Présentation du

REGLEMENT (UE) 2024/1689 DU PARLEMENT EUROPEEN ET DU CONSEIL DU 13 JUIN 2024 ETABLISSANT DES REGLES HARMONISEES CONCERNANT L'INTELLIGENCE ARTIFICIELLE

publié au Journal officiel de l'Union européenne le 12 juillet 2024

et applicable au 2 Août 2026

Jean-François Carlot – Avocat Honoraire – Médiateur

www.jurilis.fr

> **L'objectif du règlement est d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme, en particulier pour le développement, la mise sur le marché, la mise en service et l'utilisation de systèmes d'intelligence artificielle dans l'Union, dans le respect des valeurs de l'Union, de promouvoir l'adoption de l'intelligence artificielle (IA) axée sur l'humain et digne de confiance tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux, y compris la démocratie, l'état de droit et la protection de l'environnement, de protéger contre les effets néfastes des systèmes d'IA dans l'Union, et de soutenir l'innovation.**

Il garantit la libre circulation transfrontière des biens et services fondés sur l'IA, empêchant ainsi les États membres d'imposer des restrictions au développement, à la commercialisation et à l'utilisation de systèmes d'IA, sauf autorisation expresse du présent règlement.

L'IA doit être une technologie axée sur l'humain, et devrait servir d'outil aux personnes, dans le but ultime d'accroître le bien-être des humains. Elle peut cependant générer des risques et porter atteinte aux intérêts publics et aux droits fondamentaux.

Le présent règlement devrait être sans préjudice des dispositions relatives à la responsabilité des fournisseurs de services intermédiaires prévue dans le règlement (UE) 2022/2065 du Parlement européen et du Conseil.

Cette présentation ne concerne que les points du règlement concernant les obligations des fabricants, fournisseurs et déployeurs des systèmes d'IA.

CHAPITRE I. CHAMP D'APPLICATION ET DEFINITIONS (ART. 2 ET 3)

Le règlement s'applique aux systèmes d'IA (SIA), défini par l'article 3 comme un :

> « ***système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels*** » (art. 3, § 1).

Il s'applique aux SIA mis à disposition sur le marché de l'Union ou lorsque les sorties produites par le SIA sont utilisées dans l'Union, quel que soit le lieu d'établissement de l'opérateur (art. 2).

Il s'impose au fabricant, distributeur et « déployeur » d'un SIA « sous sa propre autorité » (art. 3 et 4).

Le règlement ne s'applique pas :

- aux SIA développés et utilisés à des fins militaires, de défense ou de sécurité nationale relevant de la compétence exclusive des États membres (art. 2, § 3).
- aux SIA ou modèles d'IA spécifiquement développés et mis en service à des fins exclusives de recherche scientifique et de développement, (art. 2, § 6).
- aux SIA diffusés sous licence libre et open source, sauf s'ils sont mis sur le marché ou mis en service en tant que SIA à haut risque ou en tant que SIA qui relève de l'article 5, donc prohibé, ou de l'article 50 qui implique des mesures de transparence particulière (art. 2, § 12).

CHAPITRE II. PRATIQUES INTERDITES (ART. 5)

- Les techniques **subliminales** (art. 5, § 1, a),
- Exploitation des **vulnérabilités** (art. 5, § 1, b) ;
- Opérations de **police prédictive**, notamment sans intervention humaine (art. 5 § 1, d) ;
- Création de **bases de données de reconnaissance faciale** par le moissonnage non ciblé d'images faciales provenant de l'internet ou de la vidéosurveillance (art. 5, § 1, e) ;
- **Reconnaissance émotionnelle** sur le lieu de travail ou dans les établissements d'enseignement (art. 5, § 1, f) ou encore **catégorisation biométrique** catégorisant individuellement les personnes physiques afin d'arriver à des déductions ou des inférences concernant des caractéristiques sensibles (telles que la race, les opinions politiques, l'orientation sexuelle, v. art. 5, § 1, g).
- **Notation sociale** si elle conduit à un traitement préjudiciable ou défavorable et dans le cadre de deux situations bien précises (art. 5, § 1, c).

