AI Act

La date butoir d'août 2026
et les systèmes d'IA à haut risque

Guide de conformité et d'analyse réglementaire

Introduction

Le 1er août 2024, l'Union européenne a franchi un cap historique avec l'entrée en vigueur du Règlement (UE) 2024/1689, communément appelé « AI Act ». Cette première réglementation mondiale spécifiquement dédiée à l'intelligence artificielle établit un cadre juridique harmonisé pour le développement, la commercialisation et l'utilisation des systèmes d'IA au sein de l'UE[1][2].

Au cœur de ce dispositif réglementaire se trouve une date cruciale : **le 2 août 2026**. Cette échéance marque l'application générale des obligations les plus strictes du règlement, notamment pour les systèmes d'IA à haut risque. Cependant, tous les systèmes à haut risque ne sont pas concernés de la même manière par cette date butoir, et des nuances importantes méritent d'être clarifiées[3][4].

Cet article vise à décrypter précisément le calendrier d'application de l'AI Act, à comprendre quels systèmes d'IA à haut risque sont effectivement concernés par août 2026, et à examiner la situation particulière des robots humanoïdes intégrant de l'intelligence artificielle.

Le calendrier progressif de l'AI Act

L'AI Act ne s'applique pas de manière uniforme à tous les systèmes d'IA dès son entrée en vigueur. Le règlement prévoit un déploiement progressif sur plusieurs années, permettant aux organisations de s'adapter graduellement aux nouvelles exigences[5].

Les étapes clés déjà franchies

2 février 2025 – Interdictions des systèmes à risque inacceptable

Cette première échéance a marqué l'interdiction formelle des systèmes d'IA présentant un risque jugé inacceptable pour les droits fondamentaux et la dignité humaine[6][7]. Sont notamment prohibés :

1. Les systèmes de notation sociale à usage général par les autorités publiques
2. Les techniques de manipulation subliminale visant à altérer substantiellement le comportement des personnes
3. L'exploitation des vulnérabilités de groupes spécifiques (enfants, personnes en situation de handicap)
4. L'identification biométrique à distance en temps réel dans les espaces publics (sauf exceptions strictement encadrées pour les forces de l'ordre)

2 août 2025 – Obligations pour les modèles d'IA à usage général (GPAI)

Les fournisseurs de modèles d'IA à usage général, comme les grands modèles de langage (ChatGPT, Claude, etc.), ont dû commencer à se conformer aux premières obligations de transparence et de documentation[8].

La date butoir cruciale : 2 août 2026

Le **2 août 2026** représente l'échéance majeure de l'AI Act. À partir de cette date, toutes les règles concernant les systèmes d'IA à haut risque devront être strictement respectées[9][10]. Concrètement, cela signifie :

1. Application complète des obligations de conformité pour les systèmes à haut risque listés à l'Annexe III
2. Mise en conformité obligatoire avant toute mise sur le marché de nouveaux systèmes
3. Entrée en vigueur des obligations de transparence pour les systèmes à risque limité
4. Activation des mécanismes de surveillance du marché et début effectif des contrôles

Les échéances ultérieures

2 août 2027 – Systèmes soumis à des réglementations sectorielles existantes

Les systèmes d'IA à haut risque déjà couverts par des législations européennes spécifiques (dispositifs médicaux, véhicules, équipements ferroviaires, aéronautiques, etc.) bénéficient d'un délai supplémentaire de 12 mois. Ces systèmes, listés à l'Annexe I de l'AI Act, devront être conformes au plus tard le 2 août 2027[11][12].

2 août 2030 – Systèmes des administrations publiques

Les systèmes d'IA à haut risque mis en service avant le 2 août 2026 et utilisés par des autorités publiques disposeront d'une période de transition étendue jusqu'au 2 août 2030 pour se mettre en conformité[13].

31 décembre 2030 – Systèmes informatiques à grande échelle

Les systèmes IT à grande échelle listés à l'Annexe X du règlement devront être conformes avant la fin de l'année 2030[14].

Proposition de report : l'incertitude actuelle

En novembre 2025, la Commission européenne a présenté une proposition de « Digital Omnibus on AI » visant à reporter d'un an les obligations pour les systèmes à haut risque, en raison de l'insuffisance des outils de conformité disponibles (normes harmonisées, spécifications communes, lignes directrices)[15]. Selon cette proposition :

1. Les systèmes de l'Annexe III devraient se conformer au plus tard le 2 décembre 2027 (au lieu d'août 2026)
2. Les systèmes de l'Annexe I devraient se conformer au plus tard le 2 août 2028 (au lieu d'août 2027)

Toutefois, cette proposition doit encore être adoptée par le Parlement européen et le Conseil avant août 2026. Dans le cas contraire, les dates originales s'appliqueront, créant une incertitude juridique considérable[16].

