

GUIDE PRATIQUE · 2026

IA Locale de A à Z

Utiliser l'IA sur sa machine et mieux contrôler ses données

Daniel Lumbroso

Fondateur de DannyAI.fr · Consultant IA

Sommaire

Module 0 — L'IA en entreprise : comprendre les risques

- Les chiffres clés en 2026
- Ce que les équipes peuvent faire sans le savoir
- Incidents documentés
- Ce que prévoient le RGPD et l'AI Act
- Une approche de réduction des risques

Module 1 — Comprendre l'IA locale

- IA cloud et IA locale : les différences réelles
- Ce qui se passe avec un service cloud
- Ce qui se passe avec une IA locale
- Les limites de l'IA locale

Module 2 — Installer son IA locale pas à pas

- Choisir sa machine et son environnement
- Installer Ollama et LM Studio
- Choisir et vérifier son modèle
- Configurer un fonctionnement hors ligne

Module 3 — Utiliser l'IA locale dans son quotidien pro

- Rédiger et résumer des documents sans cloud
- Analyser des fichiers sensibles en local
- Préparer des e-mails et comptes rendus
- Cas d'usage par métier

Module 4 — Sécuriser son environnement IA

- Chiffrement des fichiers et du disque
- Gestion des accès et des journaux
- Bonnes pratiques et erreurs à éviter
- Sauvegardes et mises à jour

Module 5 — Auditer et documenter sa conformité

- RGPD : ce que vous devez documenter
- AI Act : identifier vos obligations
- Checklist de conformité en 30 points
- Comment prouver sa démarche à un client ou auditeur

Bonus — Prise en main de AuditRGPD Pro et QuickMatch

- AuditRGPD Pro : réaliser son premier audit en 15 minutes

QuickMatch : trier des candidatures sans exposer les CV

Cas pratiques en situation réelle

Avant d'installer quoi que ce soit, il faut comprendre les risques liés à l'utilisation d'outils d'IA avec des données professionnelles. L'IA locale n'est pas une solution magique : c'est une approche qui peut réduire certains transferts de données, à condition d'être correctement configurée, sécurisée et documentée.

1. Les chiffres clés en 2026

Ces chiffres ne mesurent pas tous la même chose : une violation de données, un compte compromis et une personne concernée sont des notions différentes.



Selon le rapport IBM, le coût moyen mondial s'élevait à 4,44 millions de dollars en 2025. Ce montant est une moyenne statistique et ne prédit pas le coût d'un incident pour une entreprise donnée. Selon Surfshark, 43,4 millions de comptes associés à la France auraient été compromis au premier semestre 2026, sans que ce chiffre permette de déduire le nombre exact de personnes concernées.

L'IA peut aider à détecter certaines menaces, mais elle peut aussi accélérer la production de contenus malveillants. La sécurité repose sur plusieurs mesures complémentaires, pas sur un seul outil.

2. Ce que les équipes peuvent faire sans le savoir

Le risque ne vient pas uniquement de l'extérieur. Les usages non encadrés au quotidien peuvent exposer des données professionnelles sans que les utilisateurs en aient conscience.

Un contrat copié dans un service d'IA

Le contenu peut être traité par l'infrastructure du fournisseur selon les conditions de l'offre, les paramètres du compte, la durée de conservation et les engagements contractuels applicables.

Des CV envoyés dans un outil RH

Noms, coordonnées et parcours professionnels peuvent être traités par un prestataire externe. Il faut vérifier la base juridique, l'information des candidats, les transferts éventuels, la conservation et les mesures de sécurité.

Des données comptables dans un outil cloud

Chiffre d'affaires, clients et marges peuvent être transmis au fournisseur. Avant tout envoi, il faut vérifier si le traitement est autorisé, nécessaire et correctement encadré.

Du code source dans un assistant de développement

Le code envoyé peut contenir des secrets, des clés API, des identifiants ou de la logique métier. Il faut utiliser des outils et paramètres adaptés à l'environnement professionnel.

3. Incidents documentés

Ces exemples illustrent des risques réels. Ils ne permettent pas de conclure que tous les services d'IA cloud présentent le même niveau de risque.

Samsung, 2023

Samsung a indiqué que des employés avaient transmis du code et des informations internes à ChatGPT. L'entreprise a ensuite renforcé ses restrictions. Cet exemple illustre le risque d'un usage non encadré.

Secteur de la santé

L'utilisation d'un outil d'IA avec des données patients doit faire l'objet d'une analyse spécifique, d'une base juridique appropriée, de mesures de sécurité adaptées et d'une documentation complète.

Administrations et grandes organisations

Les outils non référencés, les mauvaises configurations et les accès insuffisamment contrôlés peuvent fragiliser un système d'information. L'inventaire des outils d'IA et la formation des utilisateurs doivent faire partie de la gouvernance informatique.

4. Ce que prévoient le RGPD et l'AI Act

RGPD

Si un fournisseur d'IA traite des données personnelles pour votre compte, vous devez vérifier le rôle des parties, le cadre contractuel applicable, les transferts internationaux, les durées de conservation et les mesures de sécurité. Lorsque le fournisseur agit comme sous-traitant, un contrat conforme à l'article 28 du RGPD peut être nécessaire. Les violations les plus graves peuvent entraîner une amende pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial.

