

AI Act

4 January 2026 • 7 min de lecture

Insights

AI-Act

Décryptage de l'AI Act : Le guide complet article par article

L'**AI Act** (Règlement sur l'intelligence artificielle) est un texte législatif historique de l'UE comprenant **113 articles** et plusieurs annexes. Son objectif n'est pas de réguler la technologie en elle-même, mais l'usage qui en est fait, selon une **approche fondée sur les risques**.

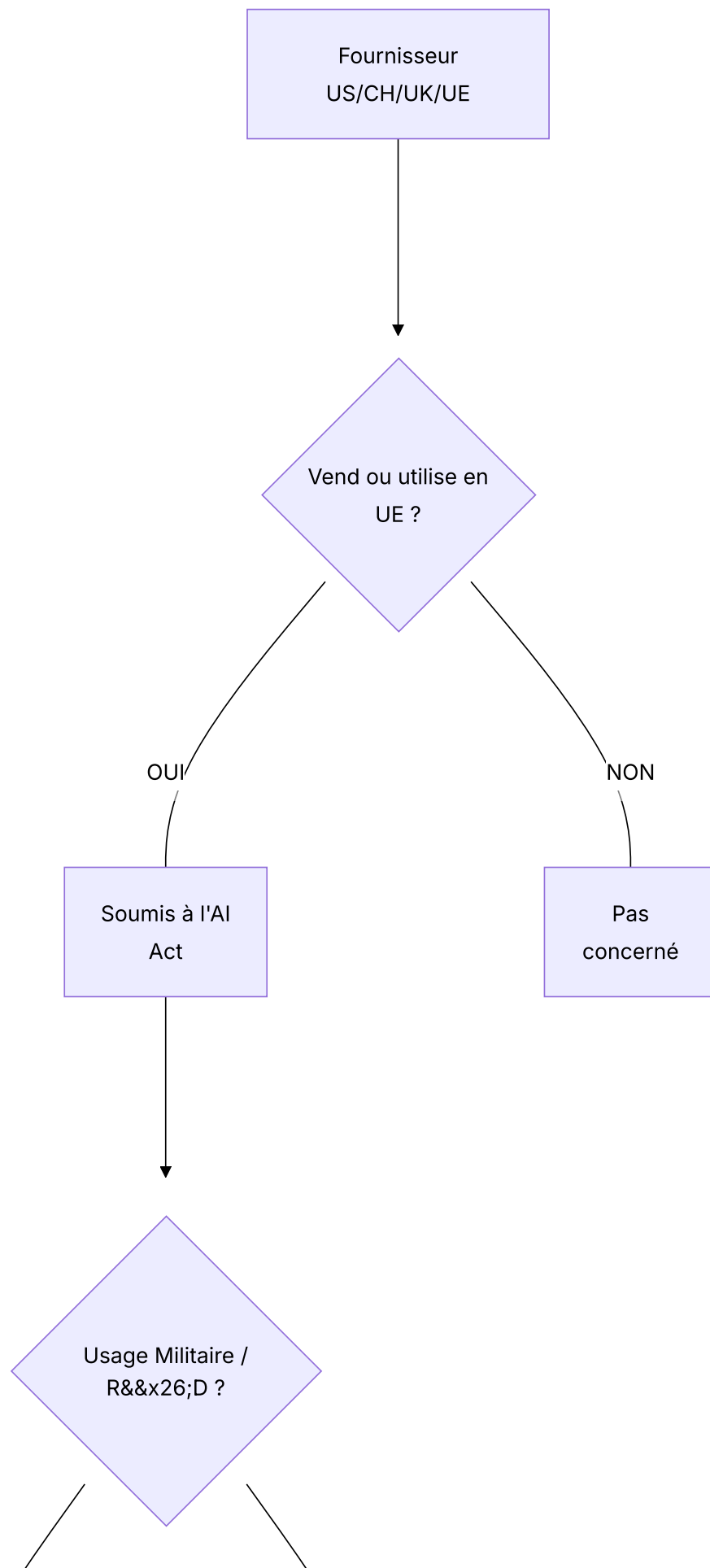
Voici le résumé structuré de l'intégralité du texte pour comprendre les obligations, les interdits et la gouvernance.

