



**HAL**  
open science

# L'AI Act, ou comment encadrer les systèmes d'IA en Europe

Antoine Boutet, Juliette Sénéchal, Margo Bernelin, William Letrone

► **To cite this version:**

Antoine Boutet, Juliette Sénéchal, Margo Bernelin, William Letrone. L'AI Act, ou comment encadrer les systèmes d'IA en Europe. The Conversation France, 2024. hal-04797429

**HAL Id: hal-04797429**

**<https://hal.science/hal-04797429v1>**

Submitted on 20 Jan 2025

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# L'AI Act, ou comment encadrer les systèmes d'IA en Europe

Margo Bernelin (*CNRS, Université de Nantes*)  
margo.bernelin@univ-nantes.fr

Antoine Boutet (*INSA Lyon, Inria, CITI*)  
antoine.boutet@insa-lyon.fr

William Letrone (*Université de Nantes*)  
william.letrone@univ-nantes.fr

Juliette Sénéchal (*Université de Lille, Inria*)  
juliette.senechal@univ-lille.fr

Depuis que les intelligences artificielles (IA) génératives, telles que ChatGPT pour le texte ou Stable Diffusion pour les images, sont entrées dans nos vies, elles ne laissent personne indifférent et suscitent fascination et crainte. Une machine peut en effet accomplir certaines tâches mieux qu'un humain, mais aussi commettre des erreurs. Entre les mains d'acteurs malintentionnés, une IA peut aussi servir à réaliser des deepfakes (contenus trompeurs) ou à influencer un résultat électoral.

Si laisser une machine résumer un texte semble peu risqué, la prise de décision automatisée par IA dans des contextes plus ou moins sensibles nécessite d'évaluer les risques et de les encadrer. Alors que le secteur de l'IA connaît une expansion fulgurante, la question de la réglementation de l'IA devient un sujet de préoccupation majeur pour les États<sup>1</sup>. C'est donc dans ce contexte de course à l'encadrement que l'Union européenne (UE) entend promouvoir sa vision de la réglementation sur l'IA avec l'AI Act.

## Pourquoi l'AI Act ?

Si l'UE manque encore de fleurons qui pourraient lui permettre de concurrencer les États-Unis et la Chine, il est un terrain où elle peut véritablement s'affirmer

---

<sup>1</sup><https://verfassungsblog.de/biden-bletchley-and-the-emerging-international-law-of-ai/>

: celui de la régulation <sup>2</sup>. En effet, au travers de l’AI Act, l’UE se met ainsi en capacité d’imposer ses règles aux autres acteurs en conditionnant l’accès au marché européen au respect de ses valeurs. C’est une étape décisive vers son objectif d’incarner un modèle de réglementation.

L’approche européenne s’articule autour du concept d’IA digne de confiance (ou trustworthy AI) et vise à faire de l’UE la pionnière des IA légales, éthiques et robustes <sup>3</sup>. Selon Carme Artigas, secrétaire d’État espagnole à la numérisation et à l’intelligence artificielle, il s’agit de stimuler l’innovation et l’adoption de l’intelligence artificielle dans toute l’Europe tout en respectant pleinement les droits fondamentaux de nos citoyens. Le défi est de taille, tant les enjeux politiques, économiques, et sociaux sont considérables<sup>4</sup>. Le 13 mars dernier, les ambitions de l’UE se sont concrétisées avec l’adoption par le Parlement européen de l’AI Act au terme d’une longue procédure.

L’AI Act dans sa version préfinale<sup>5</sup> prévoit des obligations variables en fonction du système ou du modèle d’IA et de son impact. L’étendue des obligations s’imposant aux fournisseurs et utilisateurs est proportionnelle aux risques d’atteinte aux droits fondamentaux posés par ces derniers. Ce faisant, il distingue entre les dispositifs d’IA posant des risques inacceptables pour les Européens, ceux posant des risques systémiques, ceux à haut risque, et enfin les dispositifs à risques faibles ou limités.

## Une réglementation qui distingue différents niveaux de risque

Le règlement interdit d’abord les pratiques posant des risques inacceptables. Il s’agit des systèmes les plus intrusifs dont les usages peuvent avoir des conséquences néfastes démesurées sur les droits des usagers, comme l’utilisation de systèmes d’IA à des fins de manipulation pour influencer le comportement des individus (scandale Cambridge Analytica, analyse des données personnelles d’électeurs afin d’influencer leurs intentions de vote), les systèmes d’IA permettant de mettre en place un crédit social, et, sauf exception, les dispositifs d’identification à distance des personnes sur la base de caractéristiques personnelles comme la reconnaissance faciale algorithmique.

