WilhelmGilliéron
AVOCATS

PROPRIÉTÉ INTELLECTUELLE

Réglementations en matière d'intelligence artificielle : un tour d'horizon

PHILIPPE GILLIÉRON
Avocat

Auteur: Wilhelm Gilliéron Avocats | Le : 20 novembre 2023

Réglementations en matière d'intelligence artificielle : un tour d'horizon

2023 aura été l'année de la prise de conscience pour le grand public du potentiel des systèmes d'intelligence artificielle (IA), plus particulièrement depuis le lancement de ChatGPT.

Face aux enjeux posés par l'IA, des efforts réglementaires se dessinent, à commencer par la proposition de Règlement européen sur l'IA, dont la dernière séance de trilogue se tiendra le 6 décembre 2023. Si beaucoup espèrent voir cette réglementation entrer en vigueur en 2024, des voix se font entendre pour en douter au vu des points importants sur lesquels un consensus peine à émerger, notamment s'agissant des modèles de fondation.

Toujours est-il qu'il apparaît opportun en cette fin d'année de faire un tour d'horizon des efforts en la matière, sans avoir la prétention d'entrer dans les détails.

I. Réglementation européenne sur l'IA

L'Union européenne apparaît comme le fer de lance en la matière. Une fois entrée en vigueur et à l'image du RGPD, la Réglementation sur l'IA déploiera des effets extraterritoriaux, puisqu'elle s'appliquera à tout fournisseur commercialisant de tels systèmes au sein de l'UE, ainsi qu'aux utilisateurs dont les résultats (*outputs*) faisant suite à l'utilisation de tels systèmes seraient utilisés au sein de l'UE. De nombreuses entreprises suisses s'y verront ainsi soumises.

La réglementation repose sur une appréciation des risques, en distinguant quatre catégories de systèmes :

1. Les systèmes présentant un risque inacceptable, interdits, par quoi la proposition entend les systèmes recourant à des techniques subliminales, ceux exploitant la vulnérabilité de certains groupes (enfants, personnes âgées) ou encore ceux utilisés pour calculer un crédit social. Demeure ouverte la question de savoir s'il convient de bannir purement et simplement le recours à

des systèmes d'identification biométrique en temps réel dans les espaces publics, ou s'il convient de prévoir certaines exceptions à cette interdiction, point sur lequel les avis des institutions européennes divergent.

2. Les systèmes à hauts risques, premiers visés par la réglementation et soumis à de nombreuses exigences, par quoi la proposition entend ceux mis en œuvre en des secteurs considérés particulièrement sensibles (infrastructures techniques, éducation et formation, ressources humaines, accès et droit à des services essentiels, autorités répressives, administration de la justice et processus démocratique, contrôle des frontières et migration) ou ceux intégrés à des produits d'ores et déjà soumis à certaines réglementations en matière de sécurité (comme les jouets, transports, etc.). La possibilité d'obtenir certaines exceptions, et les conditions de ces exceptions, demeure un point de discussion.

3. Les systèmes à risques limités, essentiellement soumis à une obligation de transparence, parmi lesquels on vise en particulier les systèmes de chatbot, ceux susceptibles de détecter les émotions ainsi que les outils génératifs dont les LLM (large language models) font partie. Là aussi, la manière dont ces systèmes seront exactement réglementés demeure discutée et pourrait être le point bloquant majeur, la France, l'Allemagne et l'Italie s'opposant désormais à ce que la question soit traitée au sein du Règlement.

4. Les systèmes ne présentant qu'un risque minime ou aucun risque, qui ne sont pas concernés par la proposition même si l'adoption de codes de conduite par les acteurs concernés est recommandée.

La réglementation vise pour l'essentiel les systèmes à haut risque, en imposant aux développeurs et, dans une moindre mesure aux distributeurs, importateurs et utilisateurs de ces systèmes certaines exigences à respecter lors de leur développement et de leur commercialisation.

Sans entrer ici dans les détails, ces développeurs devront ainsi, entre autres, mettre en place un système d'appréciation des risques, de gestion de la qualité, fournir de la documentation technique et des informations autour des données utilisées, ainsi que s'enregistrer dans une base de données tenue par la Commission européenne. En toute hypothèse, le système devrait toujours pouvoir être arrêté par une intervention humaine.

La question de la mise en œuvre de la réglementation demeure un sujet de discussion. Si le Parlement est favorable à la nomination d'une autorité par pays et une autorité centrale au niveau européen, la Commission plébiscite la possibilité d'avoir plusieurs autorités compétentes au sein d'un même pays, les institutions divergeant par ailleurs quant au poids que devrait jouer l'organisme européen par rapport aux autorités nationales.

Reprenant l'approche adoptée pour le RGPD, la réglementation prévoit des amendes salées en cas de non respect, puisque l'amende peut aller jusqu'au montant le plus important d'entre le 6% du chiffres d'affaire global ou € 30 millions en cas de commercialisation d'un système interdit, respectivement le 4% ou € 20 millions en cas de manquement à la plupart des obligations.