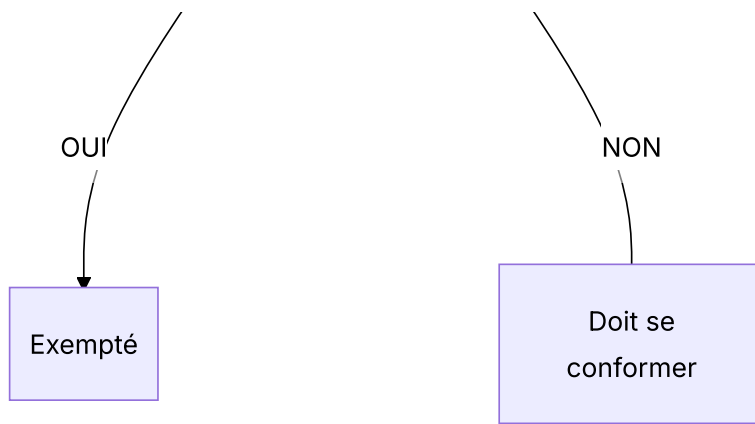
Dispositions Générales (Art. 1 - 4)

Le cadre et le périmètre.

Ce qu'il faut retenir : Le règlement s'applique à **toute IA mise sur le marché européen**, peu importe où le fournisseur est basé (UE ou hors UE).

- **Art. 3 (Définitions)** : L'IA est définie comme un système capable de déduire la manière d'atteindre des objectifs et de générer des résultats (contenu, prédictions, recommandations).
- **Art. 2 (Exclusions)** : Le texte ne s'applique **pas** aux systèmes exclusivement militaires, à la sécurité nationale, ou à la R&D (Recherche et Développement) avant la mise sur le marché. Les systèmes Open Source (sauf GPAI systémiques) bénéficient aussi d'allègements.





Pratiques d'IA Interdites (Art. 5)

La liste rouge : Risque inacceptable.

L'**Article 5** liste les pratiques bannies car elles violent les droits fondamentaux. Aucune certification ne permet de les utiliser (sauf exceptions policières très strictes).

Les 8 Interdictions majeures :

1. **Techniques subliminales** : Manipuler la conscience d'une personne pour altérer son comportement.
2. **Exploitation des vulnérabilités** : Cibler l'âge ou le handicap pour manipuler.
3. **Score Social (Social Scoring)** : Évaluation de la fiabilité des citoyens par des autorités publiques.
4. **Police prédictive** : Évaluer le risque criminel d'une personne uniquement sur son profilage.
5. **Reconnaissance des émotions** : Interdite sur le lieu de travail et dans les établissements d'enseignement.
6. **Catégorisation biométrique sensible** : Dédire race, opinions politiques, religion, orientation sexuelle.
7. **Biométrie à distance en temps réel (Espaces publics)** : Interdite pour la police (sauf terrorisme, recherche de victimes, menace imminente).

8. **Scraping facial** : Créer des bases de données de reconnaissance faciale en aspirant des photos sur internet/CCTV (ex: Clearview AI).

Exemple : Un jouet connecté qui encourage un enfant à des actes dangereux est interdit.

Systèmes d'IA à Haut Risque (Art. 6 - 49)

Le cœur du réacteur réglementaire.

C'est la section la plus dense. Elle concerne les IA critiques qui ont un impact sur la santé, la sécurité ou les droits fondamentaux.

Classification (Art. 6 - 7)

Un système est "Haut Risque" s'il est :

1. Un composant de sécurité d'un produit réglementé (voiture, dispositif médical, ascenseur, aviation).
2. Listé dans l'**Annexe III** :
 - Biométrie.
 - Infrastructures critiques (eau, gaz, élec).
 - Éducation (affectation élèves, notation).
 - Emploi (tri de CV, surveillance employés).
 - Services essentiels (crédit bancaire, assurance vie/santé, urgences).
 - Justice et contrôle aux frontières.

Obligations des Fournisseurs (Providers) (Art. 8 - 25)

Si vous développez une IA à haut risque, vous devez :