En revanche, **l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives est quant à elle autorisée dans des circonstances spéciales** (traite ou exploitation sexuelle d'êtres humains, attaques terroristes…, art. 5, § 1, h) et i) et sous réserve d'avoir :

- obtenu **une autorisation préalable octroyée par une autorité judiciaire ou une autorité administrative indépendante**,
- réalisé une **analyse d'impact sur les droits fondamentaux** (art. 27)
- été **enregistré dans la base de données de l'Union européenne** (art. 49).

Le non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5 fait l'objet d'amendes administratives pouvant aller jusqu'à 35 000 000 EUR ou, si l'auteur

de l'infraction est une entreprise, jusqu'à 7 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.

La non-conformité avec l'une quelconque des dispositions relatives aux opérateurs ou aux organismes notifiés, autres que celles énoncées à l'article 5, fait l'objet d'une amende administrative pouvant aller jusqu'à 15 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 3 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent.

Si le règlement est applicable à partir du 2 Août 2026, les dispositions de ce chapitre sont **applicables dès le 2 février 2025**.

CHAPITRE III. PRATIQUES ENCADREES : SYSTEMES D'IA A HAUT RISQUE (ART. 6)

A. Classification des SIA à haut risque

Un système d'IA mis sur le marché ou mis en service, est considéré comme étant à haut risque lorsque les deux conditions suivantes sont remplies:

a) le système d'IA est destiné à être utilisé comme **composant de sécurité** d'un produit couvert par la législation d'harmonisation de l'Union dont la liste figure à **l'annexe I**, ou le système d'IA constitue lui-même un tel produit ;

b) le produit dont le composant de sécurité visé au point a) est le système d'IA, ou **le système d'IA lui-même en tant que produit**, est soumis à une évaluation de conformité par un tiers en vue de la mise sur le marché ou de la mise en service de ce produit.

Les **systèmes d'IA visés à l'annexe III du règlement** sont considérés comme étant à haut risque, notamment :

> Biométrie, Infrastructures critiques, éducation et formation professionnelle, emploi, gestion de la main-d'œuvre et accès à l'emploi indépendant, accès et droit aux services privés essentiels et aux services publics et prestations sociales essentiels (solvabilité, évaluation des risques et la tarification en ce qui concerne les personnes physiques en matière d'assurance-vie et d'assurance maladie, hiérarchisation des urgences des personnes physiques…), répression, migration, asile et gestion des contrôles aux frontières, administration de la justice et processus démocratique.

Ne sont pas considérés comme étant à haut risque, les SIA :

- visés à l'annexe III **lorsqu'ils ne présentent pas de risque important de préjudice pour la santé, la sécurité ou les droits fondamentaux des personnes physiques**, y compris en n'ayant pas d'incidence significative sur le résultat de la prise de décision (Art. 6, 3.).
- destinés à accomplir une **tâche procédurale étroite** (art. 6, § 3, a) ;
- destinés à **améliorer le résultat d'une activité humaine préalablement réalisée** (art. 6, § 3, b) ;
- conçus pour **détecter des modèles de prise de décision**, mais pas pour remplacer ou influencer fortement les décisions humaines (art. 6, § 3, c) ;

- ou destinés à **exécuter une tâche préparatoire en vue d'une évaluation pertinente** aux fins des cas d'utilisation visés à l'annexe III (art. 6, § 3, d).

Toutefois, **le profilage de personnes physiques est toujours considéré à haut risque** (art. 6, § 3).

B. Exigences essentielles des SIA à haut risque

Chaque système d'IA à haut risque doit posséder un **système de gestion des risques** qui doit être mis en œuvre, documenté et tenu à jour sur l'ensemble de son cycle de vie (art. 9).

Il doit prévoir :

- des mesures pour contrôler la **qualité et la gouvernance des données** concernant les données d'entraînement, de validation et de test, garantissant l'adéquation, l'exactitude et la fiabilité des données ainsi que le contrôle des biais (art. 10).
- La rédaction d'une **documentation technique** et la **journalisation** des évènements pertinents (art. 11 et 12).
- Des mesures de transparence, notamment pour les fournisseurs de SIA, leur permettant d'interpréter les sorties d'un système et de les utiliser de manière appropriée.
- Rédaction d'une **notice d'utilisation** contenant divers éléments d'information (Art.13).
- Un **contrôle humain effectif** par des personnes physiques (notamment au moyen d'outils d'interface homme-machine appropriés) (art. 14).
- Conception et développement permettant d'atteindre un niveau approprié **d'exactitude, de robustesse et de cybersécurité**, et de fonctionner de façon constante à cet égard tout au long de leur cycle de vie (art. 15).

