutôt que d'interdire l'IA générative, ce qui conduirait les salariés à l'utiliser de manière clandestine et non contrôlée (**shadow AI**).

Les contenus sont rédigés et mis à jour régulièrement à partir de sources officielles. Leur usage ne remplace pas une consultation juridique et doit être validé par un professionnel du droit.