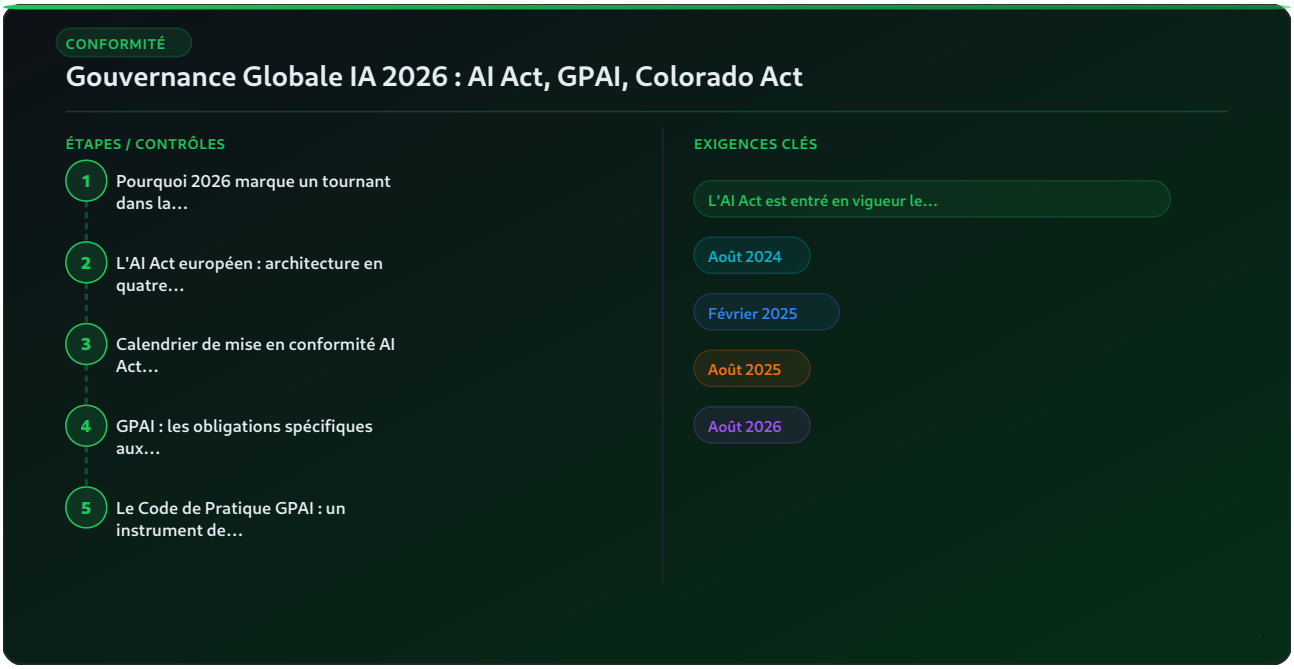
Gouvernance Globale de l'IA 2026 : AI Act, GPAI et Colorado AI Act

> Panorama de la gouvernance mondiale de l'IA en 2026 — AI Act européen, GPAI Code of Practice, Colorado AI Act, G7 Hiroshima Process et implications France

La gouvernance mondiale de l'intelligence artificielle connaît en 2026 une accélération sans précédent qui redéfinit les obligations des entreprises. L'AI Act européen entre en vigueur progressivement avec ses règles pour systèmes à haut risque pleinement applicables en août 2026, le Code de Pratique GPAI se finalise, le Colorado AI Act américain impose des obligations contraignantes aux développeurs de systèmes à haut risque, la Chine déploie son propre cadre réglementaire ambitieux, et le G7 Hiroshima Process produit ses premiers rapports d'audit. Pour les entreprises françaises, naviguer dans ce paysage réglementaire fragmenté n'est plus une option : c'est une condition de survie commerciale et de maintien de la confiance client. Cet article décrypte les grandes tendances de la gouvernance IA mondiale en 2026, leurs implications concrètes pour les organisations de toutes tailles, et les outils pratiques pour construire une conformité durable — sans sacrifier l'innovation ni la compétitivité.



Pourquoi 2026 marque un tournant dans la gouvernance de l'IA

Depuis les premiers débats autour de l'AI Act en 2021, la communauté tech considérait la réglementation IA comme une préoccupation lointaine. En 2026, ce confort a disparu. **L'AI Act est entré en vigueur le 1er août 2024**, avec des interdictions effectives depuis février 2025 et des obligations pour les systèmes à haut risque qui s'étendent tout au long de 2026. Parallèlement, des dizaines de pays ont adopté ou sont en train d'adopter leurs propres cadres nationaux.

Ce changement n'est pas anodin. Pour la première fois dans l'histoire de la technologie, des règles extraterritoriales s'appliquent simultanément à des entreprises de toutes tailles dès lors qu'elles commercialisent ou déploient des systèmes d'IA en Europe. Une PME lyonnaise qui utilise un système de scoring RH automatisé tombe sous le régime AI Act, au même titre qu'une multinationale américaine.

L'AI Act européen : architecture en quatre niveaux de risque

Le règlement européen 2024/1689 sur l'intelligence artificielle classe les systèmes d'IA selon quatre niveaux de risque, chacun avec des obligations distinctes.