  Les systèmes d'IA à haut risque doivent, notamment, :

  - Faire l'objet de **mesures techniques et organisationnelles** destinées à garantir la **résilience** en cas d'erreurs, de défaillances ou d'incohérences pouvant survenir au sein des systèmes eux-mêmes ou de l'environnement dans lequel ils fonctionnent, notamment en raison de leur interaction avec des personnes physiques ou d'autres systèmes ;
  - Être assortis de **solutions techniques redondantes**, telles que des plans de sauvegarde ou des mesures de sécurité après défaillance ;
  - **Résister aux tentatives d'agression de tiers non autorisés** visant à manipuler le jeu de données d'entraînement, modifier leur utilisation, leurs sorties ou leur performance en exploitant les vulnérabilités du système.

C. Obligations incombant aux fournisseurs et aux déployeurs de systèmes d'IA à haut risque

Les SIA sont considérés comme à « haut risque », lorsqu'ils présentent des risques pour la santé ou la sécurité, ou pour les droits fondamentaux, des personnes.

Ils font l'objet d'obligations à la charge de tous les opérateurs depuis leur conception, jusqu'à leur déploiement.

1. Obligations des fournisseurs (Art. 16)

Le « fournisseur », est désigné comme une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit (Art. 3.3).

Les fournisseurs de systèmes d'IA à haut risque doivent :

- indiquer sur le système d'IA à haut risque les éléments permettant leur **identification** ;
- veiller à ce que leurs systèmes d'IA à haut risque soient **conformes** aux exigences réglementaires relatives aux système de gestion de la qualité, la documentation, la journalisation automatique, la conformité, le marquage CE, et leur enregistrement ;
- prendre les **mesures correctives** et fournissent les **informations nécessaires**.

Le fournisseur établit une **déclaration UE de conformité** écrite, lisible par machine, signée à la main ou électroniquement concernant chaque système d'IA à haut risque et la tient à la disposition des autorités nationales compétentes pendant une durée de dix ans à partir du moment où le système d'IA à haut risque a été mis sur le marché ou mis en service (Art. 47).

Le **marquage CE** est apposé de façon visible, lisible et indélébile sur les systèmes d'IA à haut risque, éventuellement suivi du numéro **d'identification de l'organisme notifié responsable des procédures d'évaluation de la conformité (Art. 48)**.

Avant de mettre sur le marché ou de mettre en service un système d'IA à haut risque le fournisseur ou, selon le cas, **le mandataire s'enregistre dans la base de données** de l'UE visée à l'article 71 et procède également à **l'enregistrement de son système** (Art. 49).

Les fournisseurs établissent et documentent un **système de surveillance après commercialisation** d'une manière qui soit proportionnée à la nature des technologies d'IA et des risques du système d'IA à haut risque (Art. 72).

Les fournisseurs de systèmes d'IA à haut risque mis sur le marché de l'Union **signalent tout incident grave** aux autorités de surveillance du marché des États membres dans lesquels cet incident s'est produit (Art. 73).

Avant de mettre leurs systèmes d'IA à haut risque à disposition sur le marché de l'Union, les fournisseurs établis dans des pays tiers désignent, par mandat écrit, un **mandataire** établi dans l'Union (Art. 22).

2. Obligation des importateurs (Art. 23)

Les importateurs s'assurent que le système est conforme au règlement en vérifiant que:

- le fournisseur du système d'IA à haut risque a suivi la procédure pertinente d'évaluation de la conformité ;
- le fournisseur a établi la documentation technique conformément à l'article 11 et à l'annexe IV;
- le système porte le marquage CE requis et est accompagné de la déclaration UE de conformité et de la notice d'utilisation;
- le fournisseur a désigné un mandataire.

3. Obligation des déployeurs (Art. 26)

Le déployeur est celui qui utilise « sous sa propre autorité un système d'IA ».

Lorsqu'ils déploient un SIA à haut risque ils doivent notamment :

- prendre des mesures techniques et organisationnelles appropriées et confier le contrôle humain à des **personnes physiques qui disposent des compétences, de la formation et de l'autorité nécessaires** ainsi que du soutien nécessaire ;
- exercer un **contrôle sur la pertinence des données d'entrée** ;
- **surveiller le fonctionnement** de l'IA et détecter les risques ;
- assurer la **tenue de la journalisation** ;
- **coopérer** avec les autorités de police en cas d'infraction pénale.