Ajoutés tardivement dans le règlement, les modèles de fondation<sup>6</sup> (ou general-purpose AI models), de grands modèles d’intelligence artificielle exploitant de

<sup>2</sup><https://www.ege.fr/infoguerre/ai-act-la-course-europeenne-par-la-norme-face-au-leadership-americain-en-matiere>

<sup>3</sup><https://www.consilium.europa.eu/fr/press/press-releases/2023/12/09/>

<sup>4</sup><https://www.accessnow.org/wp-content/uploads/2018/11/AI-and-Human-Rights.pdf>

<sup>5</sup>[https://www.linkedin.com/posts/dr-laura-caroli-0a96a8a\\_ai-act-consolidated-version-activity-7155181240751374336-B3Ym/](https://www.linkedin.com/posts/dr-laura-caroli-0a96a8a_ai-act-consolidated-version-activity-7155181240751374336-B3Ym/)

<sup>6</sup>[https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS\\_ATA\(2023\)745708\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA(2023)745708_EN.pdf)

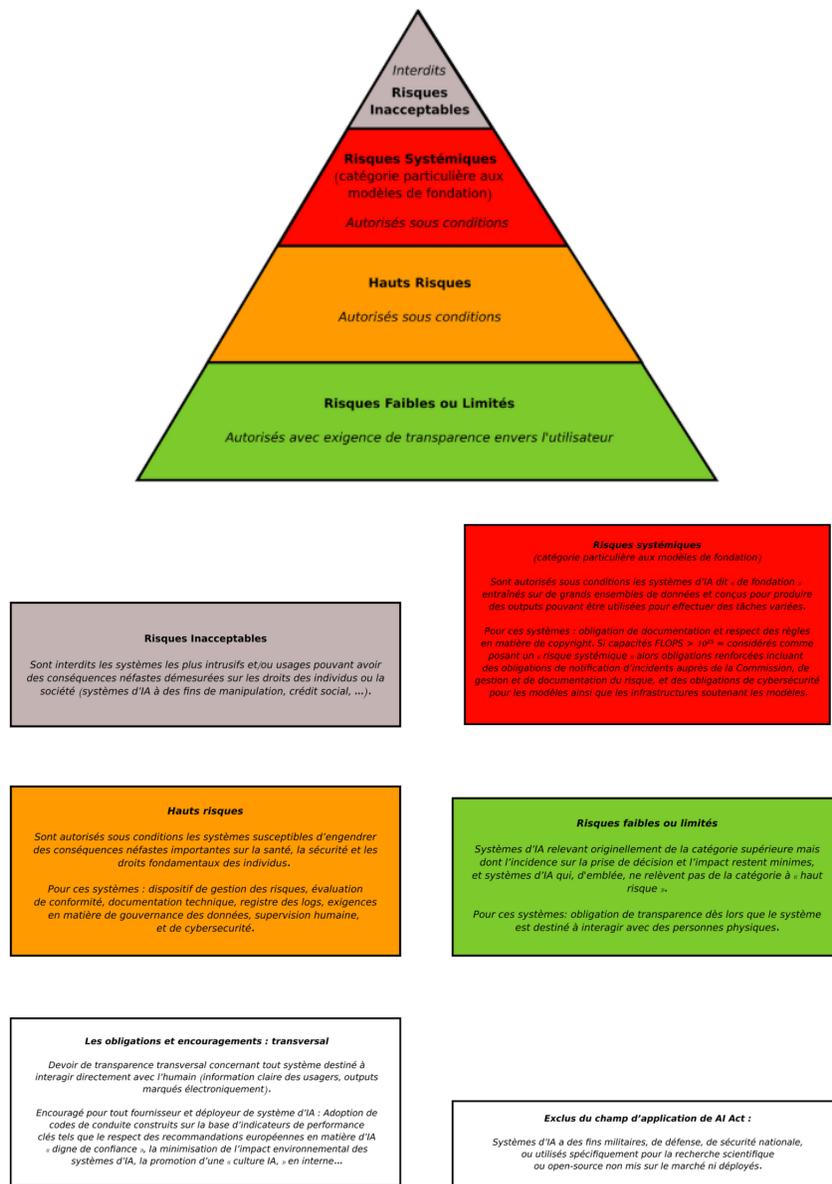


Figure 1: Classification des risques de l'IA selon l'UE.