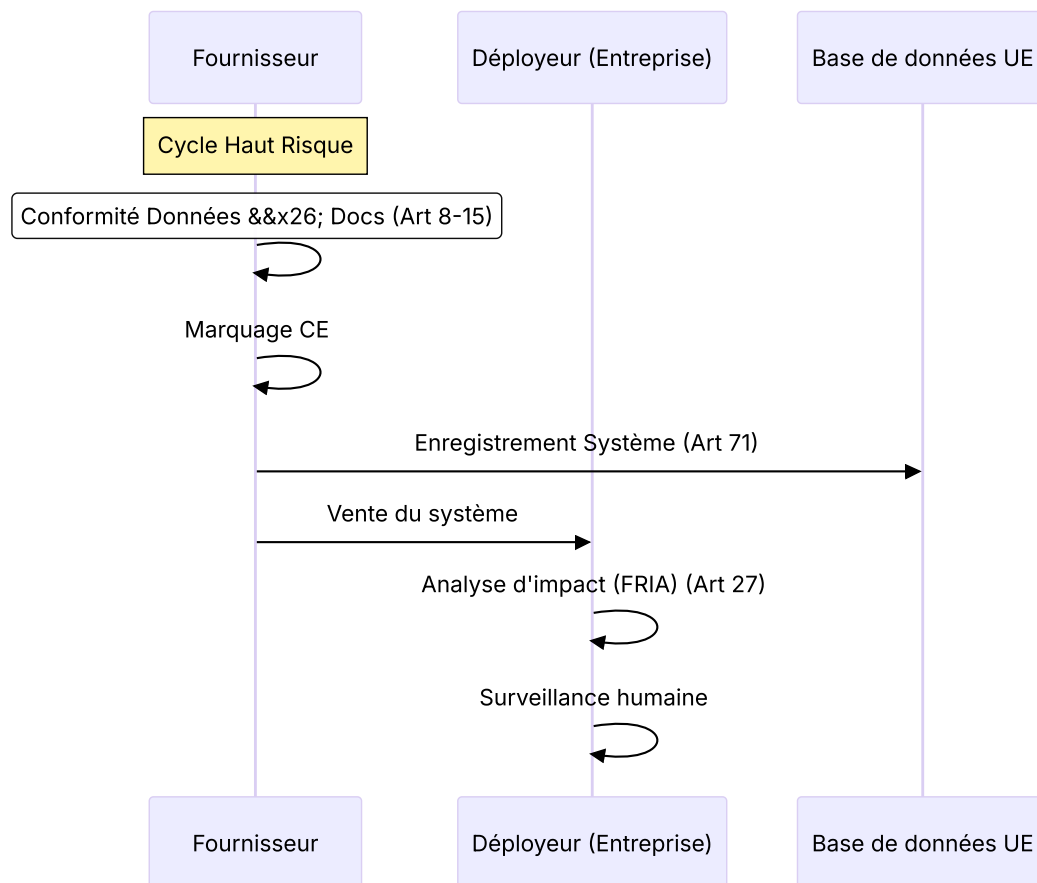
- **Art. 9** : Mettre en place un système de gestion des risques.
- **Art. 10** : Gouvernance des données (les jeux de données d'entraînement ne doivent pas être biaisés).
- **Art. 11** : Documentation technique exhaustive.
- **Art. 13** : Transparence envers l'utilisateur.
- **Art. 14** : Supervision humaine (**Human in the loop**).

- **Art. 15** : Robustesse, précision et cybersécurité.

Obligations des Déployeurs (Utilisateurs Pro) (Art. 26 – 29)

Les entreprises qui achètent et utilisent ces IA (ex: une banque) doivent :

- Utiliser l'IA selon la notice.
- Assurer la surveillance humaine.
- **Art. 27** : Réaliser une **Analyse d'Impact sur les Droits Fondamentaux (FRIA)** avant mise en service (pour les entités publiques et certains acteurs privés).



Obligations de Transparence (Art. 50)

Savoir à qui (ou quoi) on parle.

S'applique aux IA à risque spécifique/limité.

- **Chatbots / Agents conversationnels** : L'utilisateur doit être informé qu'il interagit avec une machine.
- **Deepfakes (Image/Audio/Vidéo)** : Tout contenu généré ou manipulé artificiellement doit être marqué (watermarking) et étiqueté comme tel.
- **Exceptions** : Si le contenu est visiblement artistique, satirique ou parodique (mais des mentions restent recommandées).

Modèles d'IA à Usage Général (GPAI) (Art. 51 - 56)

La régulation des "Fondations" (LLMs).

Cette section vise les modèles comme GPT-4, Claude, Llama, Mistral. Elle distingue deux catégories.

Modèles GPAI "Standard" (Art. 53)

