N°5 IA NEWSLETTER

Mars 2026

Top News

LES RISQUES DE L'IA EN ENTREPRISE

La croissance fulgurante de l'utilisation de l'IA en entreprise génère aujourd'hui des gains de productivité indéniables. Si les managers (et plus largement l'ensemble des collaborateurs) reconnaissent désormais son impact concret dans le quotidien professionnel, les risques liés à cet essor restent encore largement méconnus.

Dans ce numéro, nous avons **identifié les principaux risques** auxquels les entreprises s'exposent lors de l'intégration de l'IA : manque contrôle, défauts d'accompagnement et de formations, etc, ainsi que **les mesures à prendre pour y limiter ces risques.**

H4 Partners & l'IA

LES RISQUES DE L'IA

La plupart des entreprises, en particulier les grands groupes, se sont déjà emparées du sujet de l'Intelligence Artificielle : après l'avoir expérimentée, elles l'utilisent et l'intègrent désormais à leurs activités. Cette adoption, aujourd'hui portée principalement par les managers, ouvre toutefois la voie à de nouveaux risques, poussant les organisations à accorder une attention croissante à la sécurisation de ses usages.

L'adoption rapide des outils d'IA générative transforme les pratiques professionnelles, mais elle s'accompagne de nouveaux risques souvent sous-estimés. Pour les organisations, **l'enjeu n'est pas de freiner l'usage de l'IA, mais d'en comprendre les limites afin d'en sécuriser l'exploitation.**

Risques techniques et opérationnels

Les **risques techniques** concernent directement la **fiabilité des modèles et leurs impacts sur les processus internes**. On y entend notamment

Erreurs et biais algorithmiques : les modèles génératifs peuvent produire des informations factuellement incorrectes (dites **"hallucinations"**) ou **reproduire des biais** présents dans leurs données d'entraînement. Concrètement, cela peut affecter la qualité des analyses réalisées, des évaluations et les décisions qui en découlent.

📒 Cas réel : En 2025, Deloitte Australia a ainsi été condamné à une amende d'environ 400 000 $ pour avoir réalisé un rapport généré par IA contenant des informations fabriquées, des citations inventées et des éléments de données faux.

Impact sur la confiance et la réputation : Une enquête IBM (2025) souligne que 42 % des entreprises ont déjà constaté un impact sur la confiance des clients lié à un usage non transparent de l'IA. Cela montre que le risque n'est pas uniquement technique : il **devient aussi réputationnel lorsqu'un client découvre que des décisions ou communications ont été automatisées sans encadrement clair**.

📒 Etude étude menée par Usercentrics (2025) : montre que **70 % des consommateurs n'ont pas confiance dans les entreprises pour utiliser l'IA de façon responsable**, et que 81 % supposent que leurs données sont utilisées sans consentement explicite.

Dépendance technologique et responsabilité : le recours croissant à des solutions externes d'IA générative pose également de nouveaux enjeux sur la maîtrise des données utilisées, la dépendance à des outils tiers, mais aussi en termes de responsabilité juridique en cas d'erreur issue d'une décision partiellement automatisée. **L'utilisation de l'IA ne déplace pas la responsabilité juridique** : l'entreprise demeure pleinement responsable des décisions prises, même lorsque celles-ci s'appuient sur des recommandations générées par un modèle.

📒 Cas réel : Une action collective a été engagée contre Workday pour discrimination (sur l'âge) imputée à son système d'IA de présélection des candidats. Cette procédure témoigne de la responsabilité de l'entreprise devant les tribunaux dans les décisions automatisées.

Risques de sécurité et de conformité

Au-delà de la performance des modèles, l'IA introduit de nouveaux **enjeux de cybersécurité et de gouvernance des données.**

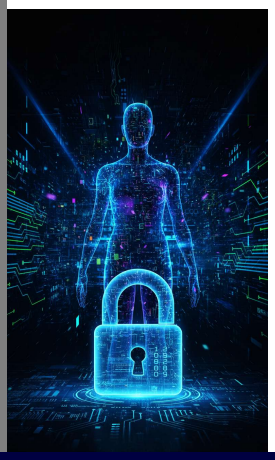
Shadow AI : le risque invisible

Un phénomène croissant concerne **l'usage d'outils d'IA non validés par l'entreprise**. Beaucoup d'entreprises, notamment parmi les plus petites structures, ne sont pas encore en mesure de mettre à disposition de leurs employés des solutions d'IA, poussant de nombreux collaborateurs, à utiliser des solutions grand public.

Conséquences possibles :

- insertion de données confidentielles dans des plateformes externes,
- absence de contrôle sur le stockage ou la réutilisation des informations,
- impossibilité pour l'entreprise de maîtriser ses flux de données.

📓 Cas réel : En janvier 2026, le directeur par intérim de l'Agence de cybersécurité américaine (CISA) a téléchargé des documents sensibles vers une version publique de ChatGPT non approuvée par son organisation, conduisant à une enquête interne.



LE SAVIEZ-VOUS ?

Après la victoire de son programme Deep Blue contre le champion du monde d'échecs Garry Kasparov en 1997, IBM a été l'une des premières entreprises à intégrer l'IA dans ses processus internes pour optimiser la maintenance, analyser les données clients et améliorer la prise de décision.

Risques réglementaires (RGPD, IA Act)

L'usage de l'IA implique de nouvelles obligations : traçabilité des décisions, transparence des traitements et maîtrise des données personnelles. Une utilisation mal encadrée peut rapidement créer un risque de non-conformité, avec des conséquences financières et réputationnelles.

