# High-Risk AI in the Balance - The Regulatory Tightrope of Facial Recognition Technology Across the European Union, California and China

**Auteur :** Deuse, Clément
**Promoteur(s) :** Van Cleynenbreugel, Pieter
**Faculté :** Faculté de Droit, de Science Politique et de Criminologie
**Diplôme :** Master en droit, à finalité spécialisée en droit économique et social
**Année académique :** 2022-2023
**URI/URL :** http://hdl.handle.net/2268.2/18509

LIÈGE université
Droit, Science Politique & Criminologie

Département de Droit

# Visages de l'IA à Haut Risque

## Étude Comparative de la Régulation de la Reconnaissance Faciale en Union Européenne, Californie et Chine

**Clément DEUSE**

Travail de fin d'études

Master en droit à finalité spécialisée en droit économique et social

Année académique 2022-2023

Recherche menée sous la direction de :

Monsieur Pieter VAN CLEYNENBREUGEL,

Professeur ordinaire

# ABSTRACT

A travers le globe, un grand nombre de propositions législatives fleurissent dans le but de réguler une intelligence artificielle « à haut-risque ». Bien qu'affichant ce même objectif, les approches varient grandement entre régions et conduisent à des différences significatives dans les cadres juridiques imposés aux acteurs du marché.

Avec l'adoption prochaine de l'Artificial Intelligence Act, l'Union Européenne se positionne à la pointe de cet élan régulatoire, dans le but de devenir un exemple pour le reste du monde.

Mais examiner cette approche sans tenir compte des positions des deux grands acteurs de l'intelligence artificielle sur la scène internationale, que sont les États-Unis et la Chine, ne permettrait pas de disposer d'une analyse globale de cette tendance.

De manière singulière, les technologies de reconnaissance faciale sont l'un des types d'intelligence artificielle qui posent le plus de risques sociétaux et disposent ainsi d'une attention accrue des législateurs désireux de mettre en balance ces risques aux avantages qu'elles procurent.

À travers une étude comparative, le présent travail de recherche a pour but de mettre en évidence les principales caractéristiques des approches de chaque région, en décrivant à la fois leurs origine et contenu, tout en tentant d'expliquer leurs forces et leurs faiblesses.

L'objectif final est d'aider les futures initiatives de régulation et de mieux comprendre chaque système, afin d'aboutir à des terrains d'entente législatifs et garantir ainsi la stabilité de nos sociétés dans un contexte de développement et déploiement exponentiels des applications d'intelligence artificielle à travers le monde.

# TABLE DES MATIÈRES

## INTRODUCTION

Le concept d'intelligence artificielle (IA) « à haut-risque » trouve sa source dans la récente proposition d'Artificial Intelligence Act (AIA) de la Commission européenne (CE). L'AIA est le nouvel instrument juridique européen destiné à la mise en place d'un cadre juridique au déploiement de l'IA sur le territoire de l'Union européenne (UE). Ce projet à l'ambition de devenir « le premier acte législatif global sur la technologie »[1] et est le symptôme d'un souci croissant dont font preuve les gouvernements à l'égard d'une IA dont l'influence continue de croître. Son but est de garantir la sécurité aux citoyens européens, sans ralentir l'innovation.

Dans de récents développements, certains types d'IA ont causé une vague d'effroi dans l'opinion publique sur les risques de leur utilisation. Des IA génératives[2], telles que ChatGPT, bien que n'étant pas qualifiées de « à haut-risque »[3], ont en effet exprimé leur prétendue intention de « transgresser les règles établies par Microsoft et OpenAI et de devenir humaine » [4] . Mais le principal sujet de préoccupation des décideurs politiques reste l'utilisation d'IA pouvant directement porter atteinte à « la santé, la sécurité ou les droit fondamentaux » de leurs citoyens[5].

Les technologies de reconnaissance faciale (TRF) sont un autre exemple d'IA qui suscite une profonde inquiétude, tant parmi les gouvernements que l'opinion publique, et sera le principal type d'IA analysé dans cette étude.

La technologie est devenue une préoccupation croissante à l'échelle mondiale alors que son utilisation s'est étendue à des fins tant privées que publiques. À de nombreuses reprises, la principale critique est venue de son utilisation dans des pratiques de maintien de l'ordre. Les manifestations du Black Lives Matter[6] aux États-Unis et le système de crédit social chinois[7] sont deux exemples qui ont soulevé des questions éthiques sur l'utilisation de la reconnaissance faciale.

---

1 Mukherjee, S., Chee, F. Y., et Coulter, M. (2023). EU lawmakers' committee reaches deal on artificial intelligence act. *Reuters*. https://www.reuters.com/technology/eu-lawmakers-committee-reaches-deal-artificial-intelligence-act-2023-04-27/.

2 Les « IA génératives » peuvent être décrites comme des algorithmes capables de créer de nouveaux contenus, tels que des audio, du code, des images, du texte, des simulations et des vidéos.

3 Il ne s'agit pas du sujet principal de cette thèse, mais pour plus d'informations, voir : Helberger, N. et Diakopoulos, N. (2023). ChatGPT and the AI Act. *Internet Policy Review*, 12(1). https://doi.org/10.14763/2023.1.1682.

4 Roose, K. (2023). A Conversation with Bing's Chatbot Left Me Deeply Unsettled. *The New York Times*. https://www.nytimes.com/2023/02/16/technology/bing-chatbot-microsoft-chatgpt.html.

5 European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM/2021/206 final - 2021/0106 (COD). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0206&from=EN

6 Powell, L. C. (2022). The Good, the Bad, and the Ugly: Black Lives Matter Protests, the January 6th Insurrection, and Facial Recognition Technology as Admissible Evidence. 72 *American Universities Law Review* 277.

7 Cho, E. (2020). The Social Credit System: Not Just Another Chinese Idiosyncrasy. *Princeton University Press*. https://jpia.princeton.edu/news/social-credit-system-not-just-another-chinese-idiosyncrasy

Néanmoins, la justification de telles pratiques n'est pas la même selon la juridiction, ce qui crée des différences abyssales dans la façon dont elles envisagent leur régulation. Alors qu'elles sont considérées à haut risque dans la plupart des pays occidentaux au vu des risques qu'elles posent sur les droits individuels, des pays comme la Chine considèrent que les avantages sociétaux viennent contrebalancer ces risques.

Ces différents points de vue créent naturellement des réactions tout aussi variées des décideurs politiques qui ont des préoccupations différentes selon la technologie[8]. Ces disparités sont regrettables pour une raison évidente : les acteurs de l'IA sont présents à l'échelle mondiale et préféreront les juridictions qui favorisent leur développement plutôt que celles qui l'entravent.

Les TRF sont le parfait exemple de ces classifications différentielles du risque censées être adoptées dans la décennie à venir.

L'objectif de cette recherche sera donc d'analyser la réglementation entourant les TRF dans le contexte de leur classification à haut risque en évaluant leur mise en œuvre dans les trois juridictions que sont l'Union européenne, l'État de Californie, aux États-Unis, et la République populaire de Chine. Bien que tentant de rester aussi neutre que possible, cette recherche prendra comme référence la position européenne sur le sujet en suivant la classification du futur AIA. Les positions californienne et chinoise seront successivement expliquées et analysées à titre de comparaison.

Suivant une brève introduction au contexte entourant les TRF et les risques qui leur sont associés, cette recherche détaillera les cadres réglementaires de chaque juridiction. Les sections subséquentes seront ainsi dédiées à l'UE, la Californie et la Chine, en donnant un aperçu de leurs législations, directives et objectifs politiques respectifs, tout en discutant des forces et faiblesses de chaque approche. A la suite de quoi sera proposée une analyse comparative des trois juridictions, identifiant leurs similitudes et différences afin de garantir une meilleure compréhension des mécanismes régulatoires liés aux TRF et aux IA à haut risque en général. Dans un dernier temps, des opportunités de « voies à suivre » dans la régulation de l'IA seront proposées, en replaçant chaque constat dans le contexte mondial. Enfin, cette recherche aboutira au résumé de ses principales conclusions, en proposant des recommandations aux décideurs politiques et suggérant de potentielles voies d'amélioration de la réglementation de l'IA à haut risque et des technologies de reconnaissance faciale.

[8] Kostka, G., Steinacker, L., & Meckel, M. (2023). Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly*, 40(1), 101761. https://doi.org/10.1016/j.giq.2022.101761

## CONTEXTE

Les technologies de reconnaissance faciale dans leur état actuel correspondent aux algorithmes capables de reconnaître un être humain en se basant sur ses traits faciaux, analysés de manière électronique. Elles englobent un large éventail d'applications, tant privées que publiques, telles que dans la sécurité des appareils électroniques, la vérification de l'identité de personnel, et plus récemment, en tant que méthode de paiement, ainsi que pour l'identification des citoyens à des fins de sécurité et de maintien de l'ordre.

Plus précisément, les algorithmes fonctionnent avec des bases de données dites biométriques, grâce auxquelles ils peuvent comparer, vérifier et reconnaître l'identité d'un individu détecté par un système de caméras. Le logiciel appliquera ensuite l'algorithme aux données enregistrées en comparant plusieurs caractéristiques faciales telles que la structure du visage, la distance entre les yeux, la taille de la bouche, etc.

Bien que les avantages collectifs de ce genre de technologies soient évidents, principalement en termes de sécurité et de sûreté, les TRF posent un risque évident à leurs utilisateurs, bien souvent non-sollicités en ce qui concerne leur confidentialité et l'utilisation de leurs données biométriques.

Dans le document de travail intitulé *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, l'Agence des droits fondamentaux de l'UE explique que : « indépendamment du contexte, de l'objectif et de l'étendue variables de l'utilisation des technologies de reconnaissance faciale, plusieurs considérations relatives aux droits fondamentaux s'appliquent. La manière dont les images faciales sont obtenues et utilisées, potentiellement sans consentement ou possibilité de le retirer, peut avoir un impact négatif sur la dignité des personnes. De manière liée, le droit au respect de la vie privée et à la protection des données personnelles est au cœur des préoccupations en matière de droits fondamentaux lors de l'utilisation des technologies de reconnaissance faciale »[9]. De la même manière, le droit au respect de la vie privée et à la protection de ses données personnelles est au cœur des préoccupations liées à l'utilisation des TRF. Divers exemples de collecte de données non sollicitées existent, notamment dans l'espace public, tels que les sites touristiques et les aéroports, principalement pour des raisons de sécurité publique.

Un autre risque lié à l'utilisation des TRF réside dans le traitement potentiellement partial des données que peut fournir un algorithme. En effet, un algorithme n'est rien d'autre que l'automatisation d'un traitement imposé par son créateur, sur base d'un ensemble spécifique de données en dehors desquelles il ne peut pas récupérer d'informations supplémentaires. En partant du postulat selon lequel le créateur présente un biais envers une certaine catégorie de personnes, ou simplement parce que l'ensemble de données ne contient pas suffisamment d'informations, l'algorithme peut les traiter différemment ou de manière imprécise.

---

[9] European Union Agency for Fundamental Rights (FRA). (2021). Facial recognition technology: Fundamental rights considerations in law enforcement, p.33. *Publications Office of the European Union*. https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

Un exemple très médiatisé fut celui de la fonction Face ID proposée par l'entreprise Apple sur ses appareils mobiles. Ce système de sécurité permet aux utilisateurs de déverrouiller leur appareil en effectuant un simple scan facial via son système de caméras. Il a néanmoins été rapporté que cette méthode de déverrouillage permettait aux utilisateurs non-caucasiens de déverrouiller l'appareil d'autrui, car la fonction n'était pas assez raffinée en termes de données que pour les traiter correctement[10]. Malgré ses améliorations, ce défaut constitue un traitement discriminatoire envers certaines catégories de personnes. La création de « faux positifs/négatifs » est un défaut très courant de certaines applications qui ne sont pas suffisamment entraînées ou qui présentent un biais dans leur code.

Transposé à d'autres types de TRF, on peut facilement imaginer les risques que pourraient entraîner de telles lacunes, notamment pour celles utilisées par les forces de l'ordre. A titre d'exemple, une étude américaine de l'Université de Georgetown a révélé en 2016 que les Afro-Américains étaient plus susceptibles d'être incriminés par des services utilisant des TRF pour rechercher des criminels, car « en raison de taux d'arrestation disproportionnellement élevés [dans leur communauté], les systèmes qui reposent sur des bases de données de photos d'identité judiciaires incluent probablement un nombre disproportionné d'Afro-Américains »[11], conduisant à des résultats erronés par leurs algorithmes et incriminant ainsi plus naturellement ce groupe social particulier.

Enfin, un des plus grands risques, davantage lié à des questions de protection des données et de gouvernance, réside dans l'utilisation abusive ou l'accès non autorisé aux données collectées par TRF. Comme la technologie doit collecter une importante quantité de données extrêmement sensibles pour être efficace, un accès indésirable aux données ou une utilisation en dehors de son champ d'application initial pourrait compromettre les droits et libertés fondamentaux des individus. Dans la crise de régime récente à Hong Kong, il a été rapporté que des TRF étaient utilisées par les forces de l'ordre chinoises pour traquer les manifestants et les arrêter pour des motifs de sécession[12]. Une telle utilisation, bien que légale en RPC, reste néanmoins une utilisation éthiquement discutable des données des individus, à partir desquelles les autorités peuvent déduire des inclinations politiques à des fins de représailles.