⚡ **Retour terrain**

Dans mes missions de conformité, j'observe que les entreprises sous-estiment systématiquement le délai de mise en œuvre des mesures techniques. Les mesures organisationnelles (politiques, procédures) s'écrivent en semaines ; les mesures techniques (segmentation réseau, chiffrement, MFA) se déploient en mois. Pour un plan de mise en

conformité réaliste, je multiplie toujours les estimations initiales des équipes IT par 2,5 — et je n'ai jamais eu à réduire ce coefficient.

Niveau	Exemples	Obligations principales	Sanctions max
Risque inacceptable	Social scoring, manipulation subliminale, BRFI temps réel espaces publics	INTERDICTION totale	35M€ ou 7% CA
Risque élevé	IA RH, crédit, éducation, infra critique, médical, frontières	Conformité avant mise sur marché, registre EU, supervision humaine	15M€ ou 3% CA
Risque limité	Chatbots, deepfakes, contenu généré IA	Obligations de transparence et marquage	7,5M€ ou 1,5% CA
Risque minimal	Filtres spam, jeux vidéo IA, recommandations culturelles	Aucune obligation spécifique	—

Calendrier de mise en conformité AI Act 2024-2027

La conformité AI Act ne s'est pas faite du jour au lendemain. Le règlement prévoit une montée en charge progressive, avec plusieurs jalons critiques que toute organisation doit intégrer dans sa roadmap.

Août 2024 : Entrée en vigueur officielle du règlement

Février 2025 : Interdictions des pratiques IA inacceptables

Août 2025 : Obligations applicables aux modèles GPAI (General Purpose AI)

Août 2026 : Règles pleinement applicables pour les systèmes à haut risque

Août 2027 : Extension aux systèmes IA intégrés dans des produits régulés

GPAI : les obligations spécifiques aux modèles d'IA à usage général

Le titre IX de l'AI Act introduit un régime inédit pour les *modèles GPAI (General Purpose AI Models)* — des systèmes comme GPT-4, Claude, Gemini ou Mistral, capables de réaliser de nombreuses tâches différentes. **Depuis août 2025, tous les fournisseurs de GPAI commercialisés en Europe doivent se conformer à des exigences de transparence** : documentation technique, politique de copyright, résumé des données d'entraînement.

Pour les modèles GPAI à **risque systémique** (définis par un seuil de calcul dépassant 10^{25} FLOPs), des obligations supplémentaires s'appliquent : évaluation adversariale, signalement des incidents graves, mesures de cybersécurité. OpenAI, Anthropic, Google et Mistral AI figurent dans cette catégorie.

Le Code de Pratique GPAI : un instrument de gouvernance sectorielle

Parallèlement au règlement, la Commission européenne a mandaté l'AI Office pour développer un **Code de Pratique GPAI** avec l'industrie. Ce code, finalisé en 2025, traduit les obligations légales en mesures concrètes et vérifiables.

Sa structure repose sur quatre piliers : **transparence et droits d'auteur** (documentation des données d'entraînement, respect du Text and Data Mining opt-out), **évaluation des risques** (red teaming, tests d'évaluation standardisés), **sécurité technique** (robustesse aux attaques adversariales, prevention de la prolifération d'armes CBRN), et **gouvernance interne** (fonctions de compliance dédiées, rapports annuels).

L'adhésion au Code n'est pas formellement obligatoire pour les fournisseurs non-systémiques, mais elle crée une présomption de conformité avec l'AI Act — un avantage considérable en cas d'inspection de l'AI Office ou d'une autorité nationale de surveillance.

Colorado AI Act : la réglementation IA aux États-Unis prend forme

Les États-Unis ont longtemps résisté à une réglementation fédérale de l'IA. En 2026, le paysage a changé avec le **Colorado Artificial Intelligence Act (SB24-205)**, entré en vigueur le 1er février 2026. C'est la première loi américaine à imposer des obligations substantielles aux développeurs et déployeurs de systèmes IA à haut risque.

Contrairement à l'AI Act européen, le Colorado AI Act adopte une *approche outcome-based* : il ne réglemente pas la technologie elle-même, mais ses effets sur les individus. Tout système d'IA qui prend des décisions automatisées "conséquentielles" dans des domaines comme l'emploi, le logement, l'éducation, le crédit ou la santé est soumis à des obligations de due diligence, de notification aux utilisateurs, et d'audit de biais discriminatoires.

La réglementation chinoise de l'IA : un modèle alternatif

La Chine a adopté une approche réglementaire fragmentée mais intense. Trois règlements majeurs structurent le cadre chinois : les **Mesures sur les services algorithmiques recommandatifs** (2022), les **Mesures sur les deepfakes et contenu synthétique** (2023), et les **Mesures provisoires sur les services IA génératifs** (2023). Ces textes imposent des obligations spécifiques : marquage obligatoire des contenus générés par IA, enregistrement auprès du

Cyberspace Administration of China (CAC), interdiction de générer des contenus "mettant en danger la sécurité nationale".

En 2026, le gouvernement chinois finalise un cadre plus global baptisé **Loi sur la Gouvernance de l'IA**, inspiré partiellement de l'AI Act mais avec des différences fondamentales : priorité aux impératifs de sécurité nationale, rôle central de l'État dans l'orientation des usages, et exemptions larges pour les usages gouvernementaux et militaires.