Tous les systèmes à haut risque ne sont pas concernés de la même manière

Deux catégories distinctes de systèmes à haut risque

L'AI Act établit une distinction fondamentale entre deux types de systèmes d'IA à haut risque, soumis à des calendriers d'application différents[17][18].

Annexe I : Les produits déjà réglementés (Août 2027)

L'Annexe I concerne les systèmes d'IA intégrés comme composants de sécurité dans des produits déjà soumis à une réglementation européenne sectorielle spécifique[19]. Ces produits incluent :

1. Dispositifs médicaux et dispositifs médicaux de diagnostic in vitro
2. Machines et équipements industriels
3. Véhicules à moteur, tracteurs agricoles et remorques
4. Systèmes ferroviaires
5. Aéronefs et équipements aéronautiques
6. Équipements maritimes
7. Appareils à gaz et équipements sous pression
8. Jouets et équipements électriques
9. Ascenseurs et installations à câbles transportant des personnes
10. Équipements de protection individuelle
11. Systèmes de transport intelligents (STI)

Date d'application : 2 août 2027 (soit 36 mois après l'entrée en vigueur)

Ces systèmes bénéficient d'un délai supplémentaire car ils sont déjà encadrés par des législations sectorielles robustes en matière de sécurité et doivent déjà passer par des évaluations de conformité par des tiers[20].

Annexe III : Les cas d'usage à haut risque (Août 2026)

L'Annexe III identifie des domaines d'application spécifiques où l'utilisation de l'IA présente des risques élevés pour la santé, la sécurité ou les droits fondamentaux des personnes[21][22]. Ces domaines incluent :

1. Identification biométrique et catégorisation des personnes

Systèmes d'identification biométrique à distance, de reconnaissance faciale, d'analyse des émotions (sauf à des fins médicales ou de sécurité).

2. Gestion et exploitation d'infrastructures critiques

IA utilisées comme composants de sécurité pour la gestion de réseaux d'eau potable, de gaz, d'électricité, de chauffage, ou d'infrastructures numériques critiques.

3. Éducation et formation professionnelle

1. Systèmes d'évaluation des acquis d'apprentissage
2. Évaluation du niveau d'éducation approprié pour une personne

3. Détection de plagiat ou de fraude aux examens
4. Surveillance et détection de comportements interdits pendant les examens

4. Emploi, gestion de la main-d'œuvre et accès à l'emploi indépendant

1. Systèmes de recrutement ou de sélection de candidats
2. Prise de décision sur les promotions, résiliations de contrats
3. Répartition des tâches et surveillance des performances
4. Évaluation et prédiction du risque de commission d'infractions par des travailleurs

5. Accès aux services privés essentiels et aux services publics

1. Évaluation de l'éligibilité aux prestations et services d'assistance publics
2. Évaluation de la solvabilité et du risque de crédit (scoring)
3. Évaluation et classification des appels d'urgence (pompiers, SAMU, police)
4. Attribution de priorités dans les services de santé d'urgence

6. Application de la loi

1. Évaluation des risques de victimisation ou de récidive
2. Évaluation de la fiabilité des éléments de preuve
3. Profilage dans le cadre d'enquêtes criminelles
4. Détection et évaluation de la probabilité de commission d'infractions

7. Gestion de la migration, de l'asile et du contrôle des frontières

Évaluation des risques liés aux demandeurs d'asile, détection de faux documents, évaluation des risques de sécurité.

8. Administration de la justice et processus démocratiques

Systèmes d'aide à la recherche et à l'interprétation des faits et du droit, application de la loi à un ensemble concret de faits.