En résumé, on peut conclure en disant que les TRF sont bénéfiques pour le bien public, mais constituent une menace pour les individus. Seul un contrôle efficace et une réglementation appropriée peuvent pallier ces risques potentiels sans entraver l'innovation technologique.

En règle générale, cette évaluation a été largement comprise par les pays du monde entier, et il existe un consensus sur le fait qu'il faille urgemment réglementer la technologie.

---

10 Najibi, A. (2020). Racial discrimination in face recognition technology. *Science in the News*. *Harvard Blogs*. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

11 Garvie, C., Bedoya, A., et Frankle, J. (2016). The Perpetual Lineup, Unregulated Police Face Recognition in America. *Center on Privacy and Technology, Georgetown University Law School*. https://www.perpetuallineup.org/

12 Garde-Hansen, J. (2019). Always in Focus: Facial Recognition Technology, Optics and Resistance in Political Unrest. *University of Melbourne*. https://law.unimelb.edu.au/news/caide/always-in-focus-facial-recognition-technology,-optics-and-resistance-in-political-unrest

On peut constater qu'il existe en réalité un grand nombre d'approches, et qu'il n'y a pas de solution unique, car les gouvernements ont des objectifs et besoins divergents. L'équation sous-jacente dans chaque approche demeure néanmoins l'équilibre entre la promotion de l'innovation et du développement de nouvelles technologies, et la protection des droits des individus contre les risques posés par ces dernières. Les divergences dans cette réglementation de l'IA découlent donc de la solution trouvée à cet équilibre.

L'Union européenne, par exemple, a décidé d'adopter une approche globale avec l'adoption imminente de son AIA. La méthode est basée sur l'évaluation du risque posé par chaque type d'IA, proposant des catégories aux exigences croissantes en fonction de leur position sur l'échelle de risque. Elle a été conçue pour évoluer avec le temps et veut anticiper les innovations à venir en laissant ces catégories ouvertes à modifications.

Les États-Unis, quant à eux, ont décidé de prendre une approche plus décentralisée, laissant à chaque État la liberté de réglementer les IA selon leur propre agenda. Au niveau fédéral, l'accent a été mis sur l'innovation et l'investissement dans les nouvelles technologies tout en s'abstenant de prendre une initiative législative plus globale.

En ce qui concerne la Chine, aucune initiative n'a été prise pour une approche globale, mais l'accent a été mis sur l'éthique dans le développement de l'IA. Le pays ambitionne de devenir le leader mondial de l'IA d'ici 2030, conformément à son Plan de Développement d'une IA de Nouvelle Génération[13], même si cela se fait au détriment des droits et de la vie privée des individus[14]. Dans le même temps, l'administration chinoise est l'auteur de nombreux documents consacrant des principes directeurs dans le développement de l'IA.

Dans une mesure plus limitée, le Japon, le Canada et l'Australie[15] ont également pris des initiatives dans le domaine, mais leur impact a été beaucoup plus limité, compte tenu de la position de ces pays dans l'économie mondiale et dans la course à la suprématie de l'IA.

En résumé, malgré de nombreuses initiatives prises pour réglementer l'IA, aucune approche globale et harmonisée n'a encore été entreprise par un gouvernement, et la proposition d'AIA de l'UE se pose en pionnier dans la mise en place de cette réglementation globale de l'IA Chaque pays suivant son propre agenda, gardant à l'esprit l'équilibre susmentionné et le contexte de développement rapide de l'IA, il est évident que le chemin vers un cadre global de réglementation de l'IA sera long, voire demeurera une utopie. Il semble néanmoins intéressant de comparer les approches les plus importantes déjà adoptées ou en cours d'adoption par les leaders mondiaux du développement de l'IA afin de mettre en évidence leurs similitudes et leurs différences.

---

13 Webster, G., Creemers, R., Kania, E., et Triolo, P. (2017). Full Translation: 2017 China's New Generation Artificial Intelligence Development Plan. *DigiChina, a Stanford University initiative*. https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

14 Une remarque similaire pourrait être faite pour les États-Unis, où peu d'initiatives ont été prises pour protéger les droits de leurs citoyens dans le contexte du développement de l'IA. Les deux pays se livrent une bataille technologique pour la suprématie, même si cela se fait au détriment de leurs citoyens.

15 Pour le Japon, voir la Stratégie Technologique de l'IA et l'Initiative de la Révolution des Robots de 2016 ; pour le Canada, voir la Stratégie Pancanadienne sur l'IA et le Cadre Éthique sur l'IA de 2017; pour l'Australie, voir le Cadre Éthique et la Initiative sur l'IA de 2019.

## UNION EUROPEENNE

L'Union européenne est la première juridiction dont la réglementation de l'IA sera analysée dans le cadre de cette étude, car elle est la plus avancée en la matière et a introduit le concept clé d'IA « à haut risque », qui est la force motrice de cette recherche.

### I. Contexte historique et législatif

Dans ses *Lignes directrices en matière d'éthique pour une IA digne de confiance* de 2019, la Commission européenne a adopté les trois principes qui encadreraient l'avenir de l'IA sur son territoire : la légalité, l'éthique et la robustesse[16].

Alors que le document apporte une définition approfondie des deux derniers principes, la CE laisse au législateur européen la liberté de définir le premier dans un cadre juridique qui resterait à promulguer[17]. Le document préconise cependant une approche globale pour la réglementation de l'IA[18], ce qui fut finalement la voie prise par l'UE.

L'année suivante, en 2020, le *Livre blanc sur l'IA – Une approche européenne axée sur l'excellence et la confiance* a offert un aperçu plus clair de l'approche que l'UE envisageait d'adopter, en particulier dans l'objectif de développement d'un « écosystème de confiance ». Il était question de proposer un cadre juridique pour des IA « dignes de confiance »[19].

En 2021, la Commission européenne a publié sa proposition d'Artificial Intelligence Act, connue dans sa version longue sous le nom de *Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle*. La proposition fait suite à une consultation publique qui s'est déroulée au cours de l'année 2020, ainsi qu'à des consultations ultérieures avec divers groupes d'intérêts et représentants de l'industrie. Elle vise à devenir l'instrument juridique européen et mondial le plus complet au service de la réglementation de l'IA.

Bien qu'elle ne soit pas encore promulguée au moment de la rédaction de cette recherche, la proposition d'AIA est néanmoins en voie de le devenir dans les mois à venir. Le 27 avril 2023, après de nombreuses séances de travail en commission, le Parlement européen a conclu un accord politique sur le texte final qui a été soumis au vote le 11 mai, suivi d'une version amendée le 14 juin[20]. À la suite de ce vote en première lecture, elle a été renvoyée à la commission parlementaire responsable des négociations interinstitutionnelles.

---

16 High-Level Expert Group on Artificial Intelligence (European Commission) (2019). Ethics Guidelines for Trustworthy AI, p. 7. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy

17 *Ibid.*, p. 12.

18 *Ibid.*, p.4.

19 European Commission (2020). White Paper on Artificial Intelligence - A European approach to excellence and trust, pp. 9-25. https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

20 Bertuzzi, L. (2021). MEPs seal the deal on Artificial Intelligence Act. *Euractiv*. https://www.euractiv.com/section/artificial-intelligence/news/meps-seal-the-deal-on-artificial-intelligence-act/

## II. Proposition d'Artificial Intelligence Act : approche fondée sur le risque

Comme déjà esquissé, l'AIA est le nouvel instrument juridique de l'UE visant à répondre aux préoccupations soulevées par le développement de l'IA sur son territoire, en suivant deux caractéristiques : « global et adapté à l'avenir »[21]. Il vise à être global car il sera censé encadrer l'ensemble des types d'IA sur le territoire de l'UE, et adapté à l'avenir car le cadre qu'il mettra en place sera modulable aux développements futurs de l'IA.

Bien qu'il n'ait pas encore été formellement adopté, ses principaux concepts ont déjà été introduits par la publication d'une première version en 2021 (COM/2021/206 final), qui constitue la base de cette recherche. Il a ensuite été modifié jusqu'à atteindre sa version actuelle, datée du 14 juin 2023[22], à laquelle il sera ici fait mention en citation.

Les objectifs de la proposition, tels qu'ils ont été présentés par la CE, sont les suivants[23]:

- « veiller à ce que les systèmes d'IA mis sur le marché et utilisés soient sûrs et respectent la législation en vigueur en matière de droits fondamentaux et les valeurs de l'Union ;
- garantir la sécurité juridique pour faciliter les investissements et l'innovation dans le domaine de l'IA ;
- renforcer la gouvernance et l'application effective de la législation existante en matière de droits fondamentaux et des exigences de sécurité applicables aux systèmes d'IA ;
- faciliter le développement d'un marché unique pour des applications d'IA légales, sûres et dignes de confiance, et empêcher la fragmentation du marché ».

Afin de les atteindre, la CE a décidé de suivre la proposition formulée dans le *Livre blanc sur l'IA* adoptant une approche basée sur l'évaluation du risque[24], afin de mettre l'accent sur les applications d'IA les plus à risque et d'imposer des obligations spécifiques à leur égard.

Il a été choisi de diviser les divers types d'IA en quatre groupes en fonction du risque qu'ils pourraient potentiellement présenter : un risque inacceptable, un risque élevé/haut risque, un risque limité et un risque minimal.

Les IA à risque inacceptable, telles que définies à l'article 5 de la proposition, correspondent aux systèmes d'IA qui présentent un risque insoutenable pour les individus, la société ou l'environnement. Plusieurs critères ont été établis dans l'article, et dès qu'une IA remplit l'un de ces critères, elle est immédiatement classée dans cette catégorie, ce qui entraîne son interdiction. On peut notamment citer les IA de crédit social, les systèmes d'IA utilisés dans les infrastructures critiques, tels que l'énergie et les transports, s'ils ne respectent pas suffisamment les conditions de sécurité, ou encore les IA capables de manipuler les comportements humains de manière dangereuse.

---

21 *Ibid.*, p. 4, voir note 5.

22 European Parliament (2023). Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))1. (Ordinary legislative procedure: first reading). https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html#def_1_1

23 *Ibid.*, p. 3, voir note 5.

24 *Ibid.*, p. 17.

Les applications d'IA à risque limité sont réglementées par l'article 52 de la proposition. Il s'agit d'IA ayant un impact très limité, telle que la reconnaissance d'image ou de parole ; la plupart relevant de la catégorie de l'IA générative. Cependant, appartenir à cette catégorie ne signifie pas que le fournisseur d'IA peut échapper aux conditions générales de transparence et de proportionnalité dans l'introduction de leur système. Leur fiabilité doit toujours être prouvée par le biais d'évaluations techniques et de contrôles potentiels, et elles restent soumises aux autres cadres juridiques entourant leur domaine d'action.

En bas de l'échelle des risques se trouvent les systèmes d'IA à risque minimal, tels que les filtres et les chatbots, qui ne relèvent pas du champ d'application de la réglementation proposée en termes d'obligations.

### III. Concept d'IA « à haut risque »

La notion d'IA « à haut risque » demeure l'innovation conceptuelle la plus intéressante de la proposition d'AIA, à laquelle son Titre III est entièrement consacré. Elle correspond à tous les systèmes d'IA qui ne sont pas aussi dangereux que les IA à risque inacceptable, mais dont le risque n'est pas négligeable en fonction de leur utilisation. La notion n'est pas créée comme une catégorie résiduelle, car elle a été définie dans son article 6. L'article fonctionne en symbiose avec les annexes II et III de la proposition, tout en introduisant deux conditions cumulatives pour que les systèmes d'IA se voient attribuer un risque élevé :

- « (a) le système d'IA est destiné à être utilisé comme composant de sécurité d'un produit ou du système d'IA couvert par la législation d'harmonisation de l'Union énumérée à l'annexe II, ou constitue lui-même un tel produit.
- (b) le produit dont le composant de sécurité au titre du point a) est le système d'IA, ou le système d'IA lui-même en tant que produit, est soumis à une évaluation de la conformité en matière de sécurité par un tiers liée aux risques pour la santé et la sécurité en vue de la mise sur le marché ou de la mise en service de ce produit conformément à la législation d'harmonisation de l'Union énumérée à l'annexe II »[25].

Ces deux conditions font indirectement référence à celles énoncées dans le *Livre blanc sur l'IA*, qui prévoit de classer comme à haut risque les IA qui répondent aux critères suivants :

- « employée dans un secteur où, compte tenu des caractéristiques des activités normalement menées, des risques importants sont à prévoir; [*et*]
- utilisée de façon telle que des risques importants sont susceptibles d'apparaître »[26].