AI Act

Le règlement européen sur l'intelligence artificielle applique des obligations différentes selon le type de système et son usage. La qualification doit être vérifiée au cas par cas. L'AI Act ne signifie pas que toute utilisation d'un outil d'IA dans les domaines RH, santé ou finance est automatiquement classée à haut risque.

5. Une approche de réduction des risques

Réduire les transmissions inutiles de données est l'un des moyens de limiter certains risques. Cela ne remplace ni le chiffrement, ni le contrôle des accès, ni les sauvegardes, ni la formation des utilisateurs, ni la documentation de conformité.

Ce qu'une configuration locale peut apporter :

✓ Réduction de certaines transmissions vers des fournisseurs externes

✓ Meilleur contrôle de l'environnement de traitement

✓ Possibilité de fonctionner hors ligne après installation

✓ Réduction de la dépendance aux politiques de conservation d'un fournisseur

Ce qu'elle ne garantit pas automatiquement :

! La sécurité du poste informatique

! La sécurité des fichiers temporaires et des journaux

! La conformité RGPD ou AI Act

! L'absence de logiciel malveillant

! L'exactitude des réponses générées

Une IA locale peut améliorer le contrôle des données, mais ses résultats et son niveau de sécurité dépendent du matériel, du logiciel, du modèle et de la configuration.

1. IA cloud et IA locale : les différences réelles

	IA cloud	IA locale
Traitement	Infrastructure du fournisseur	Votre machine ou serveur
Données	Transmises selon la configuration	Peuvent rester en local
Contrôle	Dépend de l'offre et du contrat	Plus important, selon configuration
Confidentialité	Dépend du fournisseur et réglages	Peut être renforcée
Internet	Généralement nécessaire	Peut être évité après install.
Coût	Abonnement ou facturation usage	Matériel + maintenance
RGPD	Vérifications contractuelles nécessaires	Obligations RGPD maintenues*
Maintenance	Gérée par le fournisseur	À assurer en interne
Risques	Transfert, fournisseur compromis	Poste, fichiers, modèle local

* Le local réduit les risques liés à la transmission vers un fournisseur tiers, mais ne supprime pas les obligations RGPD. Certaines offres cloud pro (Azure OpenAI, Google Workspace Enterprise) proposent des engagements de non-utilisation des données.

2. Ce qui se passe avec un service cloud

Lorsque vous envoyez un texte à un service d'IA cloud :

- 1 Transmission de la requête vers l'infrastructure du fournisseur.
- 2 Traitement de la requête par le modèle.
- 3 Conservation éventuelle dans des journaux ou un historique, selon l'offre et les paramètres.
- 4 Utilisation éventuelle pour l'amélioration du service, selon les conditions applicables.

3. Ce qui se passe avec une IA locale

Dans une configuration strictement hors ligne, la requête peut être traitée localement sans transmission vers un fournisseur distant. Elle peut néanmoins rester présente dans la mémoire, les fichiers temporaires, les journaux ou les sauvegardes de la machine.

La protection dépend de la configuration complète : système d'exploitation, contrôle des accès, chiffrement, réseau, logiciels installés et sauvegardes.

4. Les limites de l'IA locale

Une IA locale peut nécessiter un ordinateur puissant, davantage de maintenance et une gestion attentive des mises à jour. Elle peut aussi produire des réponses inexactes.

Le fait qu'un modèle soit local ne garantit ni sa fiabilité, ni sa légalité, ni son absence de biais, ni la conformité du traitement réalisé avec les données personnelles.

Ce guide couvre les modules 0 et 1. Les modules suivants font partie de la formation complète disponible sur DannyAI.fr : installation pas à pas, remplacement des outils cloud, sécurisation, automatisation locale et checklist d'audit.

Ce guide couvre les modules 0 et 1. Les modules suivants font partie de la formation complète disponible sur DannyAI.fr.

Accéder à la formation complète sur DannyAI.fr

contact@dannyai.fr

Avertissement et sources

Avertissement important

Ce guide fournit des informations générales et des méthodes pratiques. Il ne constitue pas un conseil juridique, un audit de sécurité, une certification de conformité ou une garantie d'absence de fuite de données. Les obligations applicables dépendent de votre activité, des données traitées, des fournisseurs utilisés, de la configuration technique et du rôle de chaque intervenant. Pour une situation à risque, demandez l'avis d'un professionnel qualifié.

Sources

- CNIL, rapport annuel 2025.
- CNIL, ressources relatives aux violations de données et à la sécurité.
- IBM, Cost of a Data Breach Report 2025.
- Surfshark, étude sur les comptes compromis au premier semestre 2026.
- Règlement (UE) 2016/679, notamment les articles 28 et 83.
- Règlement (UE) 2024/1689 établissant des règles harmonisées concernant l'intelligence artificielle.
- Documentation officielle des logiciels et modèles utilisés dans la formation.