Date d'application : 2 août 2026 (soit 24 mois après l'entrée en vigueur)

Les exceptions importantes de l'article 6(3)

Tous les systèmes listés à l'Annexe III ne sont pas automatiquement considérés comme à haut risque. L'article 6(3) prévoit des **exceptions** lorsqu'un système ne présente pas de risque important de préjudice[23][24]. Un système peut être exclu de la classification à haut risque s'il remplit l'une des conditions suivantes :

1. Le système est destiné à accomplir une **tâche procédurale étroite** (narrow procedural task)
2. Le système est destiné à **améliorer le résultat d'une activité humaine préalablement réalisée**, sans se substituer à elle
3. Le système est destiné à **détecter des constantes ou des écarts** par rapport aux habitudes, sans influencer l'évaluation humaine finale

4. Le système exécute une **tâche préparatoire** en vue d'une évaluation effectuée par un humain

Attention : Cette exception ne s'applique **jamais** aux systèmes effectuant du profilage de personnes physiques[25].

Importante modification proposée : les fournisseurs n'auraient plus l'obligation de publier un résumé justifiant l'application de l'exception article 6(3), réduisant ainsi le risque juridique et réputationnel de cette démarche[26].

Obligations de conformité pour les systèmes à haut risque

Les fournisseurs de systèmes d'IA à haut risque doivent satisfaire à un ensemble d'obligations strictes avant la mise sur le marché européen[27][28].

Système de gestion des risques

Mise en place d'un système complet et continu de gestion des risques tout au long du cycle de vie du système, incluant :

1. Identification et analyse des risques connus et prévisibles
2. Estimation et évaluation des risques pouvant survenir lors de l'utilisation conforme
3. Évaluation d'autres risques pouvant survenir en cas d'utilisation raisonnablement prévisible mais non conforme
4. Adoption de mesures de gestion appropriées et ciblées

Gouvernance et qualité des données

1. Validation de la qualité et de la non-discrimination des ensembles de données d'entraînement
2. Documentation complète des sources de données
3. Mesures pour détecter et corriger les biais
4. Respect du RGPD et des règles de protection des données personnelles

Documentation technique et transparence

1. Rédaction d'une documentation technique détaillée (architecture, algorithmes, données)
2. Notice d'utilisation claire et compréhensible pour les déployeurs
3. Traçabilité : logging automatique des activités du système
4. Conservation des logs pour permettre les contrôles a posteriori

Supervision humaine

Conception du système pour permettre une surveillance humaine effective :

1. Capacité d'intervention humaine pendant l'utilisation du système
2. Possibilité de désactivation ou d'interruption du système

3. Compréhension des capacités et limitations du système par les opérateurs
4. Formation appropriée des utilisateurs

Robustesse, cybersécurité et exactitude

1. Niveau élevé de robustesse technique
2. Résistance aux erreurs, pannes et incohérences
3. Résilience face aux tentatives de manipulation et aux cyberattaques
4. Exactitude, précision et performance appropriées

Évaluation de conformité et marquage CE

1. Réalisation d'une évaluation de conformité (auto-évaluation ou par organisme tiers selon les cas)
2. Établissement d'une déclaration UE de conformité
3. Apposition du marquage CE
4. Enregistrement dans la base de données européenne des systèmes d'IA à haut risque

Surveillance post-commercialisation

1. Mise en place d'un plan de surveillance post-commercialisation
2. Collecte et analyse des données d'utilisation réelle
3. Reporting d'incidents graves aux autorités compétentes
4. Mises à jour et corrections si nécessaire

Quid des robots humanoïdes intégrant de l'IA ?

La question des robots humanoïdes intelligents soulève des interrogations spécifiques dans le cadre de l'AI Act. Bien que le règlement ne mentionne pas explicitement les « robots humanoïdes », son champ d'application les concerne de manière significative[29][30].

Classification des robots humanoïdes

La classification d'un robot humanoïde intégrant de l'IA dépend de plusieurs critères[31][32] :

Critère 1 : Le robot est-il un produit réglementé ?

Si le robot humanoïde entre dans l'une des catégories de produits listées à l'**Annexe I**, il sera soumis au calendrier de cette annexe (août 2027). C'est le cas pour :

1. **Robots industriels** : couverts par le Règlement Machines (UE) 2023/1230
2. **Robots d'assistance médicale** : dispositifs médicaux selon le Règlement (UE) 2017/745
3. **Robots de transport de personnes** : véhicules autonomes

Le **Règlement Machines (UE) 2023/1230**, qui a remplacé la Directive Machines de 2006, intègre désormais explicitement les aspects liés à l'IA et à l'autonomie des machines[33][34]. Il impose :

1. Des évaluations de risques prenant en compte l'autonomie et les comportements auto-évolutifs
2. La prise en compte des interactions homme-robot dans toute la durée de vie
3. Des exigences de sécurité pour les machines intégrant des systèmes d'IA

Critère 2 : Quel est le cas d'usage du robot ?