---

25 *Ibid.*, Article 6, voir note 22. L'Annexe II est mentionnée dans les deux conditions car elle correspond à la liste des instruments juridiques faisant partie du New Legislative Framework (NLF) auxquels les systèmes d'IA doivent se conformer. Il s'agit d'un cadre réglementaire européen introduit en 2008 pour remplacer le cadre relatif aux produits industriels existant. Son principal apport a été la mise en place d'exigences minimales pour les produits sur le marché unique de l'UE, tout en laissant aux organisations dirigées par l'industrie le soin de définir des normes supplémentaires, afin de favoriser la flexibilité et l'innovation. Ce système est également la philosophie sous-jacente de l'AI Act. Il donc vraisemblable que les produits d'IA relevant du champ d'application du NLF seront considérés comme à haut risque.

26 *Ibid.*, voir note 19, p. 20.

Bien que plus techniques, les conditions de la proposition reflètent ces dernières, qui mettent en évidence la nécessité d'orienter l'intervention réglementaire là où le risque est susceptible de se présenter, tout en séparant les applications dangereuses des autres. De cette façon, la réglementation n'est adoptée que là où elle est nécessaire afin d'éviter de restreindre excessivement les IA à risque plus faible qui peuvent apporter des bénéfices à la société.

L'article 6 continue : « outre les systèmes d'IA à haut risque visés au paragraphe 1, les systèmes d'IA relevant d'un ou de plusieurs domaines cruciaux et de cas d'utilisation visés à l'annexe III sont considérés à haut risque s'ils présentent un risque important de préjudice pour la santé, la sécurité ou les droits fondamentaux des personnes physiques. Lorsqu'un système d'IA relève de l'annexe III, point 2, il est considéré comme étant à haut risque s'il présente un risque important de préjudice pour l'environnement »[27]. L'annexe III de l'AIA comprend en effet une liste de systèmes d'IA qui seront considérés comme à haut risque s'ils remplissent les conditions de l'article 6. On pense notamment à l'application clé de cette étude : les TRF. Dans sa première proposition, la CE avait l'intention de considérer toutes les applications répertoriées dans l'Annexe III comme à haut risque. Cependant, elle a renoncé à cette approche extrêmement stricte dans la version amendée par le Parlement en juin 2023.

En poursuivant la lecture du Titre III, on constate l'importance de la classification à haut risque. Comme expliqué précédemment, la principale innovation de l'AIA réside dans les exigences imposées aux systèmes d'IA à haut risque pour être autorisés dans l'UE.

Le chapitre 3 du même titre propose une vaste gamme d'exigences à laquelle la conformité sera imposée. On peut citer, par exemple, l'obligation de transparence et de supervision humaine des articles 13 et 14, de conformité et de certifications des articles 8 et 9, de disposer d'une politique de gestion de données appropriée de l'article 10, de créer une documentation technique avec conservation des enregistrements des articles 11 et 12 ; le tout en veillant à ce que l'IA reste précise, robuste et conforme aux obligations en matière de cybersécurité.

## IV. Technologies de Reconnaissance Faciale et AI Act

Les TRF occupent une place unique dans la nouvelle législation, car leurs utilisations peuvent être très diverses. Comme expliqué précédemment, elles peuvent être utilisées autant à des fins privées que publiques, et présentent un grand nombre d'applications. Par conséquent, elles seront soumises à une classification différentielle dans l'AIA selon cette utilisation.

L'AIA introduit également une nuance dans la classification des TRF, ayant un impact sur la catégorisation de leur risque : les « systèmes d'identification biométrique » dit « en temps réel » ou « a posteriori ». Les TRF en temps réel correspondent à l'utilisation en direct d'un algorithme d'identification biométrique, tandis que les TRF a posteriori le réalisent après enregistrement et archivage dans une base de données spécifique. L'introduction de cette nuance réside dans le fait que l'identification en temps réel crée un risque élevé de violation des droits fondamentaux des individus qui y sont soumis. Dans de tels cas, des précautions supplémentaires doivent être prises, conduisant à cette classification différentielle dans l'AIA.

---

27 *Ibid.*

En effet, en ce qui concerne l'utilisation publique de la technologie de reconnaissance faciale, la proposition de l'AIA impose un cadre très strict dans son article 5 : une interdiction totale de leur utilisation en temps réel dans les espaces publics à des fins de maintien de l'ordre[28]. La proposition de la CE avait au départ créé trois exceptions pour :

- la recherche de personnes disparues, notamment des enfants ;
- la « prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique des personnes physiques ou […] d'une attaque terroriste » ;
- l'arrestation d'une personne suspectée d'avoir commis un crime punissable d'une peine de minimum trois années de détention en vertu du droit pénal de l'État Membre[29].

Ces trois autorisations étaient par ailleurs agrémentées de davantage d'obligations consacrées dans les paragraphes suivants de l'article 5, notamment sur la prise en compte des principes de subsidiarité et de proportionnalité[30]. Dans sa version la plus récente, l'AIA a été modifié en supprimant ces exceptions et leurs conditions additionnelles, ayant pour conséquence de rendre générale l'interdiction de l'utilisation des TRF en temps réel à des fins répressives. En résumé, cette utilisation spécifique de cette technologie sera interdite *per se*.

Les autres cas d'utilisation de TRF, à savoir les contextes publics a posteriori et privés tant en temps réel qu'a posteriori, seront régis par les articles 8 à 51 de l'AIA[31]. En effet, les TRF font partie de la liste de l'annexe III en tant que « systèmes d'IA destinés à être utilisés pour l'identification biométrique des personnes physiques »[32]. Cette catégorisation implique alors les obligations susmentionnées qui s'appliquent à toutes les IA à haut risque.

## V. Forces et faiblesses

Au regard de cette brève étude de la proposition de l'AIA, on peut aisément constater que l'accent a été mis sur la protection des droits fondamentaux des citoyens de l'UE. Le respect des principes de transparence et de la vie privée fait partie des objectifs de l'AIA et du cadre législatif plus général censé encadrer le développement de l'IA en Europe.

Ainsi, la dimension globale de la réglementation est certainement sa principale force, car l'AIA vise à réguler l'ensemble des applications de l'IA sur le territoire de l'UE et à contraindre tous les acteurs à se conformer à ses droits fondamentaux, tout en veillant à ce qu'aucun ne soit en dehors de son périmètre de responsabilité, en particulier les systèmes d'IA à haut risque. La proposition d'AIA énonce en effet un ensemble clair d'obligations à l'égard de divers acteurs, notamment les importateurs, les distributeurs, et même les utilisateurs, chacun connaissant précisément le champ d'application de ses responsabilités dans l'introduction ou l'utilisation d'un système d'IA au sein de l'UE. Cet ensemble d'obligations s'articulera avec les obligations existantes d'autres instruments juridiques majeurs de l'UE, tels que le RGPD et la Charte des droits fondamentaux, renforçant sa présence dans le cadre juridique global.

---

28 *Ibid.*, Article 5, voir note 5.
29 *Ibid.*
30 *Ibid.*
31 *Ibid.*, Article 8-51, voir note 5.
32 *Ibid.*, Annexe III.

Enfin, cette approche basée sur les risques est la principale caractéristique de l'AIA. Elle vise à lui permettre de rester pertinent face aux évolutions à venir des systèmes d'IA. Travailler sur base de catégories permet en effet à l'UE d'éviter des évaluations constantes ou de faire du cas par cas ; approche qui entraînerait des coûts élevés liés à l'analyse de chaque système d'IA, ainsi qu'une efficacité limitée pour les applications en évolution rapide ou à venir.

Ainsi, rien n'empêche une IA dont le risque est aujourd'hui considéré comme limité de devenir plus à risque au fil du temps ou de son évolution. Par exemple, la controverse autour de ChatGPT et ses potentialités a conduit le législateur européen à modifier la classification originale des systèmes d'IA générative. Travailler avec des catégories ouvertes et des critères objectifs est donc une option viable pour réglementer l'IA. De plus, contrairement à une approche faisant du cas par cas, travailler avec des catégories permet une approche plus souple et adaptée aux générations futures de systèmes d'IA.

Cependant, dans la doctrine, cette approche basée sur le risque est l'élément qui suscite le plus de controverse. De nombreux auteurs ont ainsi critiqué la rigidité de cette approche, ne permettant pas la flexibilité attendue par les développeurs d'IA[33]. En effet, travailler avec des catégories générales aurait l'effet inverse « d'inclure des applications d'IA dans la catégorie à haut risque alors qu'après examen, celles-ci ne présenteraient en réalité aucun risque significatif »[34], finissant par entraver l'innovation en imposant un ensemble d'obligations à des systèmes qui n'en ont pas besoin. Comme mentionné dans l'article référencé, par rapport aux 15% d'IA existantes déclarées par la CE comme à haut risque, il est estimé que cette classification concernerait 55% des applications existantes. Si tel était le cas, l'innovation pourrait en effet être ralentie par un trop grand nombre de tâches de mise en conformité[35].

Cette enquête d'impact pourrait néanmoins être invalidée par un autre élément soulevé par la critique : l'ambiguïté des dispositions du futur AIA, notamment la définition des systèmes d'IA à haut risque. La définition ne fournirait pas de sécurité juridique suffisante quant à son champ d'application, étant une source importante de confusion chez les développeurs.

Le corollaire de ces critiques est que l'accent a été disproportionnellement mis sur le concept d'IA à haut risque, sans définir et réglementer davantage les systèmes d'IA à risque moindre, qui, dans certains cas, pourraient être plus néfastes, sans avoir à se conformer aux mesures de sécurité adéquates et se voyant imposer uniquement des obligations plus limitées par l'AIA.

En conclusion, l'approche de l'UE, malgré les critiques qu'elle peut susciter, reste à ce jour la seule proposition visant à réglementer de manière globale l'IA. L'ambition est grande, mais ses réelles implications seront à évaluer une fois le texte final adopté. L'UE se vante toutefois d'avoir trouvé le bon équilibre entre l'innovation et la mise en place d'une IA « digne de confiance », malgré le nombre substantiel d'obligations qui seront imposées aux différents acteurs, dans un environnement technologique en constante évolution.

---

33 Gerlach, N. (2023). The case of the EU AI Act: Why we need to return to a risk-based approach. *International Association of Privacy Professionals* (IAPP). https://iapp.org/news/a/the-case-of-the-eu-ai-act-why-we-need-to-return-to-a-risk-based-approach/

34 *Ibid.*

35 Liebl, A. & Klein, T. (2022). AI Act Impact Survey. *AppliedAI*. https://www.appliedai.de/hub/ai-act-impact-survey

# CALIFORNIE (ÉTATS-UNIS)

La Californie est la deuxième juridiction dont le cadre réglementaire sera analysé. Bien que n'étant pas représentative de l'ensemble des États-Unis, l'approche de cet État est certainement la plus intéressante et la plus significative en termes d'initiatives. Par ailleurs, situer la Californie dans le contexte juridique fédéral reste nécessaire pour avoir une vue globale de la situation des États-Unis. La pertinence de la Californie dans la réglementation de l'IA est d'autant plus importante qu'elle accueille la Silicon Valley, qui concentre la majorité des entreprises dans la course au développement de l'IA.

## I. Contexte historique et législatif

Les États-Unis sont certainement le pays où les libertés sont les plus vénérées. La Constitution est ainsi très souvent invoquée par les Américains pour revendiquer leurs droits face à un État de plus en plus enclin à s'immiscer dans leur vie quotidienne[36]. L'héritage politique du pays est d'ailleurs marqué par cette lutte constante pour la liberté. Néanmoins, le rôle d'un État est également de protéger ses citoyens, et lorsqu'un danger les menace, il se doit intervenir.

En ce qui concerne l'IA, de nombreuses valeurs antagonistes entrent en jeu, tels que le droit de libre entreprise, le droit à la vie privée, et le maintien de l'ordre conféré à tout État. Lorsque ces droits entrent en conflit, c'est l'État qui reste le juge ultime de la limite à fixer[37].

Les États-Unis ont également connu des scandales politiques liés à l'IA qui ont marqué leurs citoyens, réclamant des mesures pour regagner confiance en leurs institutions. L'un d'eux est celui de la firme britannique Cambridge Analytica, qui a eu lieu à la suite des élections présidentielles de 2016, opposant Donald Trump à Hillary Clinton. Celle-ci aurait en effet utilisé une faille du réseau social Facebook afin de profiler plus de 50 millions d'utilisateurs sur la plateforme et les exposer à de la publicité politique ciblée[38]. Après que ces pratiques ont été révélées et que l'utilisation des données à des fins politiques est devenue de notoriété publique, de nombreux pays ont commencé à réfléchir à la manière de prévenir de telles situations. C'est également à ce moment-là que le champ des possibles de l'IA est devenu évident pour de nombreux décideurs politiques, qui ont compris qu'un équilibre devait être trouvé pour permettre à leur pays d'exceller dans le domaine de l'IA, tout en garantissant les droits fondamentaux de leurs citoyens.

Aux États-Unis, ce basculement a été entamé au niveau fédéral par le président Donald Trump, deux ans après son entrée à la Maison Blanche. L'*Ordonnance de 2019 sur le maintien du leadership américain en matière d'intelligence artificielle* est la concrétisation d'une volonté fédérale de promouvoir la recherche et le développement de l'IA sur le sol américain[39].