larges quantités de données et pouvant être adaptés pour effectuer plusieurs types de tâches, font l'objet d'un régime distinct. En fonction de leurs capacités, ils pourront être considérés comme posant un risque systémique. Cette catégorie concerne notamment ChatGPT dans sa version actuelle. Les

fournisseurs de modèles posant un risque systémique seront soumis à des obligations renforcées par rapport aux autres modèles de fondation (entre autres, obligation de notification d'incidents de cybersécurité auprès de la Commission).

La catégorie des systèmes d'IA à haut risque s'applique aux systèmes susceptibles d'engendrer des conséquences néfastes importantes sur la santé, la sécurité et les droits fondamentaux des individus. L'utilisation de systèmes d'IA dans les procédures de recrutement, la détermination de l'obtention de droits sociaux ou de l'octroi de l'asile... relèvent de cette catégorie. Cette classification se traduit par des obligations variées allant de l'établissement d'un système de gestion des risques robuste, au maintien d'une documentation technique exhaustive, en passant par le respect des exigences en matière de gouvernance des données, de supervision humaine et de cybersécurité.

Les dispositifs à risques faibles ou limités restent quant à eux soumis à l'obligation de transparence commune à tout système destiné à interagir directement avec les personnes. Cette catégorie concerne surtout les systèmes d'IA ayant une influence minimale sur la prise de décision et inclut les systèmes cantonnés à des tâches très spécifiques comme la classification de dossier ou la correction orthographique.

## Un texte bienvenu mais imparfait

La gouvernance de ce cadre sera assurée par un nombre conséquent d'institutions européennes et nationales, à l'image du Comité européen de l'intelligence artificielle et du Bureau européen de l'IA, questionnant la lisibilité du dispositif. En France, la Commission nationale de l'informatique et des libertés (CNIL) s'est déjà positionnée en renforçant son expertise sur l'IA, laquelle se traduit notamment par la publication de fiches de recommandation pour le développement et le déploiement des systèmes d'IA.

Le texte était largement attendu, notamment par les acteurs de l'industrie créative<sup>7</sup>, mais aussi par des juristes et organismes indépendants<sup>8</sup>. Pourtant, l'adoption du texte n'a pas été simple, la France, l'Allemagne et l'Italie se montrant particulièrement réticentes<sup>9</sup> à l'égard des dispositions portant sur les modèles de fondation, y voyant un frein potentiel au développement de l'IA en Europe. Dans ce domaine, le règlement ne semble pas satisfaire toutes les parties.

Il est notamment reproché à l'AI Act<sup>10</sup> de proposer une définition inadéquate

<sup>7</sup><https://www.digitalmusicnews.com/2024/02/01/ifpi-ai-act-support/>

<sup>8</sup><https://amnesty.ca/human-rights-news/eu-must-ban-dangerous-ai-powered-technologies-in-historic-ai-act/>

<sup>9</sup><https://edri.org/our-work/council-to-vote-on-eu-ai-act-whats-at-stake/>

<sup>10</sup><https://thefuturesociety.org/wp-content/uploads/2023/09/heavy-is-the-head-that-wears-the-crown.pdf>