G7 Hiroshima Process : vers un standard international minimal

Lancé en mai 2023 sous présidence japonaise, le **G7 Hiroshima AI Process** a abouti en octobre 2023 à l'adoption de 11 principes internationaux de conduite pour l'IA avancée. Ces principes — transparence, sécurité, robustesse, respect des droits humains, information des utilisateurs, mécanismes de signalement — constituent une base de soft law à laquelle les fournisseurs d'IA des pays G7 sont encouragés à adhérer.

En 2025, le processus a produit son premier **rapport d'avancement annuel**, évaluant la conformité déclarée des grands fournisseurs d'IA aux 11 principes. Si l'exercice reste volontaire et auto-déclaratif, il crée un mécanisme de responsabilisation internationale qui commence à influencer les décisions d'achat des gouvernements.

Anecdote terrain : lors d'un audit de conformité IA chez un éditeur de logiciel RH français en 2025, l'équipe de conseil a découvert que le CTO ignorait totalement l'existence du G7 Hiroshima Process. Pourtant, leur client principal — une multinationale japonaise — avait inscrit l'adhésion à ces principes comme critère éliminatoire dans son appel d'offres de renouvellement. La conformité internationale ne se résume pas à la réglementation européenne.

AI Safety Summits : Bletchley, Séoul, Paris

Les **AI Safety Summits** représentent un nouveau format de gouvernance internationale, centré sur les risques catastrophiques de l'IA avancée. Le premier sommet à Bletchley Park (novembre 2023) a abouti à la *Déclaration de Bletchley*, signée par 28 pays dont la Chine et les États-Unis — une première dans l'histoire de la gouvernance IA.

Le Sommet de Séoul (mai 2024) a approfondi les mécanismes d'audit des modèles frontier, avec la création d'un réseau de **AI Safety Institutes** dans 10 pays. Le Sommet de Paris (février 2025), co-organisé par la France et l'Inde, a mis l'accent sur l'IA pour le développement et l'équité internationale, avec un engagement de 500M€ de la France pour l'IA dans les pays en développement.

ISO 42001 : le système de management pour l'IA

Publiée en décembre 2023, la norme **ISO/IEC 42001:2023** définit les exigences d'un *Système de Management de l'IA (AIMS — AI Management System)*. Elle s'inspire de la structure harmonisée des normes ISO (identique à ISO 27001, ISO 9001) et permet une intégration dans les systèmes de management existants.

La norme couvre : la politique IA de l'organisation, l'évaluation des risques et impacts IA, les contrôles opérationnels (développement responsable, qualité des données, tests), la gestion des fournisseurs IA, et l'amélioration continue. La certification tierce partie par un organisme accrédité constitue en 2026 l'un des moyens les plus crédibles pour démontrer la conformité AI Act devant les autorités de surveillance.

Articulation AI Act et ISO 42001

La Commission européenne a publié en 2025 une note technique confirmant que la certification ISO 42001 par un organisme notifié peut constituer une présomption de conformité pour certaines exigences AI Act. Les domaines couverts incluent : gestion des données (Art. 10), documentation technique (Art. 11), tenue de journaux (Art. 12), gouvernance interne (Art. 9). Les exigences spécifiques aux systèmes à haut risque (Art. 13-15) nécessitent toutefois des mesures complémentaires.

Pour les entreprises déjà certifiées ISO 27001, la passerelle vers ISO 42001 est facilitée par des clauses communes (contexte de l'organisation, leadership, planification, support, évaluation de la performance). Un projet de certification combinée ISO 27001 + ISO 42001 représente une charge de travail inférieure d'environ 35% à deux certifications séparées.

RGPD et AI Act : la double contrainte européenne

L'AI Act s'applique en parallèle du RGPD, créant une **double contrainte réglementaire** pour les systèmes d'IA traitant des données personnelles — ce qui couvre la grande majorité des applications pratiques. Les interactions sont nombreuses et parfois contradictoires.

Par exemple, l'AI Act exige la conservation de journaux d'audit pendant 10 ans pour certains systèmes à haut risque, tandis que le RGPD impose la limitation de la conservation des données personnelles au strict nécessaire. Les entreprises doivent donc mettre en place des mécanismes de pseudonymisation ou d'anonymisation pour concilier ces exigences. Le **Comité Européen de la Protection des Données (CEPD)** a publié des lignes directrices en 2025 pour aider les DPO à naviguer dans cette articulation.

Qu'est-ce qu'un système IA à haut risque selon l'AI Act ?

La liste des systèmes IA à haut risque (Annexes III et II de l'AI Act) est plus longue et plus surprenante que beaucoup d'organisations ne l'imaginent. Elle inclut :

- Systèmes d'IA intégrés dans des dispositifs médicaux, machines, ascenseurs, véhicules
- IA de recrutement, scoring de CV, évaluation des performances, licenciement automatisé
- Systèmes de scoring de crédit et évaluation de solvabilité
- IA utilisées dans l'éducation : notation automatisée, admission, orientation
- Systèmes d'IA pour l'accès aux services publics essentiels
- IA biométrique : reconnaissance faciale, analyse des émotions, catégorisation biométrique
- IA pour la gestion des infrastructures critiques (eau, énergie, transports)
- Systèmes IA d'aide à la décision judiciaire et d'application de la loi

Sanctions AI Act : un régime dissuasif

Le régime de sanctions de l'AI Act est calibré pour être dissuasif, avec des plafonds très supérieurs à ceux du RGPD. Pour les violations les plus graves (systèmes IA interdits, fausses informations aux autorités de surveillance), les amendes atteignent **35 millions d'euros ou 7% du chiffre d'affaires mondial annuel** pour le montant le plus élevé.