> **En cas de prise de décisions concernant des personnes physiques, les déployeurs doivent informer ces personnes physiques qu'elles sont soumises à l'utilisation du SIA à haut risque.**

4. Responsabilités tout au long de la chaîne de valeur de l'IA (Art. 25)

Tout distributeur, importateur, déployeur ou autre tiers est considéré comme un fournisseur d'un système d'IA à haut risque et est soumis aux obligations incombant au fournisseur dans les circonstances suivantes :

a) il **commercialise sous son propre nom** ou sa propre marque un système d'IA à haut risque déjà mis sur le marché ou mis en service, sans préjudice des dispositions contractuelles prévoyant une autre répartition des obligations;

b) il apporte une **modification substantielle à un système d'IA à haut risque** qui a déjà été mis sur le marché ou a déjà été mis en service de telle manière qu'il reste un système d'IA à haut risque ;

c) il **modifie la destination d'un système d'IA**, y compris un système d'IA à usage général, qui n'a pas été classé à haut risque et a déjà été mis sur le marché ou mis en service de telle manière que le système d'IA concerné devient un système d'IA à haut risque conformément l'article 6.

Dans ces cas, le fournisseur qui a initialement mis sur le marché ou mis en service le système d'IA n'est plus considéré comme un fournisseur de ce système d'IA spécifique mais doit coopérer étroitement avec les nouveaux fournisseurs et mettre à disposition les informations nécessaires et l'accès technique nécessaires.

5. Analyse d'impact des systèmes d'IA à haut risque sur les droits fondamentaux (Art. 27)

Avant le déploiement d'un système d'IA à haut risque les déployeurs qui sont des organismes de droit public ou des entités privées fournissant des services publics et les déployeurs de systèmes d'IA à haut risque sont tenus d'effectuer **une analyse de l'impact sur les droits fondamentaux que l'utilisation de ce système peut produire**.

D. Autorités notifiantes et organismes notifiés

1. Autorités notifiantes

Chaque État membre désigne ou établit au moins une autorité notifiante chargée de mettre en place et d'accomplir les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et à leur contrôle (Art. 28).

Les organismes d'évaluation de la conformité soumettent une demande de notification à l'autorité notifiante de l'État membre dans lequel ils sont établis (Art. 29).

2. Organismes notifiés

Un organisme notifié est constitué en vertu du droit national d'un État membre et a la personnalité juridique, et doivent se conformer aux exigences en matière d'organisation, de gestion de la qualité, de ressources et de procédures qui sont nécessaires à l'exécution de leurs tâches, ainsi qu'aux exigences appropriées en matière de cybersécurité.

La structure organisationnelle, la répartition des responsabilités, les liens hiérarchiques et le fonctionnement des organismes notifiés garantissent la confiance dans leurs activités et la fiabilité des résultats des activités d'évaluation de la conformité menées par les organismes notifiés.

Les organismes notifiés sont indépendants :

- **du fournisseur du système d'IA à haut risque** pour lequel ils mènent les activités d'évaluation de la conformité ;
- de tout **autre opérateur ayant un intérêt économique** dans les systèmes d'IA à haut risque.

Un numéro d'identification unique est attribué à chaque organisme notifié.

Les organismes notifiés vérifient la conformité du système d'IA à haut risque conformément aux procédures d'évaluation de la conformité.

Si le règlement est applicable à partir du 2 Août 2026, ces dispositions sont applicables à compter du **2 février 2025**.

CHAPITRE IV. OBLIGATIONS DE TRANSPARENCE POUR LES FOURNISSEURS ET LES DEPLOYEURS DE CERTAINS SYSTEMES D'IA (ART. 50)

1. Les fournisseurs veillent à ce que les systèmes d'IA destinés à interagir directement avec des personnes physiques soient conçus et développés de manière que **les personnes physiques concernées soient informées qu'elles interagissent avec un système d'IA.**
2. Les fournisseurs de systèmes d'IA, y compris de systèmes d'IA à usage général, qui génèrent des contenus de synthèse de type audio, image, vidéo ou texte, veillent à ce que les sorties des systèmes d'IA soient **marquées dans un format lisible par machine et identifiables comme ayant été générées ou manipulées par une IA**.
3. Les **déployeurs d'un système de reconnaissance des émotions ou d'un système de catégorisation biométrique** informent les personnes physiques qui y sont exposées du fonctionnement du système et traitent les données à caractère personnel conformément à la règlementation.
4. Les déployeurs d'un système d'IA qui génère ou manipule des images ou des contenus audio ou vidéo constituant un hypertrucage, ou qui manipulent des textes publiés dans le but d'informer le public sur des questions d'intérêt public, indiquent que **les contenus ont été générés ou manipulés par une IA**.