Si le robot humanoïde n'entre pas dans l'Annexe I mais est utilisé dans l'un des domaines listés à l'**Annexe III**, il sera considéré comme système à haut risque (échéance août 2026). Exemples :

1. **Robot d'accueil et de recrutement** : si utilisé pour sélectionner des candidats → Annexe III point 4
2. **Robot éducatif** : si utilisé pour évaluer les acquis des élèves → Annexe III point 3
3. **Robot de sécurité** : si utilisé pour surveiller et évaluer les comportements → Annexe III point 6
4. **Robot d'assistance sociale** : si utilisé pour attribuer des prestations sociales → Annexe III point 5

Critère 3 : Le système d'IA du robot présente-t-il un risque élevé ?

Même si le robot n'entre ni dans l'Annexe I ni dans l'Annexe III, son système d'IA peut être considéré comme à haut risque s'il présente un risque significatif pour la santé, la sécurité ou les droits fondamentaux, en fonction de[35] :

1. La gravité et la probabilité du préjudice potentiel
2. Le degré d'autonomie du robot
3. La capacité du robot à interagir physiquement avec des humains
4. La présence de fonctions d'identification, de reconnaissance ou de profilage

Robots humanoïdes à usage domestique ou de service

Les robots humanoïdes destinés à un usage domestique, d'assistance à la personne ou de service dans des environnements non critiques (accueil, information, divertissement) peuvent être classés comme[36] :

1. **Risque limité** : si le robot interagit verbalement avec des humains sans prendre de décisions sensibles → obligation de transparence (informer l'utilisateur qu'il interagit avec une IA)
2. **Risque minimal** : si le robot effectue des tâches simples sans impact significatif → aucune obligation spécifique de l'AI Act (mais respect du RGPD et autres réglementations)

Interaction avec d'autres réglementations

Les robots humanoïdes sont concernés par un **écosystème réglementaire complexe** combinant plusieurs textes[37] :

Réglementation	Périmètre	Application aux robots

AI Act (2024/1689)	Systèmes d'IA	IA embarquée, algorithmes de décision
Règlement Machines (2023/1230)	Sécurité des machines	Structure, actionneurs, sécurité physique
RGPD (2016/679)	Protection des données	Caméras, capteurs, traitement de données
Directive responsabilité produits défectueux	Réparation des dommages	Dommages causés par dysfonctionnements

Tableau 1 : Cadre réglementaire applicable aux robots humanoïdes

Responsabilité et robots autonomes

La question de la responsabilité juridique en cas de dommage causé par un robot humanoïde autonome fait l'objet de propositions législatives complémentaires[38] :

1. **Directive sur la responsabilité en matière d'IA** (proposition COM/2022/496) : facilite les actions en responsabilité des victimes en allégeant leur charge de la preuve
2. **Directive sur la responsabilité du fait des produits défectueux** (proposition COM/2022/495 révisant la directive 85/374/CEE) : adapte les règles de responsabilité aux produits numériques et systèmes d'IA

Ces textes visent à garantir qu'une victime puisse obtenir réparation même lorsque le comportement du robot résulte d'un apprentissage autonome ou d'interactions complexes entre plusieurs composants[39].

Implications pratiques pour les organisations

Qui est concerné par l'AI Act ?

Le règlement s'applique à toute entité qui, dans le cadre de ses activités[40][41] :

1. **Fournit** (développe) des systèmes d'IA mis sur le marché européen, quelle que soit sa localisation géographique
2. **Importe** des systèmes d'IA de pays tiers vers l'UE
3. **Déploie** (utilise) des systèmes d'IA à haut risque dans l'UE
4. **Distribue** des systèmes d'IA sur le marché européen

Cela concerne aussi bien les grandes entreprises technologiques que les PME, les startups, les administrations publiques et les organisations à but non lucratif.