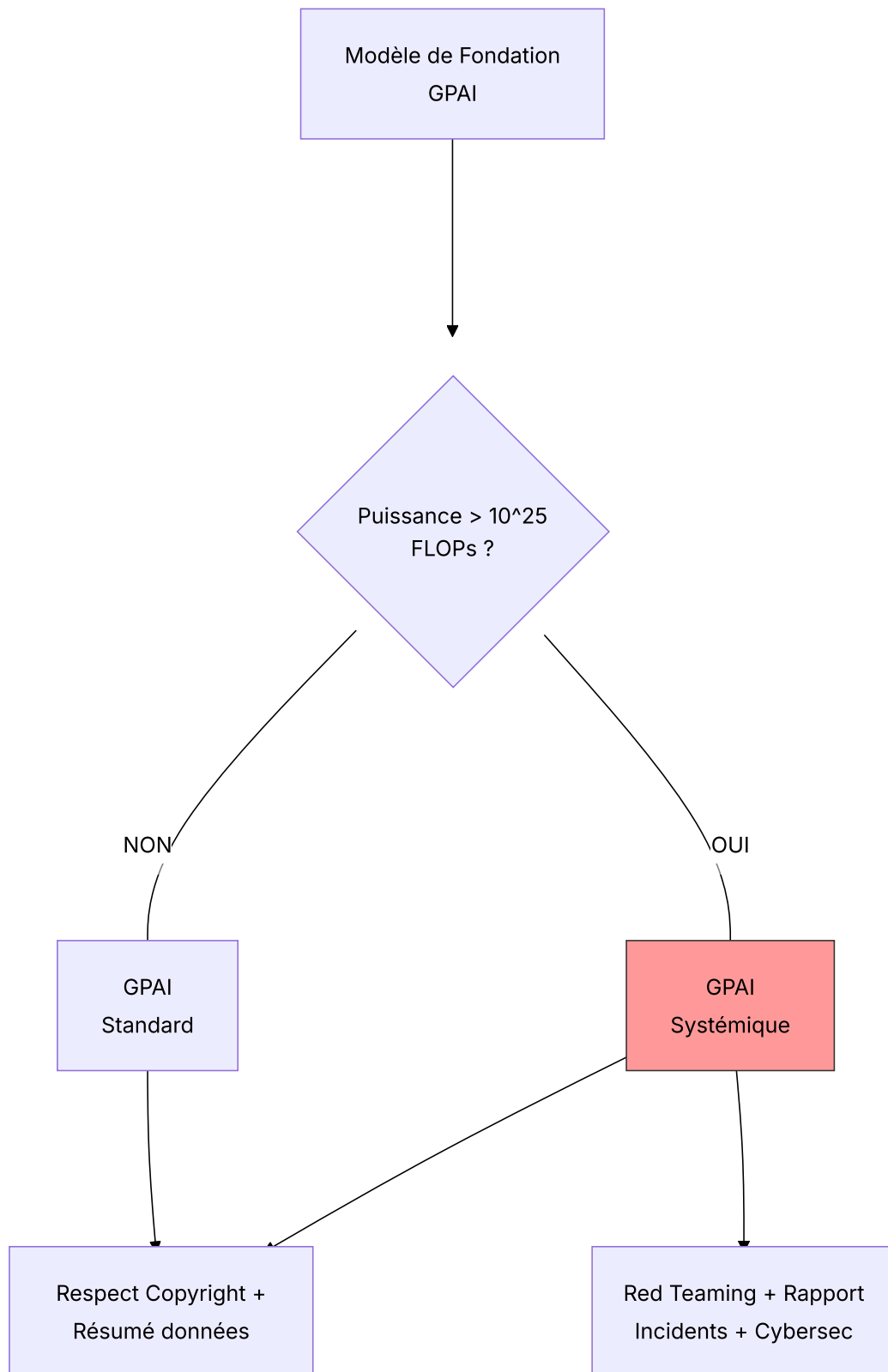
Obligations de base pour tous les modèles.

- Tenir une documentation technique à jour.
- Respecter le **Droit d'auteur** (Copyright UE).
- Publier un **résumé détaillé** des données utilisées pour l'entraînement.

Modèles GPAI à "Risque Systémique" (Art. 55)

Modèles très puissants (puissance de calcul $> 10^{25}$ FLOPs). En plus des obligations standard, ils doivent :

- Effectuer des évaluations contradictoires (**Red Teaming**).
- Évaluer et atténuer les risques systémiques.
- Rapporter les incidents graves au Bureau de l'IA.
- Assurer une cybersécurité de haut niveau.



Soutien à l'Innovation (Art. 57 - 63)

Pour ne pas freiner les startups.

- **Bacs à sable réglementaires (Sandboxes)** : Les États membres doivent créer des environnements contrôlés où les entreprises peuvent tester leurs IA innovantes sous supervision des autorités, avant la mise sur le marché.
- **Tests en conditions réelles (Art. 60)** : Possibilité de tester l'IA hors labo avec des sujets humains, sous conditions strictes (consentement éclairé, droit de retrait).

Gouvernance (Art. 64 - 70)

Qui surveille les IA ?