Pour les violations des obligations applicables aux systèmes IA à haut risque, le plafond est de 15 millions d'euros ou 3% du CA. Pour les informations incorrectes ou incomplètes fournies aux autorités, 7,5 millions d'euros ou 1,5% du CA. Les PME et startups bénéficient d'un régime proportionné, mais les exemptions restent limitées.

Le rôle de la France dans la gouvernance mondiale de l'IA

La France occupe une position particulière dans l'écosystème mondial de la gouvernance IA. D'un côté, elle abrite Mistral AI, l'un des rares fournisseurs européens de modèles GPAI concurrentiels aux géants américains. De l'autre, elle a joué un rôle moteur dans la négociation de l'AI Act via son influence au Parlement européen et au Conseil.

La **Commission nationale de l'informatique et des libertés (CNIL)** a été désignée comme l'une des autorités nationales compétentes pour l'AI Act en France, aux côtés de l'Autorité de la concurrence et de futures autorités sectorielles. En 2026, la CNIL a publié ses premières orientations sur l'application de l'AI Act aux systèmes d'IA traitant des données biométriques — un signal que l'application du règlement est désormais une réalité opérationnelle.

Construire une roadmap de conformité AI Act en entreprise

Face à la complexité du cadre réglementaire, les organisations doivent adopter une approche structurée. Voici une roadmap en cinq phases pratiquement testée :

Phase 1 — Inventaire (2 semaines) : Cartographier tous les systèmes IA utilisés ou développés, en incluant les IA embarquées dans des logiciels tiers. Souvent, les résultats surprennent : de nombreuses organisations découvrent 2 à 3 fois plus de systèmes IA qu'elles ne l'estimaient.

Phase 2 — Classification (1 semaine) : Classifier chaque système selon les annexes AI Act. Consulter un juriste spécialisé pour les cas limites.

Phase 3 — Gap analysis (3 semaines) : Pour chaque système à haut risque, identifier les écarts entre l'état actuel et les exigences AI Act.

Phase 4 — Remédiation (variable) : Mettre en œuvre les mesures correctives : documentation technique, système de gestion des risques, mécanismes de supervision humaine, etc.

Phase 5 — Enregistrement et audit (2 semaines) : Enregistrer les systèmes à haut risque dans la base de données EU (obligatoire pour certaines catégories), préparer la documentation pour les audits.

Le marché de la conformité IA : une industrie en pleine expansion

La complexité de l'AI Act a créé un marché de la conformité IA estimé à plusieurs milliards d'euros en Europe. Des cabinets de conseil spécialisés, des éditeurs de logiciels GRC (Governance, Risk, Compliance) adaptés à l'IA, et des plateformes d'audit automatisé émergent rapidement.

Opinion tranchée : Le marché de la conformité IA risque de reproduire les dérives observées avec le RGPD — une prolifération de prestataires proposant des "kits de conformité clé en main" qui donnent bonne conscience sans adresser les risques réels. La conformité AI Act efficace n'est pas une case à cocher : c'est une transformation de la gouvernance organisationnelle autour de l'IA. Les entreprises qui traiteront l'AI Act comme un exercice bureaucratique paieront le prix fort lors des premiers audits.

IA Act et innovation : le faux dilemme

L'argument selon lequel la réglementation IA étouffe l'innovation est récurrent, mais empiriquement contestable. L'AI Act inclut des dispositions explicites pour préserver l'espace d'innovation :

Les **regulatory sandboxes IA** permettent aux entreprises de tester des systèmes IA innovants dans un environnement réglementé avec des obligations allégées. Chaque État membre doit mettre en place au moins un tel bac à sable national. La France a lancé son **Bac à sable IA** sous l'égide de la CNIL en 2025, avec des projets pilotes dans les secteurs de la santé et des transports.

Par ailleurs, les systèmes IA développés exclusivement pour la recherche scientifique bénéficient d'exemptions importantes. Les startups et PME bénéficient de délais supplémentaires et d'un accès prioritaire aux bacs à sable nationaux.

Gouvernance IA interne : au-delà de la conformité réglementaire

La conformité réglementaire est une condition nécessaire mais insuffisante pour une gouvernance IA robuste. Les organisations matures développent une gouvernance IA interne qui va au-delà des exigences légales minimales.

Cela inclut : un **Comité d'éthique IA** multidisciplinaire (juristes, éthiciens, techniciens, représentants métier), des **politiques d'usage IA** claires pour les employés, des procédures d'**impact assessment IA** (AIIA) systématiques avant tout déploiement, et un programme de **sensibilisation et formation** aux risques IA pour l'ensemble du personnel.

Meilleures pratiques de documentation technique AI Act

La documentation technique est l'une des exigences les plus contraignantes de l'AI Act pour les systèmes à haut risque. L'Annexe IV du règlement liste les éléments obligatoires : description générale du système, architecture et composants, données d'entraînement et de test, performance et robustesse, mesures de cybersécurité, supervision humaine.

En pratique, les équipes techniques sous-estiment systématiquement le volume de travail requis. Une approche efficace consiste à intégrer la documentation AI Act dès les phases de design (documentation-as-code), plutôt que de la produire a posteriori lors du déploiement. Des outils comme **MLflow**, **DVC** ou des plateformes MLOps spécialisées peuvent automatiser une partie de la capture de métadonnées requises.