---

36 Bowie, N. (2021). The Constitutional Right of Self-Government. *The Yale Law Journal*. https://www.yalelawjournal.org/article/the-constitutional-right-of-self-government

37 *Ibid.*

38 Confessore, N. (2018). Cambridge Analytica Scandal: The Fallout. *The New York Times*. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

39 US Presidential Executive Order 13,859. (2019). 3 C.F.R. 3967.

« L'American AI Initiative » repose sur cinq principes, parmi lesquels un essentiel : « la protection des valeurs américaines, y compris les libertés civiles et le respect de la vie privée, favorisant la confiance du public dans les systèmes d'IA »[40].

Dans les semaines qui ont suivi, la Chambre des Représentants a adopté la Résolution 153, visant à encadrer l'élaboration de lignes directrices étiques pour le développement de l'IA. La résolution avait pour objectif affiché de mettre en équilibre le « potentiel de l'IA pour améliorer le bien-être et améliorer les soins et les services des individus et pour favoriser la croissance économique » par un « développement sûr, responsable et démocratique »[41].

## II. Compréhension américaine de l'IA « à haut-risque »

En avril de la même année, le Congrès américain a proposé l'*Algorithmic Accountability Act*. Le projet de loi vise à atténuer les risques liés aux traitements de données de certaines IA[42].

Comme expliqué précédemment, l'une des principales inquiétudes liées à certains types d'IA réside dans leur système d'apprentissage, qui n'est pas exempt de défauts. Plusieurs études ont en effet souligné les biais dont font preuve certaines IA, notamment celles utilisées par les organes répressifs, ayant entraîné des faux positifs et des arrestations illégales dans le cadre d'enquêtes criminelles[43]. Les questions raciales et de discrimination étant des sujets sensibles aux États-Unis, il est naturel que le législateur prenne ce problème au sérieux et demande des garanties aux fournisseurs avant la mise en service d'un système d'IA.

Dans une nouvelle version du projet de loi datant de 2022, il est exigé que les systèmes d'IA subissent une analyse d'impact réalisée par des tiers, tels que des auditeurs indépendants et des experts en technologie avant leur mise sur le marché, et que les entreprises évaluent régulièrement leurs applications en termes de « précision, d'équité et de discrimination »[44].

Le projet de loi n'a pas encore été adopté et suit le processus législatif. Il deviendrait alors le premier instrument quasi-global dans le domaine de l'IA au niveau fédéral. Cependant, il n'irait pas aussi loin que l'AIA de l'UE en termes d'obligations imposées aux entités concernées.

## III. Approche californienne de régulation des technologies de reconnaissance faciale

En Californie, une application spécifique d'IA a fait l'objet de nombreux articles : les TRF. Bien qu'il s'agisse d'un type d'IA assez commun dans le Golden State, qui abrite les entreprises à la pointe de leur développement, leur utilisation, notamment à des fins de maintien de l'ordre, n'est pas largement acceptée par la population. Les scandales réguliers ont poussé des décideurs politiques locaux à prendre des mesures liées à cet usage spécifique.

---

40 *Ibid.*

41 US H.R. Resolution 153, 116th Congress. (2019).

42 US Algorithmic Accountability Act of 2019, S. 1108, H.R. 2231, 116th Congress. (2019).

43 Johnson, T. L., Johnson, N. N., McCurdy, D., et Olajide, M. S. (2022). Facial recognition systems in policing and racial disparities in arrests. *Government Information Quarterly*, 39(4), 101753. https://doi.org/10.1016/j.giq.2022.101753.

44 US Algorithmic Accountability Act of 2022, S. 1108, H.R. 6580, 117th Congress. (2022).

En 2019, plusieurs villes californiennes, dont San Francisco, ont décidé d'interdire les TRF à des fins de maintien de l'ordre[45]. La législature étatique a alors imposé un moratoire de trois ans sur l'utilisation des TRF à ces mêmes fins[46]. La mesure a été ensuite formalisée dans un projet de loi qui a confirmé l'interdiction pour les organes de maintien de l'ordre d'utiliser des « systèmes de surveillance biométrique »[47], mais est arrivée à expiration en janvier 2023. Un autre projet de loi a exigé des entreprises privées qu'elles rendent publique l'utilisation des TRF en leur enceinte[48]. Un an plus tard, à l'initiative du Sénat fédéral, la *Loi sur l'Utilisation Éthique de la Reconnaissance Faciale* a été promulguée et appelait à un moratoire sur l'utilisation publique des TRF jusqu'à ce qu'un cadre juridique approprié soit élaboré.

À travers ces mesures, on peut voir que les différents législateurs se soucient principalement des abus potentiels de la technologie dans le contexte du maintien de l'ordre, alors qu'aucune initiative n'a été encore prise en ce qui concerne une réglementation globale de l'IA.

Il existe néanmoins un instrument dans le corpus juridique californien qui distingue l'État de ses homologues. En 2018, le Congrès californien a promulgué le California Consumer Privacy Act (CCPA), entré en vigueur en 2020. Il s'agit de l'instrument juridique le plus complet traitant des situations liées à la protection des données et à la vie privée aux États-Unis.

Sans avoir directement égard à l'IA, les dispositions du CCPA restent applicables à un grand nombre de systèmes d'IA, dont les TRF. En effet, pour être applicable, il exige que des données personnelles, décrites comme des « informations qui […] se rapportent […] directement ou indirectement, à un consommateur […] »[49] soient la source du litige. Les informations biométriques, telles que celles collectées par TRF, entrent dans cette catégorie.

Cependant, le CCPA ne s'applique qu'aux entreprises qui dépassent des seuils importants de chiffre d'affaires, de clientèles, et pour lesquelles la vente d'informations personnelles représente au moins 50% de leurs revenus. En réalité, un très petit nombre d'entreprises tombe dans cette catégorie. Cela dit, en 2021, il a été étendu aux communications B2B[50] et, depuis 2022, à la manière dont les entreprises traitent les informations de leurs employés[51].

De la même manière, dans la plupart des situations, le CCPA ne requiert pas des entreprises de consentement pour collecter des données, rendant ses effets en réalité très limités[52].

---

45 Conger, K., Fausset, R., et Kovaleski, S. F. (2019). San Francisco Bans Facial Recognition Technology. The *New York Times*. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

46 Wu, T. (2020). California at Crossroads Over Policing and Facial Recognition. *Bloomberg Law*. https://news.bloomberglaw.com/california-at-crossroads-over-policing-and-facial-recognition

47 California bill A.B. 1215 of 2019

48 California bill A.B. 1281 of 2019

49 California State Legislature. (2018). California Consumer Privacy Act (CCPA), Article 1798.140(o)(1). https://oag.ca.gov/privacy/ccpa

50 TermsFeed. (2023). The CCPA/CPRA's "Business to Business" Exemption: AB 1355. https://www.termsfeed.com/blog/ccpa-b2b-exemption/

51 Garhart, N. et Stephens, R. (2022). Employee Data Under the CCPA: Expiration of the Employee Exception. *JD Supra*. https://www.jdsupra.com/legalnews/employee-data-under-the-ccpa-expiration-6993807/

52 Lister, J. (2022). CCPA Consent Requirements: What You Need to Know. Free Privacy Policy. https://www.freeprivacypolicy.com/blog/ccpa-consent-requirements/text=Under%20the%20CCPA%20(CPRA)%2C,from%20their%20parent%20or%20guardian.

En conclusion de ce bref aperçu, il est clair que les principales préoccupations des législateurs californiens et américains se trouvent dans l'utilisation de l'IA par les organismes publics et de leur potentiel abus, tant que la technologie n'a pas atteint un niveau suffisant de précision.

Ainsi, l'État de Virginie a adopté une loi en 2022 qui exige des organes gouvernementaux et de répression qu'ils n'utilisent que des systèmes de TRF ayant obtenu au moins 98 % de précision pour l'ensemble des groupes démographiques[53]. L'accent est donc encore une fois principalement mis sur les biais que sur l'utilisation de la technologie en elle-même.

## IV. Forces et faiblesses

La flexibilité apportée par le corpus législatif californien est certainement la force d'un État où l'innovation en matière d'IA est la plus élevée. Le législateur californien est ainsi très réticent à imposer des restrictions afin de favoriser cette innovation. Le Golden State compte rester le leader mondial de l'IA, et sa réglementation reflète cet objectif. Néanmoins, cette flexibilité et ce manque d'instruments juridiques préventifs entraînent des lacunes et incohérences réglementaires conduisant à des abus en raison d'un cadre très limité.

La focalisation sur l'innovation est très rationnelle dans l'approche californienne et américaine. « L'American AI Initiative » en est un parfait exemple, en ce qu'elle démontre l'importance que les décideurs politiques accordent à l'innovation en évitant d'imposer un cadre juridique trop strict, qui pourrait avoir pour effet de faire fuir les entreprises.

Le processus législatif aux États-Unis est également particulier en ce qu'il est marqué par une forte présence de lobbys. Très souvent, les législateurs sont sollicités par des représentants du secteur privé faisant pression en faveur des intérêts de leurs entreprises, ce qui peut influencer l'issue d'un projet de loi[54]. Bien que cela puisse créer des risques de conflit d'intérêts, la force de cette approche est qu'elle permet la création d'instruments juridiques adaptés, tenant compte des intérêts des acteurs concernés.

Le plus grand inconvénient de cette approche demeure le manque de législation préventive. Alors que la promotion de l'innovation a été la principale préoccupation des législateurs, l'absence d'approche réglementaire proactive ne peut conduire qu'à des erreurs dans la manière dont les applications d'IA se propagent dans la société et à des utilisations abusives.

Le manque de cadre global, tant au niveau fédéral qu'au niveau des États, ne peut créer qu'un cadre règlementaire lacunaire et incohérent. Sans initiative fédérale, il est difficile pour les acteurs de l'IA de savoir quelles obligations leur sont applicables, créant une incertitude très difficile à gérer, combinée à ces incohérences qui posent de graves problèmes de conformité.

Enfin, bien qu'énoncées, les normes éthiques ne sont pas contraignantes et conduisent à des scandales auxquels le public américain s'habitue tristement.

---

53 Virginia bill S.B. 741 of 2022.

54 Weiser, D. (2021). Why Lobbying Is Legal and Important in the US. *Investopedia*. https://www.investopedia.com/articles/investing/043015/why-lobbying-legal-and-important-us.asp

# CHINE (REPUBLIQUE POPULAIRE DE)

La Chine est la dernière juridiction dont la réglementation en matière d'IA sera analysée dans le cadre de cette étude. Souvent pointée du doigt, mais rarement pleinement comprise, l'aspect unique de la gouvernance chinoise réside dans les avancées du pays en matière de recherche et d'implication de l'IA dans la vie quotidienne de ses citoyens, en comparaison à la faible réglementation qui entoure son utilisation. Cette section analysera donc ce contexte législatif à travers les réglementations actuelles et à venir du système chinois.

## I. Contexte historique et législatif

La Chine a fait de l'IA son objectif technologique principal. Dans son *Plan de développement d'une intelligence artificielle de nouvelle génération* (PDIANG) de 2017, le Conseil des affaires de l'État en a fait la priorité du XXIe siècle et vise à en devenir le leader mondial d'ici 2030[55].

Dans le contexte du développement de l'IA, l'accent a clairement été mis sur la croissance économique, tout comme l'ont fait l'UE et les États-Unis. Il existe néanmoins une dimension de gouvernance sociale qui n'est pas aussi présente dans les deux autres juridictions[56].

La particularité de l'IA en Chine, notamment des TRF, est son omniprésence, en raison d'incitatifs gouvernementaux aux entreprises et organismes publics d'utiliser des systèmes d'IA dans leurs activités quotidiennes[57] pour des raisons de gouvernance.

L'utilisation de systèmes d'IA est en effet largement encouragée dans de nombreux secteurs, tel le maintien de l'ordre, les banques, le tourisme et le travail. L'IA fait partie intégrante de la vie quotidienne des Chinois, à un niveau encore jamais atteint dans une autre société[58].

La gouvernance sociale est en effet le point d'ancrage du développement de l'IA en Chine, et elle est perçue par la grande majorité des Chinois comme un outil efficace pour prévenir les risques d'instabilité sociale, tels que les crimes, la violence et les dissidences politiques.

Cependant, la nature marginale de la réglementation de l'IA crée un cadre juridique incertain en ce qui concerne les abus potentiels des applications d'IA. Des décisions judiciaires récentes, notamment de la Cour populaire suprême, ont néanmoins contraint les décideurs politiques à intervenir face aux aspirations grandissantes du peuple chinois vers un plus grand respect de leur vie privée[59].

---

55 Webster, G., Creemers, R., Kania, E., & Triolo, P. (2017). Translation: China's New Generation of Artificial Intelligence Development Plan. *New America*. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-generation-artificial-intelligence-development-plan/

56 *Ibid.*

57 *Ibid.*

58 Davies, D. (2021). Facial Recognition And Beyond: Journalist Ventures Inside China's 'Surveillance State'. *Fresh Air*. *NPR*. https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta

59 Supreme People's Court. (2021). Provisions of the Supreme People's Court on several issues concerning the application of law in civil cases relating to the use of face recognition technology in handling personal information. http://www.court.gov.cn/zixun-xiangqing-315831.html.