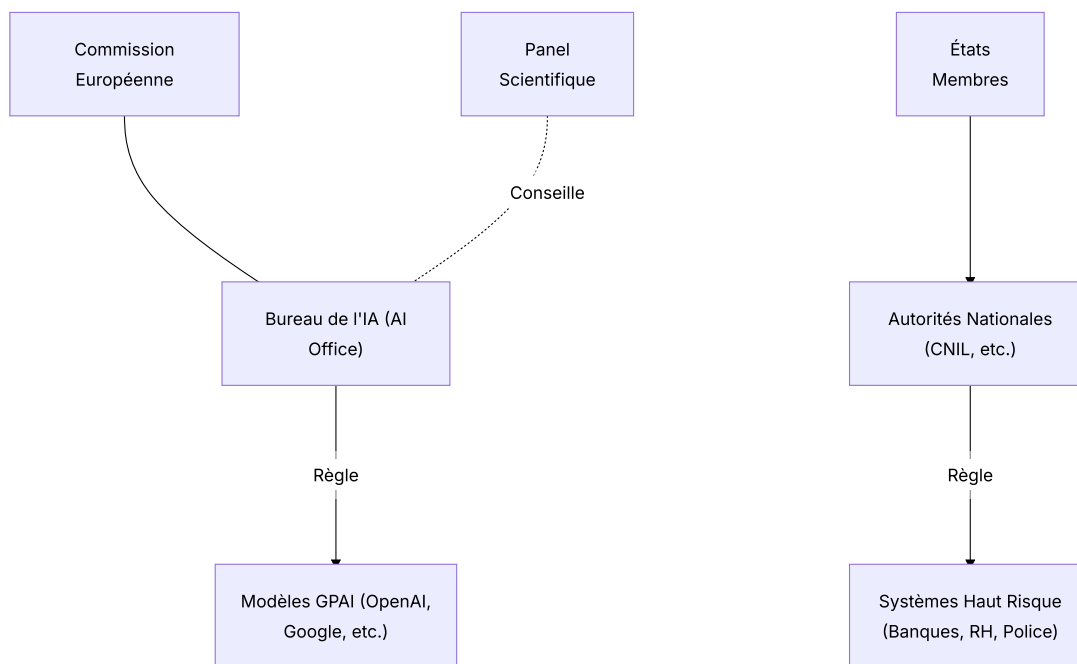
Le système est mixte entre l'UE et les États membres.

1. Au niveau Européen :

- **Bureau de l'IA (AI Office)** : Organe de la Commission. Il régule directement les **modèles GPAI** (les géants de l'IA).
- **Comité européen de l'IA** : Représentants des 27 pays pour harmoniser l'application.
- **Panel scientifique** : Experts indépendants pour alerter sur les risques systémiques.

2. Au niveau National (ex: France) :

- **Autorité de surveillance du marché (ex: CNIL)** : Elle supervise les **systèmes à haut risque** et traite les plaintes des citoyens.



Surveillance post-commercialisation (Art. 71 – 83)

- **Base de données de l'UE (Art. 71)** : Les fournisseurs d'IA à haut risque doivent enregistrer leur système dans une base publique européenne avant le déploiement.
- **Incidents (Art. 73)** : Obligation de signaler tout dysfonctionnement grave ayant entraîné la mort, des dommages corporels ou une violation des droits fondamentaux.

Pénalités et Amendes (Art. 99)

Les sanctions sont dissuasives et calculées sur le chiffre d'affaires (CA) mondial annuel.

| Infraction | Amende Max (Entreprise) | % du CA Mondial |
|--|-------------------------|-----------------|
| Pratiques Interdites (Art 5) | 35 Millions € | 7 % |
| Non-conformité Haut Risque / GPAI | 15 Millions € | 3 % |

| Infraction | Amende Max (Entreprise) | % du CA Mondial |
|--|----------------------------|--------------------|
| Informations inexactes / trompeuses | 7,5 Millions € | 1,5 % |

Calendrier d'Application (Dispositions Finales)

L'AI Act est entré en vigueur en **août 2024**. Son application est progressive :

- **Février 2025** : Application du **Titre II** (Interdictions des pratiques inacceptables).
- **Août 2025** : Application du **Titre V** (Règles pour les modèles GPAI) et des règles de gouvernance.
- **Août 2026** : Application totale du règlement (notamment pour les systèmes à **Haut Risque** de l'Annexe III).
- **Août 2027** : Obligations pour les systèmes à haut risque déjà intégrés dans des produits (voitures, ascenseurs, etc.).

Eric Blaudez - AI Innovation Strategist & Technical Lead
AI Act

© 2026 Eric Blaudez. All rights reserved.

[LinkedIn](#)

Les opinions exprimées sur ce site sont strictement personnelles et ne reflètent pas nécessairement celles de mon employeur. Les contenus sont fournis à titre informatif et ne constituent pas un conseil juridique.