Vers une convergence internationale des réglementations IA ?

La question de la convergence internationale des réglementations IA est stratégique pour les entreprises opérant dans plusieurs juridictions. En 2026, les signaux sont mixtes.

D'un côté, le **Global Partnership on AI (GPAI)**, fondé en 2020 et désormais fort de 29 membres, travaille activement à l'harmonisation des approches. La publication de recommandations communes sur les systèmes d'IA responsables, la gestion des risques et la diversité dans l'IA témoigne d'une volonté de convergence. De l'autre, les différences fondamentales d'approche — l'UE avec sa réglementation contraignante ex-ante, les États-Unis avec leur approche sectorielle post-marché, la Chine avec ses impératifs de souveraineté — rendent une harmonisation complète peu probable à court terme.

La stratégie pragmatique pour les entreprises multinationales : viser la conformité AI Act comme standard le plus exigeant, puis adapter marginalement pour les spécificités locales.

Questions fréquentes sur la gouvernance de l'IA

Mon entreprise utilise ChatGPT via API — suis-je concerné par l'AI Act ?

Oui, potentiellement. En tant que **déployeur** d'un système GPAI, vous devez vérifier si l'usage que vous en faites constitue un système IA à haut risque selon l'Annexe III. Par exemple, utiliser ChatGPT pour automatiser des décisions RH vous placerait dans la catégorie haut risque avec des obligations substantielles. Même pour les usages non-haut-risque, vous avez des obligations de transparence envers vos utilisateurs et de mise en place d'une politique d'usage acceptable.

Quelle est la différence entre AI Act et ISO 42001 ?

L'AI Act est un règlement juridiquement contraignant de l'Union européenne avec des sanctions légales. ISO 42001 est une norme internationale volontaire de système de management. La certification ISO 42001 peut créer une présomption de conformité partielle avec l'AI Act, mais ne remplace pas les obligations légales spécifiques, notamment l'enregistrement dans la base de données EU, la conformité aux exigences des systèmes à haut risque, et les évaluations tierce partie pour certaines catégories.

L'AI Act s'applique-t-il aux startups françaises ?

Oui, l'AI Act s'applique à toute organisation qui met sur le marché européen ou utilise en Europe des systèmes d'IA entrant dans son champ d'application, quelle que soit sa taille. Cependant, les PME et startups bénéficient de plusieurs mesures d'atténuation : accès prioritaire aux regulatory sandboxes, délais supplémentaires pour certaines obligations, réduction des frais d'évaluation de conformité, et obligations documentaires allégées. Les systèmes IA à risque minimal (la majorité des applications startups) ne sont soumis à aucune obligation spécifique.

Quelle autorité contrôle l'application de l'AI Act en France ?

En France, la CNIL a été désignée comme autorité nationale compétente pour les systèmes IA traitant des données personnelles. Pour les autres secteurs, des autorités sectorielles existantes (ANSM pour le médical, ACPR pour la finance, ANFR pour les télécoms) seront également compétentes dans leurs domaines respectifs. Au niveau européen, l'AI Office de

la Commission supervise les modèles GPAI et coordonne les autorités nationales. En cas de conflit entre autorités, l'AI Office a un rôle d'arbitrage.

Comment l'AI Act interagit-il avec le règlement sur les données (Data Act) ?

L'AI Act et le Data Act forment deux piliers complémentaires du cadre numérique européen. Le Data Act régule l'accès et le partage des données générées par les objets connectés et services numériques, créant un écosystème de données qui facilite l'entraînement des modèles IA. Pour les systèmes IA à haut risque, les exigences de qualité des données de l'AI Act (Art. 10) sont renforcées par les droits d'accès aux données du Data Act. Les équipes juridiques doivent analyser les deux règlements conjointement pour les projets IA intensifs en données.

À RETENIR

Points clés à retenir

L'AI Act est effectif — les premières obligations (interdictions, GPAI) s'appliquent depuis 2025 ; les règles haut risque complètes s'appliquent en août 2026.

La classification est la priorité — l'inventaire et la classification des systèmes IA doivent être finalisés immédiatement pour identifier les obligations applicables.

ISO 42001 accélère la conformité — la certification crée une présomption de conformité partielle avec l'AI Act et structure la gouvernance IA interne.

La double contrainte RGPD + AI Act exige une coordination étroite entre DPO et responsable conformité IA.

Les bacs à sable réglementaires offrent un espace sécurisé pour innover sous supervision ; en France, la CNIL gère ce dispositif.

La convergence internationale reste partielle — viser la conformité AI Act comme standard le plus strict reste la stratégie la plus sûre pour les entreprises multinationales.

Pour aller plus loin sur la mise en conformité de vos systèmes IA, consultez notre page sur le conseil en conformité réglementaire et notre offre d'audit de sécurité IA. Nous accompagnons les entreprises françaises dans leur parcours de conformité AI Act depuis l'inventaire initial jusqu'à la certification ISO 42001. Découvrez également notre service de RSSI externalisé qui intègre la gouvernance IA dans le management global de la sécurité. Pour les aspects techniques, notre équipe spécialisée en tests de sécurité IA peut valider la robustesse de vos modèles face aux attaques adversariales.

Ressources officielles : le texte consolidé de l'AI Act sur EUR-Lex et la page officielle de la Commission européenne sur l'AI Act.