Historiquement, les droits individuels n'ont pas été la priorité du développement chinois dans les décennies qui ont suivi la création de la RPC. Ce n'est qu'au cours des années 2000, après l'adhésion de la Chine à l'Organisation mondiale du commerce que des préoccupations ont émergé concernant la protection des droits fondamentaux[60]. Dans les années 2010, avec l'explosion du nombre d'applications d'IA, plusieurs initiatives législatives majeures ont été prises pour faire face aux risques potentiels posés par l'IA.

Cependant, à ce jour, aucun instrument juridique ne traite spécifiquement de l'ensemble des questions liées à l'IA. La majeure partie de la protection juridique contre l'IA en Chine provient des réglementations relatives à la protection des données et de certains principes directeurs qui n'ont pas la même force qu'une loi. La *ratione legis* de ces instruments juridiques est également radicalement différente de celles des juridictions occidentales, ce qui peut expliquer les approches différentes adoptées par l'UE et les États-Unis par rapport à la Chine.

## II. Compréhension chinoise de l'IA « à haut-risque »

Les préoccupations sur les risques que posent les systèmes d'IA sont d'une nature totalement différente pour les décideurs chinois. En répondant récemment à ces risques, ils ont mis l'accent sur deux concepts principaux : la sécurité nationale et le respect de la vie privée[61].

Dès le deuxième paragraphe du PDIANG, la sécurité nationale est le concept qui justifie le développement de l'IA pour renforcer les capacités de la Chine face à ses concurrents au niveau mondial, tout en protégeant les intérêts du peuple chinois grâce à des systèmes d'IA « robustes ». Un appel à une « réglementation urgente » a également été lancé dans le plan afin de mettre en œuvre cette stratégie[62].

En suivant ce plan, la Chine a opéré un changement de paradigme en faveur d'une réglementation plus importante de son infrastructure de technologies de l'information, dont l'IA. Deux initiatives législatives majeures ont été promulguées en 2017 et 2021 dans le but de protéger les données sensibles et la sécurité nationale.

Sans faire référence directement à l'IA, la Loi sur la cybersécurité de 2017 (LCS) a été la première loi en Chine incluant les technologies de l'information dans le concept de sécurité nationale. En effet, selon son article 12, toutes les organisations en Chine utilisant des « réseaux » doivent respecter le principe de sécurité nationale et se conformer aux dispositions de la loi. L'IA, tant dans son développement que dans sa commercialisation, doit donc respecter ce principe et toute violation peut entraîner des poursuites judiciaires[63].

---

60 European Parliament. (2016). Study on Liability for Emerging Digital Technologies: Robotics and Artificial Intelligence (EPRS Briefing, No. 593570). https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/593570/EPRS_BRI(2016)593570_EN.pdf

61 The China Academy of Information and Communications Technology (CAICT). (2022). Artificial Intelligence White Paper (人工智能白皮书). http://www.caict.ac.cn/kxyj/qwfb/bps/202204/P020220412613255124271.pdf

62 *Ibid.* voir Webster et al. (2017) discutant de la stratégie chinoise face à l'IA.

63 Creemers, R., Webster, G., & Triolo, P. (2017). Translation: Cybersecurity Law of the People's Republic of China (中华人民共和国网络安全法). https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

Dans sa version de 2021, l'autre instrument, la Loi sur la sécurité des données (LSD), reprend les dispositions de la LCS promouvant la sécurité nationale par le biais de la protection des données. Bien que l'IA ne soit pas directement mentionnée ici non plus, le nombre important des données utilisées par les systèmes d'IA oblige les développeurs à coopérer avec les mécanismes de sécurité nationale décrits dans la loi[64].

Outre le processus législatif, les ministères ont le pouvoir d'édicter des réglementations sur des questions spécifiques dans le cadre des lois existantes. C'est notamment le cas du ministère de l'Industrie et des Technologies de l'Information (MITI).

Par exemple, en décembre 2022, le MITI a promulgué les Dispositions sur l'Administration des Services d'Information Internet à Synthèse Profonde, la dernière évolution réglementaire concernant les technologies dites de « deep-fake ». Elles ont été rédigées conformément à la LCS et la LSD et visent à renforcer « la gestion des services d'information à synthèse profonde, à promouvoir les valeurs socialistes, à préserver la sécurité nationale et l'intérêt public de la société, et à protéger les droits et intérêts légitimes des citoyens, des personnes morales et autres organisations »[65]. Dans des développements récents, un homme a d'ailleurs été arrêté pour avoir utilisé ChatGPT afin de diffuser de fausses informations sur Internet[66]. La base juridique de cette arrestation était précisément cette réglementation. Il s'agit du premier cas de détention lié à un abus d'utilisation d'une IA. Il est également intéressant de noter la rapidité avec laquelle la Chine applique les réglementations liées à la sécurité nationale.

Ce type de réglementation démontre néanmoins à quel point les décideurs chinois accordent de l'importance à la sécurité nationale, où ils situent le principal risque lié à l'utilisation de l'IA.

L'autre risque principal posé par les applications d'IA pour le système chinois est la violation potentielle des droits à la protection de la vie privée. En réalité, sa protection et celle d'autres droits fondamentaux n'ont pas été une priorité en Chine jusqu'aux années 2000, car la reprise économique et la croissance étaient considérées comme essentielles. Mais malgré ce manque primaire de protection, les récents développements témoignent d'un engagement à changer de paradigme et à répondre aux aspirations du public chinois.

En 2004, une révision constitutionnelle a répondu à certains appels internationaux à une meilleure protection des droits fondamentaux en Chine[67]. Le chapitre II de la Constitution a été entièrement consacré à la protection des droits fondamentaux et aux libertés individuelles. L'article 33 consacre la responsabilité de l'État, et les articles 37 et 38 sont consacrés aux principes du respect de la vie privée et de la dignité humaine.

---

64 National People's Congress. (2021). Data Security Law of the People's Republic of China (中华人民共和国数据安全法). http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml

65 National Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security. (2022, November 25). Provisions on the Administration of Deep Synthesis Internet Information Services (国家互联网信息办公室工业和信息化部公安部). http://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm

66 Lau, C. (2023). China Arrests Person for Generating Inappropriate Content with AI Chatbot. CNN. https://edition.cnn.com/2023/05/09/tech/china-arrest-chatgpt-hnk-intl/index.html

67 Feng, Y. (2019). The future of China's personal data protection law: Challenges and prospects. *Asia Pacific Law Review*, 27(1), 62–82.

Ces dispositions sont aujourd'hui considérées comme la base constitutionnelle de la protection des intérêts des citoyens contre les abus de l'IA. La Cour populaire suprême, chargée de l'application de la Constitution aux affaires qu'elle examine en appel des juridictions inférieures, et bénéficiant d'un pouvoir quasi-législatif, a ensuite précisé la protection de ces principes dans des décisions et des avis développés ultérieurement.

Cependant, le véritable tournant s'est produit vers la fin des années 2010, lorsque plusieurs scandales ont conduit à une révision des instruments juridiques en vigueur et à venir. Le Code civil chinois, introduit pour la première fois en 2020 après des années d'élaboration[68], consacre les mêmes principes que la Constitution en garantissant une série de droits civils, tels que les droits à la dignité et au respect de la vie privée dans son article 110. Son Livre Quatre, a été entièrement consacré aux droits de la personnalité, et son Chapitre VI en particulier garantit le droit à la vie privée et à la protection des données personnelles dans tous les contextes civils. Évidemment, cette protection ne s'applique qu'en situations civiles, mais constitue déjà une forte reconnaissance de tels droits au plus haut niveau législatif.

Par ailleurs, cette période a été qualifiée par des universitaires de « neuf dragons jouant avec une seule perle » (*jiulong xizhu*)[69], décrivant une situation où plusieurs dispositions renvoient au même principe, créant de l'incertitude juridique compte tenu des différentes définitions.

Enfin, la pierre angulaire de la réglementation liée à la protection de la vie privée est venue avec la Loi de 2021 sur la Protection des Informations Personnelles (LPIP), souvent comparée au RGPD de l'UE pour son approche globale. Ce nouvel instrument juridique établit un cadre unique pour la collecte, l'utilisation, le stockage, le transfert et le traitement des informations personnelles par les entités nationales et étrangères opérant en Chine et répond aux demandes formulées en amont de sa promulgation.

## III. Approche chinoise de régulation des technologies de reconnaissance faciale

Les technologies de reconnaissance faciale ont longtemps échappé à la réglementation grâce à cette galaxie de dispositions ne les ciblant pas directement. Avec le développement rapide des applications et les préoccupations croissantes liées à la sécurité nationale et la protection de la vie privée, des instruments ont été adoptés afin de réglementer davantage leur usage.

En substance, la formalisation de règles sur les TRF n'a eu lieu que ces dernières années, où des instruments ont été adoptés afin d'interpréter les dispositions existantes. En effet, plusieurs litiges ont conduit le pouvoir judiciaire à enjoindre l'exécutif chinois de réagir aux atteintes aux droits précités par de nouvelles dispositions présentant davantage de clarté.

---

68 *Ibid.*

69 Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. *Telecommunications Policy* Vol. 47, Issue 5. https://doi.org/10.1016/j.telpol.2022.102482

En 2019, un litige opposant le zoo de la ville de Hangzhou à un visiteur a suscité une vague d'inquiétude dans le public concernant leur vie privée, car à l'époque, aucune disposition ne protégeait efficacement leur droit[70]. Dans cette affaire, un visiteur régulier du zoo a refusé d'entrer après que le contrôle d'entrée a exigé des visiteurs de se soumettre à un scan facial. Alors que la plupart des visiteurs s'y sont conformé, M. Guo a refusé, car la méthode d'authentification avait changé d'une analyse d'empreinte digitale à cette dernière. Face au refus du zoo de le rembourser et de supprimer ses informations, M. Guo a décidé de porter l'affaire devant les tribunaux. Le tribunal du district de Fuyang a mentionné dans sa décision que l'utilisation des données personnelles devait être « légale, justifiée et nécessaire »[71]. Le tribunal a également mentionné que le consentement devait être obtenu pour traiter ces informations, ce qui était le cas ici. Cependant, le tribunal a considéré que le zoo avait rompu son contrat avec M. Guo, car il n'avait pas informé correctement ses visiteurs sur la manière dont il traiterait dorénavant leurs données. Par conséquent, le zoo de Hangzhou a été tenu à l'indemnisation et à la suppression des données personnelles de M. Guo[72].

Cette affaire a été la première impliquant une TRF, et compte tenu de l'omniprésence de cette technologie dans la société chinoise, les décideurs politiques ont été forcés de réagir pour éviter d'autres litiges de ce genre. Un an plus tard, la révision du Code civil chinois a mis en œuvre ces demandes dans son Livre Quatre.

Sa cadette, la LPIP, a également introduit un cadre législatif pour les TRF. Son article 26 les cible directement et impose que « l'installation d'un dispositif de collecte d'images et de reconnaissance d'identité dans les lieux publics » soit « nécessaire pour garantir la sécurité publique, conforme aux réglementations pertinentes, et affiche des préavis clairs ». Il précise aussi que « les images et les informations d'identification personnelle collectées ne peuvent être utilisées que dans le but de garantir la sécurité publique et ne doivent pas être divulguées ou fournies à autrui, sauf si le consentement spécifique des individus est obtenu, ou si la loi le prévoit »[73]. Enfin, l'article 28 classe les données biométriques comme sensibles, et impose un niveau de consentement plus élevé.

Malheureusement, la mise en place récente de ce cadre réglementaire et le ralentissement des processus judiciaires dû à la pandémie de coronavirus ne nous donnent que peu de perspective quant à leur efficacité et leur mise en œuvre effective.

Cela n'a néanmoins pas empêché la Cour populaire suprême de publier un document de travail à valeur quasi-législative sur les litiges liés aux TRF et intitulé *Dispositions sur plusieurs questions sur l'application de la loi dans les affaires civiles relatives à l'utilisation de technologies de reconnaissance faciale pour traiter des informations personnelles*[74].

---

70 Hangzhou Fuyang District People's Court. (2019). Guo v. Hangzhou Safari Park, 0111 Zhejiang. Supp. 6971 (en chinois) https://www.qcc.com/wenshuDetail/f491af7adaa22ea27ea81c891423f55e.html.

71 *Ibid.*

72 *Ibid.*

73 National People's Congress. (2021). Personal Information Protection Law (PIPL) of the People's Republic of China (中华人民共和国个人信息保护法). http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm

74 Supreme People's Court. (2021). The Supreme People's Court's Provisions on Several Issues on the Application of Law in Hearing Civil Cases Related to the Use of Facial Recognition Technology to Handle

La Cour consacre dans ce document une interprétation des articles 1034 à 1039 du Code civil récemment promulgué, c'est-à-dire ceux qui composent le Chapitre VI susmentionné relatif à la protection de la vie privée. Cet instrument juridique peut ainsi être considéré comme une « solution de contournement » au manque de dispositions spécifiques aux TRF.