📓 Cas réel : La société DeepSeek a été visée par une plainte auprès de l'Autorité belge de protection des données pour avoir transféré illégalement des données personnelles d'utilisateurs européens vers des serveurs situés en Chine, en dehors des dispositifs garantissant la conformité au RGPD.

Exposition accrue aux cyber-risques

Selon une étude PwC (2024), près de 68 % des dirigeants estiment que l'IA expose leur organisation à de nouveaux risques, notamment :

- fuites ou divulgations involontaires de données sensibles,
- augmentation des surfaces d'attaque cyber : chaque nouveau service ou API connectée à un outil d'IA peut constituer un point d'entrée potentiel pour des cyberattaquants ;
- génération automatisée de contenus trompeurs ou malveillants : par exemple, la création involontaire de données financières incorrectes ou d'instructions frauduleuses générées par l'IA

Le risque vient souvent des usages informels des employés plutôt que des outils eux-mêmes.

SECURISER L'IA

À retenir

Réduire les risques liés à l'IA repose moins sur la technologie elle-même que sur la qualité de son déploiement organisationnel. Les entreprises les plus avancées combinent :

- des outils sécurisés et officiels,
- une gouvernance claire au niveau dirigeant,
- une formation large des équipes,
- une intégration directement au sein des processus métiers

1 **Fournir des outils d'IA sécurisés et adaptés**

Selon l'enquête mondiale « AI at Work » du Boston Consulting Group (BCG), lorsque les collaborateurs ne disposent pas des outils d'IA dont ils ont besoin, plus de la moitié déclarent qu'ils chercheront des alternatives et les utiliseront malgré tout. Proposer des outils officiels, simples d'accès et utiles pour éviter les contournements demeure ainsi l'un des enjeux clés de l'implémentation de l'IA au sein des entreprises.

2 **Accompagner les dirigeants dans la gouvernance de l'IA**

Le déploiement de l'IA ne peut pas reposer uniquement sur les équipes techniques. Il nécessite une implication forte du management. Les dirigeants doivent notamment chercher à établir une politique claire sur son usage, identifier les cas d'usages prioritaires et mettre en place des dispositifs de contrôle adaptés.

3 **Former les équipes**

La formation constitue aujourd'hui l'un des leviers les plus efficaces pour réduire les risques. Elle doit couvrir : les limites des modèles (hallucinations, biais), les bonnes pratiques de confidentialité, les règles internes d'utilisation.

4 **Accélérer l'intégration réelle des agents IA dans les workflows**

Malgré l'engouement autour de l'IA, l'intégration opérationnelle reste encore limitée. Selon l'étude BCG, seuls 13 % des employés perçoivent aujourd'hui l'IA comme profondément intégrée à leurs flux de travail quotidiens. L'enjeu n'est donc plus seulement d'expérimenter, mais de l'intégrer pleinement dans les processus relatifs aux différents métiers.

+75 %
des managers utilisent l'IA générative quotidiennement

51%
des autres collaborateurs utilisent l'IA générative quotidiennement

+872M
de violations de pertes de données enregistrées
(rapport 2025 Zscaler ThreatLabz)

LE MUR DES CAS IA

4 exemples d'utilisation mal maîtrisée de l'IA : à vous de retrouver le risque dominant associé à chacun …

Dans une affaire fédérale à New York, deux avocats ont soumis une requête contenant des jurisprudences inventées par l'IA (ChatGPT) lors d'un procès contre la compagnie aérienne Avianca. Après que ces faux ont été découverts, l'affaire a été rejetée et les avocats ont été sanctionnés par une amende de 5 000 $.

Réponse : erreurs et biais algorithmiques (hallucinations)

En mars 2025, un prestataire travaillant pour le gouvernement d'un état australien a téléchargé sur ChatGPT un fichier Excel contenant des données sensibles de 3 000 personnes. C'est plus de 12 000 lignes d'informations personnelles (noms, adresses e-mail, numéros de téléphone, etc.) qui ont fuitées.

Réponse : Shadow IA

L'entreprise américaine Clearview AI a développé une IA de reconnaissance faciale en collectant des milliards de photos sur internet et les réseaux sociaux sans le consentement des personnes. En 2022, cette pratique a été sanctionnée en France pour non-respect du RGPD et a conduit à la suppression des données concernant les citoyens français.

Réponse : risques réglementaires

En 2025, Tesla a été reconnue partiellement responsable d'un accident mortel impliquant son système d'assistance à la conduite Autopilot, en partie basé sur l'IA, et a été condamnée à verser 243 millions de dollars de dommages et intérêts aux victimes.

Réponse : dépendance technologique et responsabilité

SOURCES :

- *Deloitte To Repay Australian Government After AI Errors Found In Official Report* — NDTV
- *The State of Digital Trust in 2025* — Usercentrics
- *Job applicants can't bring disparate impact age bias claims, Workday argues* — HR Dive
- *Trump's acting cyber chief uploads sensitive files to public ChatGPT* – TRT World
- *Italian data privacy agency probes China's DeepSeek AI, as EU tests GDPR compliance* — Euronews
- *PwC's 2024 Global Digital Trust Insights Survey* — PwC
- *Judge Fines Two Lawyers For Using Fake Cases From ChatGPT* — Forbes
- *NSW flood victims' personal details loaded to ChatGPT in major data breach* – ABC News
- *Facial recognition: the French SA imposes a penalty payment on CLEARVIEW AI* – EDPB
- *Tesla rejected $60 million settlement before losing $243 million Autopilot verdict* – Reuters