Supervision humaine dans les systèmes IA à haut risque : exigences concrètes

L'article 14 de l'AI Act impose que les systèmes IA à haut risque soient conçus de façon à permettre une **supervision humaine effective**. Cette exigence est plus complexe qu'il n'y paraît. Une supervision humaine effective ne signifie pas qu'un humain doit approuver chaque décision — cela rendrait tout système IA inopérant. Elle signifie que les humains responsables doivent être capables de comprendre les capacités et limites du système, de détecter les anomalies, d'intervenir et d'arrêter le système si nécessaire, et de ne pas être induits en erreur par une confiance excessive (automation bias).

Les mesures techniques requises incluent : des interfaces de supervision claires avec indicateurs de confiance, des mécanismes d'alerte en cas de fonctionnement hors des paramètres nominaux,

des options de remplacement manuel accessibles, et des journaux d'audit exploitables par des opérateurs non-techniques. Pour les systèmes de décision à fort enjeu (scoring de crédit, recrutement), l'AI Act exige explicitement que les décisions automatisées puissent être contestées et examinées manuellement sur demande de l'individu concerné.

Gestion des données d'entraînement : conformité AI Act et qualité

L'article 10 de l'AI Act impose aux systèmes IA à haut risque des exigences strictes sur les *pratiques de gouvernance des données* d'entraînement, de validation et de test. Ces données doivent être pertinentes, représentatives, exemptes d'erreurs dans la mesure du possible, et complètes compte tenu de l'objectif visé. La notion de représentativité est particulièrement délicate : comment s'assurer que les données d'entraînement représentent fidèlement la population sur laquelle le système sera déployé ?

En pratique, les équipes MLOps doivent implémenter : une **traçabilité complète des données** (data lineage) depuis leur source jusqu'à leur utilisation en entraînement, des **analyses de biais systématiques** (fairness metrics par sous-groupe démographique), des **tests de distribution shift** entre données d'entraînement et données de production, et une **politique de rétention des données d'entraînement** compatible avec les obligations documentaires AI Act. Les outils comme DVC (Data Version Control), Delta Lake, ou Apache Iceberg facilitent cette traçabilité.

Cybersécurité des systèmes IA : obligations spécifiques AI Act

L'article 15 de l'AI Act impose que les systèmes IA à haut risque atteignent un niveau approprié de **robustesse, précision et cybersécurité**. Pour la cybersécurité, cela se traduit par des exigences de résistance aux attaques adversariales, aux tentatives de manipulation des données d'entraînement (data poisoning), et aux attaques visant à extraire le modèle ou ses données d'entraînement (model extraction, membership inference).

Ces exigences créent un pont entre la réglementation IA et les pratiques de **sécurité offensive IA**. Un système IA à haut risque déployé sans avoir subi de tests adversariaux structurés est non-conforme à l'AI Act. Pour les entreprises, cela signifie intégrer les tests de sécurité IA spécialisés dans le cycle de développement et les évaluations périodiques. Les standards MITRE ATLAS et OWASP LLM Top 10 constituent des références utiles pour structurer ces évaluations.

Exigences de transparence pour les systèmes IA au contact des utilisateurs

L'article 50 de l'AI Act impose des obligations de transparence spécifiques pour les systèmes IA interagissant directement avec des humains. Un chatbot doit informer les utilisateurs qu'ils interagissent avec une IA (sauf si c'est évident). Les contenus audio, image, vidéo ou texte générés par IA doivent être marqués comme tels de façon machine-readable (watermarking). Les systèmes de reconnaissance des émotions et de catégorisation biométrique doivent informer les personnes concernées.

Ces obligations de transparence sont moins techniques que les exigences pour les systèmes à haut risque, mais leur champ d'application est potentiellement très large. Tout service de chatbot client, tout système de génération de contenu marketing, toute application d'analyse RH basée sur la voix ou le visage tombe sous ces obligations. La Commission européenne développe des spécifications techniques pour les watermarks IA — un chantier complexe car les techniques actuelles restent fragiles face aux modifications simples (compression, re-encodage).

Gouvernance IA dans les secteurs réglementés : finance et santé

Les secteurs financier et de la santé font face à une **double réglementation IA** : l'AI Act horizontal et leurs réglementations sectorielles spécifiques. Dans la finance, les systèmes IA de scoring de crédit sont à haut risque selon l'AI Act ET soumis aux orientations EBA sur l'IA dans

les modèles de risque. Dans la santé, les dispositifs médicaux intégrant de l'IA combinent les exigences AI Act avec celles du règlement MDR (Medical Device Regulation).

La **Banque de France et l'ACPR** ont publié en 2025 un document de position sur la gouvernance des modèles IA dans le secteur financier, précisant comment les obligations AI Act s'articulent avec les exigences existantes (modèles validés, backtesting, documentation du modèle). Pour les établissements de santé et industriels du médicament, l'ANSM a développé un guide similaire intégrant les critères de qualification IA dans le cadre MDR/IVDR.

Formation et compétences : le facteur humain de la conformité IA

L'article 4 de l'AI Act impose aux opérateurs (fournisseurs, déployeurs) de veiller à ce que leur personnel disposant d'un niveau suffisant de **compétences en matière d'IA**. Cette obligation de *littératie IA* (AI literacy) est souvent négligée dans les programmes de conformité, au profit des aspects techniques et documentaires.

