Lex Electronica

Lex Electronica

L'intelligence artificielle (IA) : le rôle des États face aux géants numériques. L'exemple de l'Union européenne (UE)

Céline Castets-Renard

Volume 29, numéro 4, 2024

Souveraineté culturelle et géants numériques : regards croisés : Canada, Québec, France, Belgique

URI : https://id.erudit.org/iderudit/1115126ar
DOI : https://doi.org/10.7202/1115126ar

Aller au sommaire du numéro

Éditeur(s)

Centre de recherche en droit public Université de Montréal

ISSN

1480-1787 (numérique)

Découvrir la revue

Citer cet article

Castets-Renard, C. (2024). L'intelligence artificielle (IA) : le rôle des États face aux géants numériques. L'exemple de l'Union européenne (UE). *Lex Electronica*, *29*(4), 44–49. https://doi.org/10.7202/1115126ar

L'INTELLIGENCE ARTIFICIELLE (IA) : LE RÔLE DES ÉTATS FACE AUX GÉANTS NUMÉRIQUES. L'EXEMPLE DE L'UNION EUROPÉENNE (UE)

Céline Castets-Renard[15]

15 Professeure titulaire, Section de droit civil à la Faculté de droit de l'Université d'Ottawa et titulaire de la Chaire de recherche sur l'intelligence artificielle responsable à l'échelle mondiale.

[1] Monsieur le Président, je voudrais bien sûr remercier les collègues du CRDP et du Laboratoire de cyberjustice pour leur belle invitation, tout particulièrement le professeur Nicolas Vermeys. Je suis particulièrement ravie de venir ici à l'Université de Montréal comme très souvent, très régulièrement participer aux activités du Centre. C'est toujours très stimulant et plaisant.

[2] Ma mission du jour est plutôt de parler du droit canadien, c'est-à-dire du projet de loi C-27, mais je vais faire des petites passerelles avec le droit de l'Union européenne, puisque c'est aussi un droit que je connais bien depuis plusieurs années. En outre, l'Union européenne s'est mise en marche dès le mois d'avril 2021 pour réguler l'IA, ce qui a évidemment influencé les autres législateurs ailleurs dans le monde. Je ne suis pas pour autant certaine qu'il y ait un « effet Bruxelles » selon les travaux de la professeure Anu Bradford (2020). C'est un « concept valise » que tout le monde aime emprunter mais qui ne veut plus rien dire, mis à part le fait que l'Union européenne se met en marche en premier sur les sujets du numérique depuis plus de 10 ans. Donc ce phénomène de leadership et de volonté d'influencer n'est pas nouveau. Par ailleurs, ce n'est pas parce que certains États, comme le Canada, s'inspire un peu de l'Europe que l'on reprend le droit européen, loin s'en faut. La législation européenne, c'est-à-dire le règlement sur l'intelligence artificielle (dit RIA)[16] comporte aujourd'hui 250 pages et je ne crois pas que le projet de loi c-27, la partie 3 sur *Loi sur l'intelligence artificielle et les données* (dite LIAD)[17], fasse 250 pages. La LIAD n'atteindra pas le niveau de complexité du RIA. Pour parler du projet de loi c-27, il s'agit d'un projet de loi publié en juin 2022 et sponsorisé par le ministre Champagne, ministre de l'Innovation, des Sciences et de l'Industrie du Canada. Ce projet de loi intègre une troisième partie sur l'intelligence artificielle et les données qui s'ajoutent à deux autres parties : la première partie vise à réformer la loi LPRPDE, c'est-à-dire la *Loi sur la protection des renseignements personnels et les documents électroniques* dans le secteur privé[18]. La deuxième partie crée un tribunal des renseignements personnels. On peut dire d'emblée que cette troisième partie a beaucoup surpris les parties prenantes. Il est d'ailleurs énormément reproché le manque de concertation dans les discussions devant le Comité INDU (comité permanent de l'industrie et de la technologie) au sein de la Chambre des communes devant lequel le texte est discuté depuis l'automne 2023. Mais une fois la surprise passée, on a eu tout le temps de réfléchir au projet de loi depuis le mois de juin 2022. Je pense qu'il faut aller de l'avant avec ce projet de loi et il faut effectivement réglementer puisqu'il y a un certain nombre de risques liés à l'utilisation de l'IA, notamment des risques de discrimination algorithmique qui ne sont absolument pas acceptables dans nos sociétés. La nécessité de réglementer à mon avis n'est plus vraiment discutée aujourd'hui.