Suivies de près, les négociations n'ont cependant pas encore abouti, certains redoutant que le Règlement ne devienne un frein à l'innovation favorisant la concurrence américaine et chinoise au détriment des européens, en particulier en ce qui a trait aux PME, par des exigences trop importantes dont le respect s'avérerait trop coûteux. Affaire à suivre dans les jours qui viennent.

II. USA

Le 30 octobre 2023, le Président Biden a émis un décret exécutif intitulé « *Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence* ». L'objectif de ce décret consiste à favoriser l'innovation tout en garantissant la sécurité, la protection de la vie privée et l'équité dans le développement et l'utilisation de l'IA aux États-Unis, tout en encourageant la coopération internationale.

A la différence de l'approche européenne, l'approche américaine ne consiste pas à adopter une loi fédérale qui s'imposerait à chacun, mais à établir un ensemble de principes et de lignes directrices que les agences fédérales doivent respecter lors de la conception, de l'acquisition, du déploiement et de la supervision des systèmes d'IA. Un accent particulier est mis sur la création de normes strictes pour le criblage de la synthèse biologique, contribuant ainsi à prévenir les risques liés à l'utilisation de l'IA dans la conception de matériaux biologiques dangereux. S'y ajoute l'encouragement d'un cadre de coopération et de coordination entre les différentes parties prenantes, y compris le secteur privé, le monde universitaire, la société civile et les partenaires internationaux.

S'il est louable, le décret souligne l'approche sectorielle toujours favorisée aux Etats-Unis par rapport à une approche horizontale recherchée au sein de l'Union Européenne, et l'absence de volonté d'adopter une loi formelle au niveau fédéral. On peut dès lors craindre que les différents Etats ne continuent à adopter des législations éparses en différents domaines, tel l'Etat du Colorado dans le domaine des assurances ou la ville de New-York dans le domaine de l'emploi, induisant un patchwork difficile à suivre pour les entreprises. Affaire là encore à suivre.

III. Chine

En Chine, le gendarme du Net est la « *Cyberspace Administration of China* » (CAC), autorité toute puissante en la matière. La CAC a été l'une des premières agences à adopter une réglementation sur certaines thématiques particulières. Ainsi en a-t-il été de :

- 1er mars 2022 : réglementation en matière de recommandation algorithmique.
- 25 novembre 2022 : réglementation en matière de données synthétiques.
- 13 juillet 2023 : réglementation en matière d'outils génératifs.

On retrouve dans cette dernière réglementation des soucis communs avec les Etats occidentaux, comme la transparence, la sécurité ou la gouvernance autour des données pour éviter les biais, d'autres sont propres à la Chine comme l'interdiction d'inciter au trouble social et le besoin de se voir attribuer une licence par la CAC. Est particulièrement intéressante l'obligation faite aux développeurs de prendre des mesures pour lutter contre les addictions, respectivement ne pas développer d'algorithme poursuivant un tel objectif (étant précisé qu'une telle obligation ne s'applique que pour les développements internes, non ceux destinés à l'étranger). La réglementation est assortie de sanctions pénales, y compris la possibilité pour la CAC de prononcer une sanction lorsqu'elle l'estime appropriée, quand bien même la réglementation ne le prévoirait pas…

Relevons que la Chine a émis en sus de ces réglementations la volonté d'adopter une loi générale autour du développement et du déploiement de ces systèmes.

IV. Autres

Des efforts législatifs se sont également dessinés à des degrés divers au Brésil, au Mexique, au Japon ou à Singapour. Bien qu'il n'existe aucune loi au sens formel édictée à Singapour ou en passe de l'être, cet Etat a mis sur pied un cadre intéressant de gouvernance autour de l'adoption de ces systèmes appelé « AI Verify ».

Ce cadre, tout comme celui adopté aux Etats-Unis par NIST, constituent d'importants référentiels, que certains experts considèrent au final avec les nombreux standards adoptés aujourd'hui par des instituts comme ISO/IEC comme des outils plus adéquats que l'adoption de lois au sens formel.

V. Conclusion

Au final, on constate que de nombreuses initiatives se dessinent ainsi pour encadrer le développement et le déploiement de systèmes IA au sein de différents pays.

Si les approches divergent, une certaine uniformité se dessine en ce qui a trait aux grands principes, tels que reflétés par l'adoption à Hiroshima le 30 octobre 2023 par le G7 d'un accord en la matière.

La prise de conscience des enjeux que présentent le développement et le déploiement de ces systèmes, ressortie lors de différents sommets récents tenus en ce mois de novembre 2023, devrait conduire à un renforcement de la coopération internationale en la matière.

S'il est difficile de savoir quelle est la meilleure approche, il apparaît clair qu'une approche purement nationale apparaît un bien mauvais garde-fou, par ailleurs source d'interrogations sous l'angle de la compétitivité internationale, comme le reflètent les discussions entourant l'adoption du Règlement sur l'IA au sein de l'Union Européenne.

Il ne reste plus qu'à espérer qu'après ces démarches isolées s'étant dessinées en 2023, 2024 sera l'année de la concertation et de la coopération internationale en la matière. Affaire à suivre.

Source : https://www.wg-avocats.ch/actualites/reglementations-en-matiere-dintelligence-artificielle-un-tour-dhorizon/