En pratique, cela implique des formations adaptées à différents niveaux : sensibilisation générale pour tous les employés (risques IA, biais, droit à l'explication), formation approfondie pour les équipes métier utilisant des systèmes IA à haut risque (comment exercer la supervision humaine, comment signaler les anomalies), et formation technique pour les équipes de développement et de déploiement (conception robuste, tests adversariaux, documentation technique). Les entreprises les plus avancées intègrent la formation IA dans leurs programmes d'onboarding et leurs plans de développement des compétences annuels.

Incidents IA et obligation de signalement

L'AI Act introduit un **mécanisme de signalement des incidents graves** impliquant des systèmes IA à haut risque. Les fournisseurs doivent notifier leur autorité nationale de surveillance dans un délai défini lorsqu'un système IA à haut risque cause ou contribue à causer un incident grave —

défini comme un risque pour la santé, la sécurité ou les droits fondamentaux, ou un dommage grave à l'infrastructure critique.

La gestion des incidents IA nécessite donc une procédure dédiée, distincte des processus de gestion des incidents informatiques classiques. Les éléments clés : identification des critères de qualification d'un incident IA grave, chaîne d'escalade dédiée incluant les responsables juridiques et conformité, documentation standardisée pour les rapports aux autorités, et analyse post-incident pour prévenir la récurrence. Les entreprises déjà dotées d'un SOC peuvent intégrer ces procédures dans leurs playbooks existants, en ajoutant une couche d'analyse spécifique aux systèmes IA.

Interopérabilité et portabilité dans la gouvernance IA

Un aspect souvent négligé de la gouvernance IA est la question de la **portabilité des modèles et des données**. Le Data Act européen, en vigueur depuis septembre 2025, impose aux fournisseurs de services cloud et de plateformes d'IA de faciliter la portabilité des données et des modèles. Pour les entreprises, cela signifie que leurs systèmes IA ne doivent pas créer de dépendances irréversibles vis-à-vis d'un fournisseur spécifique.

Les bonnes pratiques d'interopérabilité incluent : l'utilisation de formats ouverts pour la sérialisation des modèles (ONNX, PMML), la documentation des interfaces d'API en standards ouverts (OpenAPI), la conservation des données d'entraînement dans des formats exportables, et la conception d'architectures modulaires permettant de substituer des composants IA. Ces pratiques servent à la fois la conformité réglementaire et la résilience opérationnelle.

Évaluation d'impact sur les droits fondamentaux (DPIA IA)

Pour les systèmes IA à haut risque déployés par des entités publiques ou par des opérateurs privés dans certains contextes, l'AI Act introduit l'obligation de conduire une *évaluation d'impact*

sur les droits fondamentaux avant déploiement. Cette procédure, qui complète la DPIA du RGPD pour les données personnelles, évalue l'impact potentiel du système IA sur les droits fondamentaux reconnus par la Charte des droits fondamentaux de l'UE.

La méthodologie d'évaluation couvre : l'identification des droits fondamentaux potentiellement affectés (non-discrimination, droit à un recours effectif, présomption d'innocence, protection des données), l'évaluation de la probabilité et gravité des impacts, les mesures d'atténuation prévues, et les mécanismes de contrôle et de révision. Les résultats de l'évaluation doivent être enregistrés dans la base de données EU pour les systèmes déployés par des autorités publiques. Pour les acteurs privés, la documentation doit être conservée et mise à disposition des autorités de surveillance sur demande.

Standards techniques harmonisés : le rôle du CEN-CENELEC

L'AI Act délègue aux organismes européens de normalisation **CEN et CENELEC** le développement de standards techniques harmonisés qui précisent les modalités de mise en œuvre des exigences du règlement. Ces standards, une fois publiés au Journal Officiel de l'UE, créent une présomption de conformité pour les systèmes IA qui les respectent.

En 2026, plusieurs standards sont en cours de développement : standards sur les processus d'évaluation de la qualité des données (groupe de travail JTC21), standards sur les tests de robustesse et précision pour les systèmes à haut risque, standards sur la documentation technique, et standards sur la gestion des risques IA. Le calendrier de publication est incertain, mais les premières versions devraient être disponibles courant 2026-2027. En attendant, les entreprises peuvent s'appuyer sur les spécifications techniques publiées par l'AI Office et sur des standards existants comme ISO/IEC 23894 (gestion des risques IA) et ISO/IEC 42001.

AI Act et marchés publics : les obligations des entités adjudicatrices

Les entités publiques françaises (collectivités, établissements publics, ministères) sont soumises à des obligations AI Act spécifiques en tant que déployeurs de systèmes IA. L'article 26 du règlement impose aux déployeurs de systèmes à haut risque dans le secteur public de conduire des **évaluations d'impact sur les droits fondamentaux** avant déploiement, d'enregistrer les systèmes dans la base de données EU, et de nommer un responsable de la gouvernance IA.

Dans le contexte des marchés publics, les acheteurs publics commencent à intégrer des critères de conformité AI Act dans leurs cahiers des charges pour les acquisitions de logiciels intégrant de l'IA. La **Direction interministérielle du numérique (DINUM)** a publié en 2025 un guide de l'achat public d'IA responsable, fixant des critères minimaux de transparence, de non-discrimination et d'explicabilité pour les systèmes IA achetés par l'État.