CHAPITRE V. MODELES D'IA A USAGE GENERAL

A. Règles de classification

Les modèles d'IA à usage général peuvent être classés comme présentant un risque systémique lorsqu'ils sont à fort impact, et doivent être déclarés à la Commission.

B. Obligations incombant aux fournisseurs de modèles d'IA à usage général (Art. 53)

Les fournisseurs de modèles d'IA à usage général:

- élaborent et tiennent à jour la **documentation technique** du modèle, y compris son processus d'entraînement et d'essai et les résultats de son évaluation, avec un résumé détaillé ;
- mettent à disposition des **informations** et de la documentation à l'intention des fournisseurs de systèmes d'IA qui envisagent d'intégrer le modèle d'IA à usage général dans leurs systèmes d'IA ;

  Ces obligations ne s'appliquent pas aux fournisseurs de modèles d'IA qui sont publiés dans le cadre d'une licence libre et ouverte permettant de consulter, d'utiliser, de modifier et de distribuer le modèle et rendus publics, sauf s'ils présentent un risque systémique.
- mettent en place une politique visant à se conformer au droit de l'Union en matière de **droit d'auteur et droits voisins**.

A noter qu'avant de mettre un modèle d'IA à usage général sur le marché de l'Union, les fournisseurs établis dans des pays tiers désignent, par mandat écrit, un mandataire établi dans l'Union, lequel est habilité à accomplir certaines tâches incombant à son mandant et à servir d'interlocuteur, en plus ou à la place du fournisseur, au Bureau de l'IA ou aux autorités compétentes, pour toutes les questions liées au respect du présent règlement.

La Commission peut infliger aux fournisseurs de modèles d'IA à usage général des amendes n'excédant pas 3 % de leur chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, ou 15 000 000 EUR, le montant le plus élevé étant retenu, lorsque la Commission constate que le fournisseur, de manière délibérée ou par négligence a enfreint les dispositions du règlement.

C. Obligations incombant aux fournisseurs de modèles d'IA à usage général présentant un risque systémique (Art. 55)

Les fournisseurs de modèles d'IA à usage général présentant un risque systémique doivent également :

- effectuer une **évaluation des modèles** sur la base de protocoles et d'outils normalisés reflétant l'état de la technique ;
- **évaluer et atténuent les risques** systémiques éventuels au niveau de l'Union ;
- **Signaler les incidents graves** et leurs mesures correctives ;
- Garantir un niveau approprié de protection en matière de **cybersécurité**.

Ils peuvent s'appuyer sur des **codes de bonne pratique** pour démontrer qu'ils respectent leurs obligations, jusqu'à la publication d'une norme harmonisée. Le respect de ces normes confère au fournisseur une présomption de conformité dans la mesure où lesdites normes couvrent ces obligations.

Si le règlement est applicable à partir du 2 août 2026, ces dispositions sont applicables à compter du **2 février 2025**.

Sanctions :

Conformément aux conditions établies dans le présent règlement, les États membres déterminent le régime des sanctions et autres mesures d'exécution, qui peuvent également comprendre des avertissements et des mesures non monétaires, applicables aux violations du présent règlement commises par des opérateurs, et prennent toute mesure nécessaire pour veiller à la mise en œuvre correcte et effective de ces sanctions, tenant ainsi compte des lignes directrices publiées par la Commission.

Ces sanctions doivent être **effectives, proportionnées et dissuasives**. Elles tiennent compte des intérêts des PME, y compris les jeunes pousses, et de leur viabilité économique

Certaines sanctions spécifiques ont été rappelées dans le corps de la présente présentation.

Le présent règlement est applicable à partir du 2 août 2026, toutefois, certaines dispositions rappelées dans la présentation sont applicables dès le 2 février 2025.