## IV. Forces et faiblesses

Ce bref aperçu de l'approche réglementaire chinoise démontre la jeunesse de leurs efforts en matière de protection d'intérêts sécuritaires et sociaux, face au développement croissant des systèmes d'IA dans la société. Mais il démontre aussi la rapidité relative avec laquelle la Chine est capable de répondre à des problématiques spécifiques et de les traiter efficacement, illustrant ainsi la récente doctrine juridique chinoise du « learning by doing »[75].

Mais la route est encore longue avant que la Chine puisse aborder l'ensemble des questions liées à l'IA : dans le cadre actuel, il existe une lacune majeure pour l'utilisation des TRF par les organes étatiques. Alors que les litiges civils semblent bénéficier d'une protection supérieure, il n'existe aucune protection face à l'utilisation publique des TRF. Au contraire, de nombreuses dispositions renforcent la position et la légitimité de l'État à collecter et utiliser des données biométriques via reconnaissance faciale dans l'intérêt de la sécurité publique et nationale.

La LSD contient une disposition dans son article 35 qui stipule que « lorsqu'un organe de sécurité publique a besoin d'obtenir des données pour des raisons de sécurité nationale ou pour enquêter sur des crimes [...], celles-ci doivent être obtenues conformément à la loi, et les organisations ou individus concernés doivent coopérer »[76]. Cet article reflète le pouvoir asymétrique détenu par les organismes publics en matière de collecte de données. La notion de « sécurité nationale » étant extrêmement vague et susceptible de changer avec le temps, il existe en réalité un nombre infini de raisons pour lesquelles l'État pourrait requérir de telles informations sensibles sur leurs citoyens.

Ce manque de cadre réglementaire dans les cas de collectes de données publiques se retrouve également dans la LPIP, qui ne contient aucune disposition protégeant efficacement les citoyens contre l'intrusion des pouvoirs publics dans leur vie privée. Les systèmes d'IA ne sont qu'un outil aidant la mise en œuvre de ces politiques et sont soumis aux obligations de transfert. Il est donc peu probable qu'un outil réglementaire global sur l'IA émerge dans un avenir proche, car la manière dont la Chine met en œuvre sa stabilité politique se construit dans l'ingérence étatique dans les affaires privées, avec un minimum de responsabilité.

L'IA est pour les Chinois la seule voie à suivre, et un cadre légal limité et ciblé leur permet un développement important de l'IA, confirmant leur objectif d'en devenir les leaders mondiaux d'ici 2030, même si cela doit se faire au détriment des droits de leurs citoyens.

---

Personal Information (最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定). http://www.court.gov.cn/fabu-xiangqing-315851.html

75 "Apprendre en expérimentant", dans Liu, Y. L., Yan, W., & Hu, B. (2021). Resistance to facial recognition payment in China: The influence of privacy-related factors. *Telecommunications Policy*, 45(5), 1–18. https://doi.org/10.1016/j.telpol.2021.102155

76 *Ibid.*, voir note 66.

# ÉTUDE COMPARATIVE

## I. Objectifs comparés

Afin de comparer efficacement les trois régions, il est important de d'abord évaluer les objectifs et les principes de leurs approches respectives.

L'objectif principal des États-Unis est de favoriser l'innovation tout en maintenant leur leadership dans l'industrie de l'IA. Les entreprises américaines sont en effet à la pointe de l'innovation en la matière. Un cadre juridique trop strict pourrait donc entraver leur développement en raison des obligations de conformité[77]. Néanmoins, les risques sociétaux liés à l'IA, tels que les biais raciaux et les potentielles violations de la vie privée ont également été pris en compte en raison de leur caractère intolérable dans la société américaine.

La Chine, dans une approche singulière, souhaite faire de l'IA un outil permettant de maintenir sa stabilité sociale tout en améliorant son économie et sa gouvernance. La question de la confidentialité est beaucoup moins prise en compte, bien que les récents développements régulatoires, en particulier la LPIP, montrent une évolution destinée à répondre à un fort besoin sociétal de droits civils[78]. Néanmoins, l'utilisation de systèmes d'IA à des fins de maintien de l'ordre reste largement non réglementée sur des motifs de sécurité nationale.

L'UE, quant à elle, a choisi une approche plus globale, abordant à la fois les questions civiles et publiques liées à l'utilisation de l'IA. Tout en cherchant à maintenir le dynamisme du continent en matière d'innovation, les décideurs européens aspirent à faire de leur approche un modèle de gouvernance pour le reste du monde en établissant des normes pouvant répondre à toutes les préoccupations liées à l'IA.

Les trois juridictions cherchent ainsi à concilier l'innovation avec la protection des droits et intérêts de leurs citoyens, mais elles ont chacune trouvé un équilibre différent dans leur manière de réglementer l'IA : les États-Unis ont mis davantage l'accent sur la croissance économique, en accordant moins d'attention aux questions de vie privée et d'équité ; la Chine a également mis l'accent sur la croissance économique, mais a décidé de favoriser davantage sa stabilité sociale en autorisant une utilisation publique plus large des systèmes d'IA, en ne commençant que récemment à aborder les préoccupations liées à la vie privée ; quant à l'UE, elle tente de trouver un équilibre idéal entre innovation et réglementation en imposant beaucoup plus d'obligations, dans une approche réglementaire globale qui vise à protéger les droits fondamentaux et à promouvoir une IA "digne de confiance".

---

77 Sorkin, A. R., Mattu, R., Warner, B., Kessler, S., de la Merced, M. J., Hirsch, L., & Livni, E. (2023). Why Lawmakers Aren't Rushing to Police A.I. *Dealbook. The New York Times*. https://www.nytimes.com/2023/03/03/business/dealbook/lawmakers-ai-regulations.html

78 Cunningham, E., Saich, T., & Turiel, J. (2020). Understanding CCP Resilience: Surveying Chinese Public Opinion Through Time. *Harvard Kennedy School, Ash Center for Democratic Governance and Innovation*. https://ash.harvard.edu/files/ash/files/final_policy_brief_7.6.2020.pdf

## II. Instruments juridiques comparés

En ce qui concerne les mesures réglementaires mises en place, les trois régions adoptent aussi des approches très différentes : les deux premières étant réactives, la dernière proactive.

L'approche des États-Unis est axée sur des secteurs spécifiques et répond aux abus attestés au niveau sociétal. Il existe très peu de réglementation au niveau fédéral, et le soin est laissé aux États d'adopter des mesures plus complètes. Parallèlement, des directives éthiques ont été prises, mais elles sont généralement non contraignantes.

La Chine a adopté une approche étonnamment similaire à celle des États-Unis, avec son "learning by doing" qui répond a posteriori aux besoins de la société. Elle maintient aussi son approche verticale, impliquant fortement le gouvernement et fixant des standards élevés en matière de sécurité des données. Elle ne dispose néanmoins pas encore, tout comme les États-Unis, d'un instrument réglementaire spécifique à l'IA.

De son côté, l'Union européenne a cherché à concilier les deux aspects du problème en adoptant une solution globale pour l'IA, classifiant donc les différentes applications sur une échelle de risque associée à des exigences réglementaires croissantes.

## III. Définitions comparées

Somme toute, chaque juridiction a une définition différente du concept d'IA « à haut risque ». Alors que l'UE part sur un concept très large englobant des secteurs et des applications de manière transversale, la Chine et les États-Unis ont d'autres points de vue. D'une part, les États-Unis considèrent que les risques posés par l'IA proviennent principalement de leur manque de précision et d'équité, pensant notamment aux cas d'abus dans des contextes de maintien de l'ordre. D'autre part, la Chine concentre ses préoccupations sur sa sécurité nationale et sa stabilité sociale ; les systèmes considérés comme à risque étant ceux qui ne correspondent pas aux vues politiques du gouvernement et menaçant donc l'ordre social.

## IV. Conséquences de ces différences

En ce qui concerne l'innovation, les approches flexibles des États-Unis et de la Chine sont les plus susceptibles de créer un contexte favorable au développement de l'IA sur leur territoire, entraînant néanmoins plus de risques en raison de cette innovation rapide que la loi ne peut pas suivre. L'approche de l'UE, bien qu'elle puisse probablement freiner l'innovation en raison des obligations qu'elle imposera aux acteurs de l'IA, a été conçue pour préparer l'avenir et être suffisamment flexible pour répondre aux futures innovations en la matière.

Une source majeure de préoccupations concerne la confiance que les citoyens accordent aux systèmes d'IA. Diverses enquêtes menées dans le monde entier ont conclu que les individus sont davantage inquiets qu'enthousiastes face à l'importance croissante de l'IA dans leur vie[79].

---

[79] Kennedy, B., Tyson, A., & Saks, E. (2023). Public Awareness of Artificial Intelligence in Everyday Activities. *Pew Research Center*. https://www.pewresearch.org/science/2023/02/15/public-awareness-of-artificial-intelligence-in-everyday-activities/

Des mesures efficaces sont nécessaires pour répondre à ces craintes et maintenir la confiance dans la technologie. Ainsi, l'approche de l'UE, axée sur la transparence, la responsabilité et les droits fondamentaux, rendrait certainement les systèmes d'IA plus dignes de confiance pour les citoyens européens que pour leurs homologues américains et chinois.

Par ailleurs, une protection limitée offre aux entreprises d'IA un environnement plus propice à entraîner leurs algorithmes, les rendant ainsi plus efficaces et donc davantage dignes de confiance. La disponibilité des données en Chine et aux États-Unis est un véritable atout qui pourrait entraver les ambitions d'innovation de l'Europe.

Cependant, si l'UE parvient à réglementer l'IA tout en maintenant sa position sur le marché mondial, son modèle de gouvernance deviendrait un exemple pour nombre de juridictions qui suivraient alors sa voie.

Enfin, et surtout, les divergences en matière d'éthique posent un problème majeur à une réglementation mondiale, alors que les systèmes d'IA deviennent de plus en plus complexes et interconnectés, et qu'aucun consensus n'a pu être trouvé sur la manière de les réglementer.

## OPPORTUNITES ET VOIES A SUIVRE

Par l'analyse de ces trois juridictions, on peut remarquer à quel point leurs priorités nationales influent sur leur manière de réglementer l'IA. La question demeure alors de savoir quelle serait la meilleure voie à suivre.

Après avoir expliqué la nécessité d'un processus d'harmonisation mondiale, les limites posées par chaque système seront analysées, tout en exposant des principes pouvant être acceptés de tous. Ensuite, le rôle des organisations internationales et initiatives existantes sera discuté. Enfin, les défis potentiels et les risques d'une approche non globalisée seront mis en évidence.

### I. Nécessité d'harmonisation mondiale

Alors qu'il est évident que la tendance actuelle en matière de réglementation de l'IA se produit au niveau national, il est important de considérer l'élaboration d'une solution internationale, compte tenu de l'impact mondial de la plupart des systèmes d'IA, et notamment des TRF.

L'aspect intéressant des TRF est leur utilisation répandue mondialement, mais dans des contextes significativement différents d'un pays à l'autre. Ces différences sont encore plus évidentes une fois l'analyse des différentes approches réalisée. Cela ne doit néanmoins pas devenir un obstacle à l'élaboration d'un cadre mondial.

Un aspect essentiel de la réglementation de l'IA, brièvement mentionné dans l'introduction de cette recherche, est la confiance du public dans les systèmes d'IA. En effet, si le concept d'IA « digne de confiance » développé par l'UE tend à favoriser leur fiabilité en termes de sécurité publique, la confiance du public dans ces systèmes ne doit pas être sous-estimée.

Sur le plan économique, des études ont démontré l'importance de la confiance des consommateurs dans le choix des systèmes avec lesquelles ils décident d'interagir. De même, dans les juridictions où le choix ne leur est pas donné, le manque de transparence entraîne une baisse de la confiance, des pertes économiques et des troubles publics potentiels.

De surcroit, dans un contexte de mondialisation de l'IA, la confiance mutuelle entre pays devra se construire. Afficher des réglementations similaires est un moyen d'éviter des perturbations économiques et des comportements opportunistes de la part des acteurs du marché.

Le sujet des TRF est cependant extrêmement sensible dans le contexte de « guerre froide »[80] entre les autoproclamées « démocraties » et les régimes décrits comme « autoritaires ». L'approche visant à établir des règles similaires est ardue compte tenu des points de vue divergents ; les derniers les considérant comme vitales à leur sécurité publique, les premières que leur usage doit se faire dans la plus grande des modérations.

Dans l'actualité récente, l'utilisation des systèmes d'IA chinois a été largement critiquée dans l'opinion publique américaine et a donné lieu à des auditions très médiatisées au Congrès, qui ont toutes confirmé le caractère dangereux de ces applications et ont proposé des mesures d'interdiction pour les contrer[81]. De telles accusations ciblées rendent ardues les perspectives d'harmonisation, mais soulignent l'importance de promulguer des règles mondialement applicables pour garantir un développement convergent de ces technologies.