Registre EU des systèmes IA à haut risque

L'AI Act crée une **base de données EU** publique, gérée par l'AI Office, dans laquelle certaines catégories de systèmes IA à haut risque doivent être enregistrées avant déploiement. Cet enregistrement est obligatoire pour les systèmes IA à haut risque listés à l'Annexe III lorsqu'ils sont destinés au grand public ou aux autorités publiques — par exemple, les systèmes IA pour l'accès aux services publics, les systèmes d'aide à la décision judiciaire, ou les systèmes biométriques.

L'enregistrement requiert de fournir : une description du système, les coordonnées du fournisseur, la date de mise sur le marché, les États membres dans lesquels le système est déployé, et une description sommaire de l'évaluation de conformité effectuée. Cette base de données publique constitue un outil de transparence pour les citoyens et les régulateurs, et un signal fort pour les acheteurs potentiels.

IA générative et droits d'auteur : le casse-tête juridique

L'une des tensions les plus vives dans la gouvernance IA mondiale concerne le rapport entre l'IA générative et les droits d'auteur. L'AI Act impose aux fournisseurs de GPAI de publier un résumé des données d'entraînement et de respecter les opt-outs de Text and Data Mining (TDM) prévus par la directive Copyright. Mais la mise en œuvre pratique reste complexe.

Plusieurs contentieux majeurs ont été engagés en Europe et aux États-Unis par des auteurs, journalistes et créateurs contre les fournisseurs de modèles IA. En France, le **tribunal de grande instance de Paris** a rendu en 2025 une première décision reconnaissant le droit d'auteur sur des contenus utilisés sans autorisation pour entraîner un modèle IA commercial — une décision surveillée de près par l'ensemble de l'industrie. La question de la rémunération des créateurs pour l'utilisation de leurs œuvres dans l'entraînement des modèles IA reste ouverte et fait l'objet d'un groupe de travail spécifique au sein du CEPD et de l'HADOPI.

IA et emploi : le volet social de la gouvernance

La gouvernance de l'IA ne se limite pas à la réglementation technologique. Son volet social — impact sur l'emploi, transition des compétences, dialogue social autour de l'IA — devient en 2026 un enjeu de gouvernance d'entreprise à part entière. En France, la loi PACTE II a introduit en 2025 une obligation d'information-consultation des comités sociaux et économiques (CSE) avant tout déploiement significatif de systèmes IA affectant les conditions de travail.

Cette obligation de dialogue social s'articule avec les exigences AI Act sur la supervision humaine et la non-discrimination. Les entreprises qui investissent dans une **gouvernance IA inclusive** — associant les représentants du personnel à la définition des politiques d'usage IA, formant les employés aux outils IA déployés, mettant en place des mécanismes de signalement internes — construisent simultanément leur conformité réglementaire et leur capital de confiance sociale.

Perspectives 2027-2030 : l'évolution prévisible du cadre réglementaire

La gouvernance de l'IA est un champ en évolution rapide. Plusieurs dynamiques prévisibles structureront le cadre réglementaire à horizon 2027-2030. D'abord, la montée en puissance des **AI Safety Institutes nationaux** : après le Royaume-Uni, les États-Unis, le Japon et la Corée, d'autres pays créeront leurs propres instituts de sécurité IA, avec des mandats d'évaluation des modèles frontier. La coordination entre ces instituts, encore naissante, devient une infrastructure critique de la gouvernance mondiale.

Ensuite, l'émergence de standards techniques harmonisés AI Act (CEN/CENELEC) changera la dynamique de conformité, en offrant des voies certifiées vers la présomption de conformité. L'adoption d'un **traité international sur l'IA** — en négociation sous l'égide du Conseil de l'Europe depuis 2024 — ouvrira une troisième dimension, juridiquement contraignante au niveau international, à côté des réglementations nationales et régionales. Enfin, l'évolution des capacités IA elles-mêmes — AGI partielle, agents IA autonomes, IA dans les systèmes d'armement — créera des pressions pour adapter les cadres réglementaires existants, aujourd'hui principalement conçus pour les systèmes IA à usage civil spécifique.

Conformité AI Act : comment choisir son prestataire d'accompagnement ?

Face à la complexité du cadre réglementaire, de nombreuses entreprises font appel à des prestataires externes pour structurer leur démarche de conformité AI Act. Le choix du bon partenaire est stratégique. Les critères essentiels incluent : une expertise combinée juridique et technique (la conformité AI Act est indissociablement les deux), une expérience sectorielle dans votre domaine d'activité (les enjeux sont très différents entre la finance, la santé et l'industrie), une méthodologie éprouvée intégrant l'inventaire, la classification, la gap analysis et le plan de remédiation, et une capacité à vous accompagner dans la durée (la conformité AI Act n'est pas un projet ponctuel mais un programme continu).

Méfiez-vous des prestataires qui promettent une conformité AI Act "en quelques semaines" via des questionnaires automatisés. **Une conformité réelle nécessite une analyse approfondie de**

vos systèmes IA, de vos flux de données, et de vos processus de décision. Notre équipe de consultants spécialisés en conformité réglementaire IA combine des compétences juridiques (droit du numérique européen, AI Act, RGPD) et techniques (architecture ML, sécurité IA, MLOps) pour vous accompagner à chaque étape — de l'inventaire initial jusqu'à la certification ISO 42001 et l'enregistrement dans la base de données EU.

© Ayi NEDJIMI Consultants — Tous droits réservés