Actions urgentes avant août 2026

Pour les organisations qui développent ou utilisent des systèmes d'IA potentiellement à haut risque, plusieurs actions doivent être entreprises immédiatement[42][43] :

Étape 1 : Cartographier l'existant

1. Inventorier tous les systèmes d'IA développés ou utilisés

2. Identifier les données traitées et les finalités
3. Documenter les fournisseurs et les chaînes d'approvisionnement

Étape 2 : Évaluer le niveau de risque

1. Vérifier si les systèmes correspondent aux descriptions des Annexes I ou III
2. Évaluer si les exceptions de l'article 6(3) peuvent s'appliquer
3. Classer chaque système selon les catégories de risque

Étape 3 : Prioriser les systèmes à haut risque

1. Concentrer les efforts sur les systèmes de l'Annexe III (échéance 2026)
2. Planifier la mise en conformité des systèmes de l'Annexe I (échéance 2027)
3. Identifier les systèmes à risque inacceptable à cesser immédiatement

Étape 4 : Mettre en place la gouvernance de conformité

1. Désigner un responsable de la conformité AI Act
2. Établir un système de gestion des risques
3. Documenter tous les processus de développement et d'utilisation
4. Former les équipes techniques et métiers

Étape 5 : Préparer la documentation requise

1. Rédiger la documentation technique détaillée
2. Préparer les notices d'utilisation
3. Mettre en place les mécanismes de logging et de traçabilité
4. Établir les plans de surveillance post-commercialisation

Étape 6 : Planifier les évaluations de conformité

1. Identifier les organismes notifiés compétents
2. Planifier les délais d'évaluation (plusieurs mois)
3. Prévoir les budgets nécessaires

Étape 7 : Surveiller l'évolution réglementaire

1. Suivre les lignes directrices de la Commission (attendues février 2026)
2. Monitorer les normes harmonisées en cours d'élaboration
3. Se tenir informé de l'éventuel report des dates d'application

Sanctions en cas de non-conformité

L'AI Act prévoit un régime de sanctions administratives dissuasif en cas de violation[44] :

Type de violation	Montant maximal de l'amende
Utilisation d'IA à risque inacceptable	35 millions € ou 7% du CA mondial

Non-conformité des systèmes à haut risque	15 millions € ou 3% du CA mondial
Informations incorrectes aux autorités	7,5 millions € ou 1,5% du CA mondial

Tableau 2 : Sanctions prévues par l'AI Act

Pour les PME, le montant maximal de l'amende est plafonné en pourcentage du chiffre d'affaires, afin de garantir la proportionnalité[45].

Conclusion

La date du **2 août 2026** représente un tournant majeur dans la régulation de l'intelligence artificielle en Europe. À cette échéance, les systèmes d'IA à haut risque relevant de l'Annexe III devront être pleinement conformes à l'ensemble des obligations de l'AI Act, marquant ainsi l'entrée effective dans l'ère de l'IA régulée.

Toutefois, il est crucial de comprendre que tous les systèmes d'IA à haut risque ne sont pas concernés par cette date unique. Les systèmes intégrés dans des produits déjà réglementés (Annexe I) bénéficient d'un délai supplémentaire jusqu'en août 2027, tandis que certains systèmes utilisés par les administrations publiques disposent de périodes de transition étendues jusqu'en 2030.

Concernant les robots humanoïdes intégrant de l'IA, leur classification dépend de multiples facteurs : leur nature de produit réglementé, leur cas d'usage spécifique, et le niveau de risque qu'ils présentent. Un robot industriel, un robot médical, un robot de recrutement et un robot d'accueil domestique ne relèveront pas du même régime juridique ni du même calendrier d'application.

Face à cette complexité, les organisations doivent agir dès maintenant pour cartographier leurs systèmes d'IA, évaluer les risques, et mettre en place les processus de conformité nécessaires. Le temps presse, d'autant que l'incertitude persiste sur un éventuel report des dates d'application.

L'AI Act marque le début d'une nouvelle ère où l'intelligence artificielle sera encadrée par des règles juridiques contraignantes visant à protéger les droits fondamentaux tout en encourageant l'innovation responsable. Les mois à venir seront décisifs pour déterminer si l'Europe parviendra à concilier ces objectifs ambitieux avec les réalités opérationnelles des acteurs économiques.

Références

[1] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle. Journal officiel de l'Union européenne, L, 2024/1689, 12.07.2024.

[2] Deloitte France. (2024). EU AI Act : comprendre le premier cadre réglementaire sur l'intelligence artificielle.

[3] AI Act Blog. (2025). Key EU AI Act Developments in 2025 and Outlook for 2026.

[4] Leto Legal. (2026). AI Act 2026 : Guide complet de conformité IA pour les entreprises.

[5] Commission européenne. (2026). AI Act Implementation Timeline.