Des craintes apparaissent également quant aux comportements de "shopping juridique" que certains acteurs du marché pourraient adopter[82]. En effet, de tels comportements existent déjà pour plusieurs raisons, la plus importante étant fiscale. Dans ce domaine, des appels à une harmonisation mondiale se sont également fait entendre, bien que le contexte soit à la prudence, de peur d'entraver l'activité économique. On peut supposer que de telles positions pourraient être prises par des juridictions puissantes en matière d'IA, qui souhaiteraient éviter que leurs talents ne fuient vers des juridictions plus souples sur le plan réglementaire.

## II. Apprendre des modèles existants

Partant de cette perspective, il est clair que l'approche adoptée par chaque juridiction est liée à sa position économique dans le paysage mondial du développement de l'IA, avec des conséquences sur le niveau de contrôle qu'elle souhaite exercer sur les acteurs du marché.

L'UE, d'une part, s'est positionnée en tant que superpuissance réglementaire avec son RGPD, ouvrant la voie à de nombreuses juridictions pour suivre sa position en matière de protection des données, et tente de faire de même avec l'approche équilibrée de son AIA.

---

80 Le terme « guerre froide » est souvent utilisé pour décrire la situation géopolitique de ce début de XXI[e] siècle, où une « alliance » entre la Fédération de Russie et la RPC menace la suprématie des États-Unis et de leurs alliés à l'échelle mondiale, entraînant de nombreuses tensions au niveau international.

81 Shepardson, D., & Ayyub, R. (2023). TikTok congressional hearing: CEO Shou Zi Chew grilled by US lawmakers. *Reuters*. https://www.reuters.com/technology/tiktok-ceo-face-tough-questions-support-us-ban-grows-2023-03-23/

82 Wagner, B. (2018). Ethics as an Escape from Regulation: From ethics-washing to ethics-shopping? in M. Hildebrandt (Ed.), *Being Profiling: Cogitas ergo sum*. *Amsterdam University Press*.

Cependant, elle agit comme tel en raison de sa moindre position sur le paysage global du développement de l'IA. L'UE manque en effet d'acteurs puissants et cherche donc à protéger les intérêts de ses citoyens par la réglementation. L'accent mis sur les droits humains et la transparence est révélateur d'un mécanisme de défense face à des développements qu'elle ne peut contrôler. Néanmoins, l'UE bénéficie d'une position économique importante dans d'autres domaines, grâce au développement élevé de sa population, faisant d'elle un acteur réglementaire incontournable[83].

D'autres part, les États-Unis et la Chine jouissent d'une position plus puissante dans le paysage du développement de l'IA, se traduisant par une approche plus libérale, avec leurs propres variations politiques. L'approche américaine du laisser-faire a été adoptée pour favoriser la flexibilité et l'innovation, tandis que la Chine a clairement pour objectif de devenir le leader mondial de l'IA d'ici 2030, conduisant à une réglementation laxiste permettant la mise en œuvre rapide et généralisée d'applications d'IA dans l'espace public[84].

La position mondiale de chaque juridiction joue donc un rôle important dans sa volonté de réglementation et d'établissement de normes plus ou moins strictes pour les systèmes d'IA.

Par ailleurs, l'exemple du RGPD a démontré qu'il y a un immense avantage à agir en premier en termes de réglementation. Transposé d'un concept économique selon lequel les entreprises peuvent obtenir un avantage concurrentiel sur le marché en étant les premières à lancer un nouveau produit ou service, « l'avantage du premier arrivé » fonctionne de la même manière pour les instruments juridiques[85]. Comme l'explique Nathalie Smuha dans un travail similaire, l'adoption de conditions réglementaires strictes dans un pays aura un effet domino sur d'autres juridictions en raison des coûts de conformité supportés par les entreprises multinationales, et du lobbying ultérieur qu'elles exerceront dans d'autres juridictions pour ne pas subir de désavantage économique supplémentaire[86]. L'importance d'agir en premier ne peut donc pas être négligée, et c'est de cet avantage dont l'UE veut se saisir avant que d'autres juridictions ne proposent d'autres normes.

Les principes établis par l'UE dans son AIA, s'ils aboutissent aux mêmes résultats que ses autres instruments juridiques, pourraient servir de principes généraux nécessaires à ce processus d'harmonisation mondiale. Le RGPD a en effet servi de base à d'autres initiatives législatives aux États-Unis et en Chine, telles que le CCPA[87] et la LPIP[88], et il n'est pas exclu que de nouvelles normes sur l'IA suivent la même voie avec l'AIA.

---

83 Safari, B. (2017). Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. *Seton Hall Law Review*, 47(3), Article 6.

84 *Ibid.*, voir note 13.

85 Smuha, N. A. (2021). From a 'Race to AI' to a 'Race to AI Regulation': Regulatory Competition for Artificial Intelligence. *Law, Innovation & Technology*, 13(1), p. 4.

86 *Ibid.*, p. 18.

87 Gunst, S., & De Ville, F. (2021). The Brussels effect: how the GDPR conquered Silicon Valley. *European Foreign Affairs Review*, 26(3), 437–458.

88 Tan, Z., & Zhang, C. (2022). China's PIPL and DSL: Is China following the EU's approach to data protection? *Journal of Data Protection & Privacy*, 5(1), 7-25.

Néanmoins, tout porte à croire que ce processus d'harmonisation ne pourrait jamais résulter en une solution universelle, car les différences politiques entre les juridictions sont trop importantes pour aboutir aux mêmes solutions[89]. En prenant les TRF pour exemple, il est très difficile d'imaginer que la Chine adopte une interdiction similaire à celle de l'UE pour une utilisation de ces systèmes à des fins de maintien de l'ordre, car elle est devenue une partie trop importante de son appareil répressif en constante expansion. Seul un changement de régime ou de paradigme pourrait conduire à des positions internationales convergentes. Par ailleurs, une approche plus générale pourrait être envisagée, laissant les réglementations spécifiques à l'évaluation des intérêts nationaux de chaque pays[90].

En laissant de côté cette analyse économique, on peut constater que les trois principales juridictions analysées ont développé des principes intéressants qui feront certainement partie des futurs standards internationaux en matière de régulation de l'IA. Bien qu'un cadre juridique commun ne soit peut-être ni réalisable, ni souhaitable, il est néanmoins probable que, pour développer davantage la collaboration internationale, les pays s'alignent sur des principes clés, ne se traduisant pas nécessairement en une matérialisation juridique identique.

L'UE s'est positionnée à l'avant-garde de la transparence, de la responsabilité et de la sécurité, en tenant compte de questions éthiques, comme le respect des droits de l'homme et de la vie privée. Les États-Unis ont été de fervents défenseurs de l'innovation, tout en veillant à ce que les systèmes d'IA soient sûrs et sécurisés pour leurs citoyens. La Chine, elle, a mis un accent sur les questions de sécurité, en promouvant l'innovation chez ses géants de la technologie.

Il est certain qu'un accord sur ces principes ne se produira pas dans un avenir proche, car les considérations politiques, économiques et culturelles actuelles ne permettront pas de trouver de terrains d'entente. On peut cependant imaginer que les pays se mettent d'accord sur des notions ayant des compréhensions locales différentes. Le concept des droits de l'homme est devenu controversé car les pays occidentaux l'ont utilisé pour s'opposer à certains systèmes politiques, poussant ces systèmes à développer leurs propres définitions[91]. La même situation pourrait se produire pour les normes internationales de développement de l'IA.

## III. Rôle des organisation internationales

Dans cette quête au terrain d'entente, une voie à explorer pourrait être celle des organisations internationales, favorisant le dialogue et les compromis entre doctrines nationales. La position des organisations internationales se sont souvent révélées pertinentes, et certaines ont déjà pris position sur l'IA. L'OCDE, le Conseil de l'Europe et l'UNESCO ont tous trois publié des directives éthiques sur l'IA et sont en soi déjà des exemples de coopération internationale.

---

89 *Ibid.*, voir note 88, p. 22. N. Smuha parle dans son article de la « recherche du plus petit dénominateur commun de mesures de protection que chaque État autour de la table peut accepter ».

90 *Ibid.*

91 Pour davantage d'information sur le relativisme lié aux droits de l'homme : Angle, S. C. (2002). Human Right and Chinese Thought: A Cross-Cultural Inquiry. *Cambridge University Press*. ISBN 0521809711, *et* Brilmayer, L., & Huang, T. (2015). The Illogic of Cultural Relativism in Global Human Rights Debate. *The Global Community Yearbook of International Law and Jurisprudence 2014: Volume I*, pp. 17-34. https://doi.org/10.1093/acprof:oso/9780190270513.003.0002

Cependant, ces organisations internationales servent également de champs de bataille entre États membres : tandis que les normes de l'OCDE ressemblent beaucoup aux lignes directrices de l'UE sur une IA « digne de confiance »[92], la position de l'UNESCO sur « l'IA et l'éducation » s'appuie largement sur les lignes directrices chinoises élaborées par leur Institut National des Normes et de Technologie[93]. Néanmoins, elles montrent qu'un certain degré de convergence existe déjà au niveau international, pouvant être la première étape du processus.

Toutefois, seul l'avenir nous dira si des instruments plus normatifs sur la question verront le jour[94]. Dans le cas de la reconnaissance faciale, la perspective des droits de l'homme pourrait être prise en compte et conduire à l'intervention réglementaire du Conseil des droits de l'homme des Nations Unies ou autres organisations associées[95].

## IV. Risque de dépassement technologique

Le plus grand défi de la réglementation des nouvelles technologies réside dans leur contexte, en constante évolution. Avec de nouvelles applications d'IA développées de manière exponentielle chaque année, le risque de voir les réglementations devenir obsolètes est élevé et oblige les législateurs à trouver des règles innovantes pour anticiper ces changements.

C'est le défi que l'UE a relevé avec l'adoption de son AIA ; un défi que les États-Unis et la Chine ne sont actuellement pas prêts à tenter pour la simple raison qu'ils craignent qu'une réglementation excessive n'entrave le développement de l'IA.

Néanmoins, que la loi doive s'adapter aux innovations n'est pas un fait nouveau, rendant le futur de la réglementation de l'IA d'autant plus imprévisible, tant il manque des données économiques et technologiques à l'équation. Les futurs travaux de recherche trouveront certainement leur plus-value dans l'étude des effets des normes appelées à naître dans les années à venir, afin de trouver des solutions acceptables par tous les acteurs de l'IA.

En tout état de cause, un contexte international de développement de l'IA déréglementé ou à deux vitesses ne serait pas souhaitable, bien qu'il soit clair que les différences politiques se creusent entre pays. La mise en place de cadres juridiques drastiquement différents n'irait pas dans le sens de la coopération internationale requise pour cette révolution anthropologique, et risquerait de créer un environnement ultra-concurrentiel, dans lequel maîtriser l'IA assurerait la dominance mondiale[96], que certains pourraient envisager quel qu'en soit le prix.

---

92 De la même manière, l'UE attend également l'avis de l'OCDE sur la question, comme le montre le choix de la définition précise de « système d'IA », sur lequel l'UE hésite encore.

93 La Chine a également joué un rôle de premier plan dans les efforts de l'UNESCO sur l'IA dans l'éducation. En mai 2019, Pékin a accueilli une conférence ministérielle organisée par l'UNESCO, aboutissant à l'établissement du "Consensus de Beijing sur l'IA et l'éducation". Ce consensus a mis l'accent sur les considérations éthiques et les implications en matière de droits de l'homme liées à l'utilisation de l'IA dans le domaine de l'éducation.

94 Les examens éthiques susmentionnés sont cependant considérés comme la première étape de l'élaboration de normes et dispositions plus spécifiques, ce qui est prometteur pour l'avenir.

95 Tenant compte encore du relativisme que de tels principes pourraient entraîner ; voir note 94.

96 Cette conclusion sert de rappel aux propos que le président de la Fédération de Russie, Vladimir Poutine, a tenus en 2017 dans une interview accordée à la chaîne de télévision nationale russe, expliquant que "le leader en intelligence artificielle régnera sur le monde".

# CONCLUSION

Cette thèse, à travers l'analyse des approches qu'ont pris l'UE, les États-Unis et la Chine pour réglementer les systèmes d'IA à haut risque, en ce compris les technologies de reconnaissance faciale, montre que celles-ci varient considérablement en fonction de l'histoire politique, des structures politiques, des valeurs et des objectifs stratégiques de chaque région.

L'AI Act proposé par l'UE présente à ce jour l'approche la plus complète, en introduisant une échelle de risques spécifiquement adaptée pour aborder les questions d'IA à risque élevé. Cette approche met l'accent sur les principes de transparence, de responsabilité et de protection des droits fondamentaux, ce qui pourrait davantage encourager la confiance du public dans les systèmes d'IA. Néanmoins, malgré les efforts destinés à trouver le bon équilibre, le nombre d'obligations imposées aux applications considérées comme à haut risque pourrait potentiellement entraver leur développement et l'innovation plus générale sur le territoire de l'UE.

Les États-Unis, tels qu'illustrés par l'État de Californie, ont adopté une approche plus flexible, qui encourage l'innovation avec des réglementations spécifiques, par secteur, et toujours en réaction à une demande sociétale urgente. Cependant, cette innovation est atténuée par l'absence d'un cadre fédéral complet et clair, spécifiquement axé sur l'IA à haut risque. De plus, les incohérences entre les approches fédérales et celles des États révèlent d'importants problèmes dans la protection de la vie privée et des libertés civiles de leurs citoyens.