[3] La question est plutôt de savoir comment s'y prendre. Il est vrai qu'à l'origine, ce projet de loi était un peu vide. Mais le ministre Champagne et son ministère ont ajouté

16 Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), *JO L, 2024/1689, 12.7.2024, en ligne :* <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689#d1e 5487-1-1>.

17 Chambre des communes du Canada, 1ère session, 44e législature, 70-71 Elizabeth II, 2021-2022, première lecture 16 juin 2022, Projet de loi C-27, Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois, en ligne : <https://www.parl.ca/documentviewer/fr/44-1/projet-loi/C-27/premiere-lecture>

18 Loi sur la protection des renseignements personnels et les documents électroniques (L.C. 2000, ch. 5).

des informations complémentaires au fur et à mesure dans les mois qui ont suivi. A notamment été publié un document complémentaire, divulgué en mars 2023, ainsi que des amendements au projet de loi apporté par le Ministre Champagne lui-même devant le comité INDU à la Chambre des communes. S'il est un peu surprenant de faire ses propres modifications, c'est aussi un moyen de dire qu'on a entendu les critiques et qu'on veut essayer d'améliorer le texte. Ce faisant, on retrouve quelques influences du droit de l'Union européenne, même le projet de loi canadien est très loin de la complexité du texte européen au plan de la gouvernance, de la multitude des dispositions et obligations mises à la charge des parties prenantes. Ce que l'on peut dire au travers de ces amendements, si je m'en tiens à la dernière version, est une première modification qui me paraît importante portant sur la définition même du système d'intelligence artificielle qui a été modifiée. La même modification s'est produite dans l'Union européenne : on avait au départ dans les deux juridictions une définition qui détaillait les techniques et méthodes de l'IA. Mais, de manière un peu maladroite, on a intégré aussi des techniques incluant des systèmes experts qu'on connaît depuis très longtemps et qui ne sont pas de l'IA. La définition a été resserrée et aujourd'hui la notion d'inférence est une notion. La définition retenue aujourd'hui est qu'un système d'IA est un système qui procède par inférence pour générer des résultats, notamment des prédictions, des recommandations, des décisions ou la génération de contenus. Ce que l'on veut dire avec la notion d'inférence est cette idée d'intelligence : on va inférer et les objectifs des systèmes d'IA peuvent être déterminés par des humains, mais aussi désormais par les systèmes d'IA eux-mêmes. L'inférence se fait à partir de données et on sait que le choix des bases de données constitue un enjeu important, en lien évidemment avec les enjeux de droit d'auteur aussi bien de protection des données personnelles. Il faut aussi comprendre, et c'est là à mon avis qu'est la rupture de l'IA par rapport à des technologies précédentes, c'est le fait que l'IA aujourd'hui puisse mettre en œuvre des fonctions cognitives. Désormais, des systèmes d'IA commencent à se généraliser, par exemple dans les cabinets d'avocats et plus largement pour soutenir des métiers intellectuels. L'arrivée sur le marché de l'IA générative, comme les fameux modèles de langage tels ChatGPT, est une des caractéristiques de l'IA. L'emphase est mise sur les fonctions cognitives de l'IA et cette définition retenue dans le projet de loi canadien rejoint la définition européenne, ainsi que la définition américaine, précisée dans un document élaboré par le NIST qui est l'organe de standardisation américain (NIST, 2023), et reprise par *l'Executive Order* du président Biden sur un développement de l'IA sûr et digne de confiance[19]. Surtout, est reprise la définition de l'OCDE que l'on connaît depuis 2019, modifiée en 2023[20]. On voit qu'il y a un certain alignement international.