[6] Info.gouv.fr. (2025). Qu'est-ce que l'AI Act ?

[7] Vie Publique. (2025). Intelligence artificielle : le cadre juridique européen de l'IA (AI Act).

[8] AI Act Blog. (2025). Key EU AI Act Developments in 2025 and Outlook for 2026.

[9] DataGuard. (2025). EU AI Act Timeline: Key Compliance Dates & Deadlines.

[10] Commission européenne. (2026). AI Act | Shaping Europe's digital future.

[11] Ringover. (2024). AI Act : Tout savoir sur la Loi Européenne sur l'Intelligence Artificielle.

[12] Larcier Intersentia. (2025). Tout ce que vous devez savoir sur l'EU AI ACT.

[13] Commission européenne. (2026). AI Act Implementation Timeline.

[14] Commission européenne. (2026). AI Act Implementation Timeline.

[15] Timelex. (2025). The European Commission proposes a one-year delay for high-risk AI obligations.

[16] Timelex. (2025). The European Commission proposes a one-year delay for high-risk AI obligations.

[17] Commission européenne – AI Act Service Desk. (2024). Article 6 : Règles relatives à la classification de systèmes d'IA comme systèmes à haut risque.

[18] AI EU Act. (2024). Article 6 – Règles relatives à la classification de systèmes d'IA comme systèmes à haut risque.

[19] NAAIA. (2025). IA à haut risque : comprendre la liste de l'AI Act pour les entreprises.

[20] Entreprises.gouv.fr. (2025). Le Règlement européen sur l'intelligence artificielle.

[21] Aumans Avocats. (2025). Systèmes d'IA à haut risque : quels enjeux et quelles obligations.

[22] NAAIA. (2025). IA à haut risque : comprendre la liste de l'AI Act pour les entreprises.

[23] AI EU Act. (2024). Article 6 – Règles relatives à la classification de systèmes d'IA comme systèmes à haut risque.

[24] Timelex. (2025). AI, autonomous robots, and the EU's regulatory overhaul.

[25] Commission européenne – AI Act Service Desk. (2024). Article 6 : Règles relatives à la classification de systèmes d'IA comme systèmes à haut risque.

[26] Timelex. (2025). The European Commission proposes a one-year delay for high-risk AI obligations.

[27] Commission européenne. (2026). AI Act | Shaping Europe's digital future.

[28] Deloitte France. (2024). EU AI Act : comprendre le premier cadre réglementaire sur l'intelligence artificielle.

[29] Timelex. (2025). AI, autonomous robots, and the EU's regulatory overhaul.

[30] Démarre Ton Aventure. (2025). Robotique – Régulation et lois IA.

[31] Timelex. (2025). AI, autonomous robots, and the EU's regulatory overhaul.

[32] Démarre Ton Aventure. (2025). Robotique – Régulation et lois IA.

[33] Règlement (UE) 2023/1230 du 14 juin 2023 sur les machines, abrogeant la directive 2006/42/CE. Journal officiel de l'Union européenne, L165, 29.06.2023, p. 1-102.

[34] Scup. (2024). Smart Robotics in the EU Legal Framework.

[35] Timelex. (2025). AI, autonomous robots, and the EU's regulatory overhaul.

[36] Kaizen Solutions. (2025). AI Act : Obligations des entreprises pour les ChatBots et l'IA.

[37] Lexing Avocats. (2024). Observatoire du Droit des Robots et de l'IA.

[38] Proposition de directive du Parlement européen et du Conseil du 28 septembre 2022 relative à l'adaptation des règles en matière de responsabilité civile extracontractuelle au domaine de l'intelligence artificielle (COM/2022/496 final).

[39] Proposition de directive du Parlement européen et du Conseil du 28 septembre 2022 relative à la responsabilité du fait des produits défectueux (COM/2022/495 final).

[40] Entreprises.gouv.fr. (2025). Le Règlement européen sur l'intelligence artificielle.

[41] Info.gouv.fr. (2025). Qu'est-ce que l'AI Act ?

[42] Leto Legal. (2026). AI Act 2026 : Guide complet de conformité IA pour les entreprises.

[43] Artificial Intelligence Act. EU AI Act – Updates, Compliance, Training.

[44] Vie Publique. (2025). Intelligence artificielle : le cadre juridique européen de l'IA (AI Act).

[45] Leto Legal. (2026). AI Act 2026 : Guide complet de conformité IA pour les entreprises.