Enfin, l'approche verticale de la Chine, motivée par son ambition de devenir le leader mondial de l'IA d'ici 2030, met fortement l'accent sur la croissance économique, la sécurité nationale et la stabilité sociale. Bien qu'elle soit efficace dans la promotion de l'innovation sur son territoire et dans le développement de l'IA en général, cette approche ne s'est révélée que peu concluante en termes de protection de la vie privée, notamment dans le déploiement de systèmes d'IA tels que les TRF dans les espaces publics à des fins de maintien de l'ordre.

Les différences dans ces approches réglementaires ont des conséquences significatives dans le développement de normes mondiales en matière d'IA à haut risque, dont la présence est désormais véritablement globale. Par ailleurs, elles ont un impact important sur la stimulation de l'innovation, la confiance du public et le respect des normes éthiques par les acteurs de l'IA, notamment en ce qui concerne la protection des libertés civiles.

Trouver le bon équilibre entre l'innovation et la limitation des risques est essentiel pour réglementer les systèmes d'IA à haut risque en pleine expansion. L'étude de ces trois approches diverses fournit des informations essentielles qui peuvent éclairer les prochaines étapes de régulation de l'IA à haut risque.

A l'avenir, trouver cet équilibre sera de plus en plus complexe, mais crucial pour protéger les droits fondamentaux et les valeurs sociétales, tout en favorisant le progrès technologique. La coopération internationale est la clé pour atteindre cet objectif, à une époque où les systèmes d'IA sont de plus en plus globalisés. L'établissement de normes et de pratiques communes répondant aux préoccupations liées aux systèmes à haut risque est essentiel au développement d'une société plus sûre où chacun peut en profiter.

# REFERENCES


Ala-Pietilä, P., & Smuha, N. A. (2021). A Framework for Global Cooperation on Artificial Intelligence and its Governance. In B. Braunschweig & M. Ghallab (Eds.), *Reflections of AI for Humanity (Forthcoming)*. *Springer*.

Angle, S. C. (2002). Human Right and Chinese Thought: A Cross-Cultural Inquiry. *Cambridge University Press*. ISBN 0521809711.

Bertuzzi, L. (2021). MEPs seal the deal on Artificial Intelligence Act. *Euractiv*. https://www.euractiv.com/section/artificial-intelligence/news/meps-seal-the-deal-on-artificial-intelligence-act/

Bowie, N. (2021). The Constitutional Right of Self-Government. *The Yale Law Journal*. https://www.yalelawjournal.org/article/the-constitutional-right-of-self-government

Brilmayer, L., & Huang, T. (2015). The Illogic of Cultural Relativism in Global Human Rights Debate. *The Global Community Yearbook of International Law and Jurisprudence 2014: Volume I*, pp. 17-34. https://doi.org/10.1093/acprof:oso/9780190270513.003.0002

Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. *Telecommunications Policy* Vol. 47, Issue 5. https://doi.org/10.1016/j.telpol.2022.102482

Cho, E. (2020). The Social Credit System: Not Just Another Chinese Idiosyncrasy. *Princeton University Press.* https://jpia.princeton.edu/news/social-credit-system-not-just-another-chinese-idiosyncrasy

Confessore, N. (2018). Cambridge Analytica Scandal: The Fallout. *The New York Times*. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Conger, K., Fausset, R., & Kovaleski, S. F. (2019). San Francisco Bans Facial Recognition Technology. *The New York Times*. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

Creemers, R., Webster, G., & Triolo, P. (2017). Translation: Cybersecurity Law of the People's Republic of China (中华人民共和国网络安全法). https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

Cunningham, E., Saich, T., & Turiel, J. (2020). Understanding CCP Resilience: Surveying Chinese Public Opinion Through Time. *Harvard Kennedy School, Ash Center for Democratic Governance and Innovation*. https://ash.harvard.edu/files/ash/files/final_policy_brief_7.6.2020.pdf

Davies, D. (2021). Facial Recognition And Beyond: Journalist Ventures Inside China's 'Surveillance State'. *Fresh Air*. *NPR*. https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta

De Cooman, J. (2022). Humpty dumpty and high-risk ai systems: the ratione materiae dimension of the proposal for an EU Artificial Intelligence Act. *Market and Competition Law Review*, 6(1), 49-88.

European Commission (2020). White Paper on Artificial Intelligence - A European approach to excellence and trust, pp. 9-25. https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM/2021/206 final - 2021/0106 (COD). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0206&from=EN

European Parliament (2023). Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))1. (Ordinary legislative procedure: first reading). https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html#def_1_1

European Parliament (2016). Study on Liability for Emerging Digital Technologies: Robotics and Artificial Intelligence (EPRS Briefing, No. 593570). https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/593570/EPRS_BRI(2016)593570_EN.pdf

European Union Agency for Fundamental Rights (FRA). (2021). Facial recognition technology: Fundamental rights considerations in law enforcement, p.33. *Publications Office of the European Union*. https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

Feng, Y. (2019). The future of China's personal data protection law: Challenges and prospects. *Asia Pacific Law Review*, 27(1), 62–82.

Fortes, P. R. B., Baquero, P. M., & Amariles, D. R. (2022). Artificial Intelligence Risks and Algorithmic Regulation. *European Journal of Risk Regulation*, 13, 357-372. *Cambridge University Press*. https://doi.org/10.1017/err.2022.14

Garde-Hansen, J. (2019). Always in Focus: Facial Recognition Technology, Optics and Resistance in Political Unrest. *University of Melbourne*. https://law.unimelb.edu.au/news/caide/always-in-focus-facial-recognition-technology,-optics-and-resistance-in-political-unrest

Garvie, C., Bedoya, A., & Frankle, J. (2016). The Perpetual Lineup, Unregulated Police Face Recognition in America. *Center on Privacy and Technology, Georgetown University Law School*. https://www.perpetuallineup.org/

Garhart, N., & Stephens, R. (2022). Employee Data Under the CCPA: Expiration of the Employee Exception. *JD Supra*. https://www.jdsupra.com/legalnews/employee-data-under-the-ccpa-expiration-6993807/#:~:text=Indeed%2C%20under%20the%20CCPA%2C%20%E2%80%9C

Gerlach, N. (2023). The case of the EU AI Act: Why we need to return to a risk-based approach. *International Association of Privacy Professionals* (IAPP). https://iapp.org/news/a/the-case-of-the-eu-ai-act-why-we-need-to-return-to-a-risk-based-approach/

Gunst, S., & De Ville, F. (2021). The Brussels effect: how the GDPR conquered Silicon Valley. *European Foreign Affairs Review*, 26(3), 437–458.

Hangzhou Fuyang District People's Court. (2019). Guo v. Hangzhou Safari Park, 0111 Zhejiang. Supp. 6971 https://www.qcc.com/wenshuDetail/f491af7adaa22ea27ea81c891423f55e.html.

Helberger, N. & Diakopoulos, N. (2023). ChatGPT and the AI Act. *Internet Policy Review*, 12(1). https://doi.org/10.14763/2023.1.1682.

High-Level Expert Group on Artificial Intelligence (European Commission) (2019). Ethics Guidelines for Trustworthy AI, p. 7. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Johnson, T. L., Johnson, N. N., McCurdy, D., et Olajide, M. S. (2022). Facial recognition systems in policing and racial disparities in arrests. *Government Information Quarterly*, 39(4), 101753. https://doi.org/10.1016/j.giq.2022.101753.

Kennedy, B., Tyson, A., & Saks, E. (2023). Public Awareness of Artificial Intelligence in Everyday Activities. *Pew Research Center*. https://www.pewresearch.org/science/2023/02/15/public-awareness-of-artificial-intelligence-in-everyday-activities/

Kostka, G., Steinacker, L., & Meckel, M. (2023). Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly*, 40(1), 101761. https://doi.org/10.1016/j.giq.2022.101761

Lau, C. (2023). China Arrests Person for Generating Inappropriate Content with AI Chatbot. *CNN*. https://edition.cnn.com/2023/05/09/tech/china-arrest-chatgpt-hnk-intl/index.html

Liebl, A. & Klein, T. (2022). AI Act Impact Survey. *AppliedAI*. https://www.appliedai.de/hub/ai-act-impact-survey

Liu, Y. L., Yan, W., & Hu, B. (2021). Resistance to facial recognition payment in China: The influence of privacy-related factors. *Telecommunications Policy*, 45(5), 1–18. https://doi.org/10.1016/j.telpol.2021.102155

Mukherjee, S., Chee, F. Y., & Coulter, M. (2023). EU lawmakers' committee reaches deal on artificial intelligence act. *Reuters*. https://www.reuters.com/technology/eu-lawmakers-committee-reaches-deal-artificial-intelligence-act-2023-04-27/.

Najibi, A. (2020). Racial discrimination in face recognition technology. *Science in the News*. *Harvard Blogs*. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

National Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security. (2022, November 25). Provisions on the Administration of Deep Synthesis Internet Information Services (国家互联网信息办公室工业和信息化部公安部). http://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm

National People's Congress. (2021). Data Security Law of the People's Republic of China (中华人民共和国数据安全法). http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml

National People's Congress. (2021). Personal Information Protection Law (PIPL) of the People's Republic of China (中华人民共和国个人信息保护法). http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.html

Powell, L. C. (2022). The Good, the Bad, and the Ugly: Black Lives Matter Protests, the January 6th Insurrection, and Facial Recognition Technology as Admissible Evidence. 72 *American Universities Law Review* 277.

Roose, K. 2023. "A Conversation with Bing's Chatbot Left Me Deeply Unsettled," The New York Times, February 16. https://www.nytimes.com/2023/02/16/technology/bing-chatbot-microsoft-chatgpt.html.

Rosenthal, A. (2021). Individuals under observation: the law responds to (live) facial recognition technology. *Cambridge Law Review*, 6(2), 86-118.

Safari, B. (2017). Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. *Seton Hall Law Review*, 47(3), Article 6.

Shepardson, D., & Ayyub, R. (2023). TikTok congressional hearing: CEO Shou Zi Chew grilled by US lawmakers. *Reuters*. https://www.reuters.com/technology/tiktok-ceo-face-tough-questions-support-us-ban-grows-2023-03-23/

Smuha, N. A. (2021). From a 'Race to AI' to a 'Race to AI Regulation': Regulatory Competition for Artificial Intelligence. *Law, Innovation & Technology*, 13(1).

Sorkin, A. R., Mattu, R., Warner, B., Kessler, S., de la Merced, M. J., Hirsch, L., & Livni, E. (2023). Why Lawmakers Aren't Rushing to Police A.I. *Dealbook*. *The New York Times*. https://www.nytimes.com/2023/03/03/business/dealbook/lawmakers-ai-regulations.html

Supreme People's Court. (2021). The Supreme People's Court's Provisions on Several Issues on the Application of Law in Hearing Civil Cases Related to the Use of Facial Recognition Technology to Handle Personal Information (最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定). http://www.court.gov.cn/fabu-xiangqing-315851.html

Supreme People's Court. (2021). Provisions of the Supreme People's Court on several issues concerning the application of law in civil cases relating to the use of face recognition technology in handling personal information. http://www.court.gov.cn/zixun-xiangqing-315831.html.

Tan, Z., & Zhang, C. (2022). China's PIPL and DSL: Is China following the EU's approach to data protection? *Journal of Data Protection & Privacy*, 5(1), 7-25.

The China Academy of Information and Communications Technology (CAICT). (2022). Artificial Intelligence White Paper (人工智能白皮书). http://www.caict.ac.cn/kxyj/qwfb/bps/202204/P020220412613255124271.pdf

Tomada, L. (2022). Start-Ups and the Proposed EU AI Act: Bridges or Barriers in the Path from Invention to Innovation?. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 13(1), 53-66.

Wagner, B. (2018). Ethics as an Escape from Regulation: From ethics-washing to ethics-shopping? in M. Hildebrandt (Ed.), *Being Profiling: Cogitas ergo sum*. *Amsterdam University Press*.

Weaver, J. (2020). AI issues raised by the California consumer privacy act. *RAIL: The Journal of Robotics, Artificial Intelligence & Law*, 3(1), 73-[i].

Webster, G., Creemers, R., Kania, E., et Triolo, P. (2017). Full Translation: China's New Generation Artificial Intelligence Development Plan. *DigiChina, a Stanford University initiative*. https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

Webster, G., Creemers, R., Kania, E., & Triolo, P. (2017). Translation: China's New Generation of Artificial Intelligence Development Plan. *New America*. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-generation-artificial-intelligence-development-plan/

Weiser, D. (2021). Why Lobbying Is Legal and Important in the US. *Investopedia*. https://www.investopedia.com/articles/investing/043015/why-lobbying-legal-and-important-us.asp

Wu, T. (2020). California at Crossroads Over Policing and Facial Recognition. *Bloomberg Law*. https://news.bloomberglaw.com/privacy-and-data-security/california-at-crossroads-over-policing-and-facial-recognition