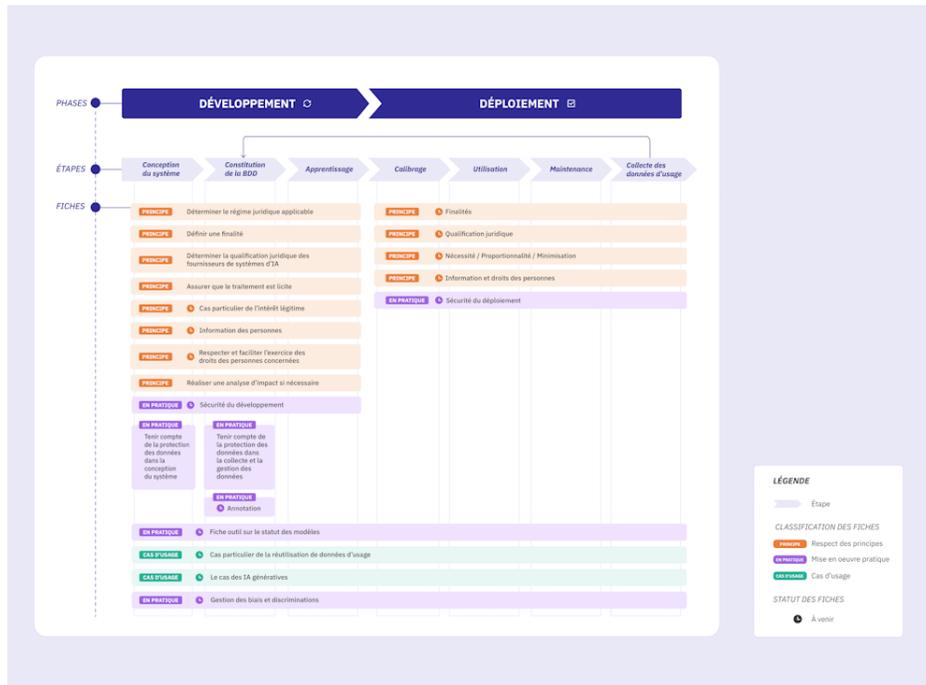


Figure 2: Cartographie des fiches de recommandations pour le développement et le déploiement des systèmes d'IA de la CNIL (CNIL, CC BY-NC).

des modèles de fondation à risque systémique, une insuffisance à laquelle le Bureau européen de l'IA (chargé entre autres d'éclairer la mise en œuvre de l'AI Act) devra pallier rapidement. Par ailleurs, plusieurs compromis ont été critiqués comme pouvant donner lieu à des abus, comme la possibilité laissée aux États d'utiliser des dispositifs d'identification biométrique en temps réel pour des motifs de sécurité nationale.

## Combiner l'AI Act et les textes déjà en vigueur

En outre, la mise en conformité au règlement, en particulier pour les systèmes à haut risque, est subordonnée au respect de standards techniques relatifs à la qualité des systèmes, à leur sécurité ou encore à la gouvernance des données qui reste encore à déterminer. Dans cette perspective, les efforts s'intensifient pour proposer des standards techniques pertinents.

Enfin, l'AI Act n'épuise pas toutes les questions soulevées par l'IA ni les besoins d'encadrement. Il faudra donc combiner sa lecture avec d'autres textes comme le Règlement général sur la protection des données (RGPD) dans le cas d'IA impliquant un traitement de données personnelles, ou le Règlement sur les

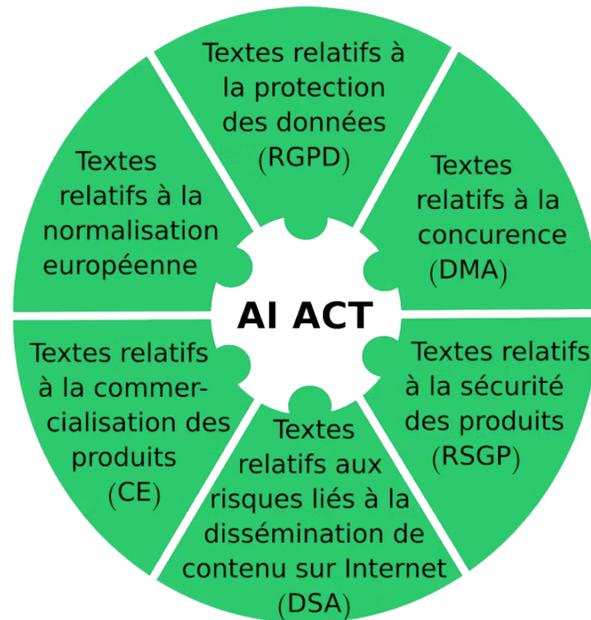


Figure 3: L'AI Act fonctionnera en synergie avec d'autres textes européens.

services numériques (ou Digital Services Act – DSA) et le Règlement sur les marchés numériques (ou Digital Market Act – DMA) dans le cas d'IA intégrées à des plates-formes de services.

Quoiqu'il en soit, en Europe comme ailleurs, il n'est plus question de laisser les grandes sociétés de l'IA s'autoréguler. Reste à espérer que la phase de mise en œuvre parvienne à réduire les zones d'ombres qui subsistent à ce stade.