[4] Ensuite, dans ce projet de loi canadien, tout comme en Europe et aux États-Unis, une approche par les risques a été retenue. Une partie de la doctrine critique cette approche en disant qu'elle est mal adaptée, d'abord parce que cette approche par les risques est plus traditionnellement appliquée à la sécurité des produits suivant des modèles de conformité avant la mise sur le marché des produits. Tel est le cas dans le domaine pharmaceutique par exemple. Ce n'est peut-être pas tout à fait adapté à l'IA en

19 PRESIDENT BIDEN, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, octobre 2023, en ligne : <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

20 Voir les explications sur les changements apportés à la définition sur le site de l'OCDE, en ligne : <https://oecd.ai/en/wonk/ai-system-definition-update>

raison justement de ces fonctions cognitives et en raison des risques d'atteinte aux droits fondamentaux. De nombreux droits fondamentaux, comme le principe d'égalité et de non-discrimination ou encore la protection de la vie privée, pourraient être à risque dans le la mise en œuvre des systèmes d'IA. Cependant, si à l'inverse on voulait retenir une protection par les droits fondamentaux, même si lesdits droits sont protégés par des textes au sommet de la hiérarchie des normes, comme la *Charte des droits fondamentaux* de l'UE, une protection concrète est difficilement garantie. Il faudrait que ces droits soient repris par des lois d'un niveau inférieur et que la protection de ces droits se traduise par des obligations tangibles imposées aux parties prenantes, comme les acteurs fournissant les modèles et systèmes d'IA. Si je prends l'exemple du Canada, la *Charte canadienne des droits et libertés* ne concerne que les relations verticales, donc il ne va pas être possible de mettre en œuvre cette charte dans les relations entre acteurs privés. Il y a donc une limite systémique par rapport à la mise en œuvre des droits fondamentaux en tant que tels dans le contexte de cette technologie.

[5] Par ailleurs, si on avait choisi d'élaborer une législation en intégrant des droits pour les personnes, ce qu'on a fait par exemple pour les législations sur les renseignements personnels, cela voudrait dire qu'il faudrait attendre de mettre en œuvre des systèmes d'IA et de les déployer sur le marché pour savoir si un préjudice est subi et s'il faut accorder des droits pour pouvoir exercer des recours. Ce n'est pas très satisfaisant car cela implique que peu d'obligations s'imposeraient en amont pour éviter la survenance des préjudices. Cette solution est d'autant moins satisfaisante qu'il n'est pas toujours possible de réparer les préjudices. L'avantage de mettre en œuvre un modèle de conformité est d'agir avant la mise sur le marché de systèmes d'IA qui peuvent s'avérer dangereux. C'est exactement la logique de cette approche par les risques mise en œuvre en Europe et au Canada. Est ainsi consolidée la logique régulation-marché-innovation. Ces dispositions législatives apportent en outre la sécurité juridique nécessaire, permettant aux acteurs de connaître les règles avant de mettre un produit sur le marché.

[6] Cependant, l'approche par les risques au Canada et en Europe n'est pas identique, Malheureusement, au Canada, on s'est concentré sur l'IA à haut risque ou « à incidence élevée » sans que ne soit prévu un niveau de risque « inacceptable » comme l'a fait l'Union européenne et c'est très regrettable. C'est regrettable à plusieurs titres parce que d'abord, cette solution est moins protectrice pour les individus. Cela veut dire aussi que le Canada rate une occasion de dire quels sont les valeurs et principes à défendre pour justifier d'interdire certains usages de l'IA dans certains contextes. Même si les technologies évoluent et qu'on ne veut pas fixer les choses de manière trop définitives, il y a des choses qui socialement ne sont pas acceptables. Par exemple, dans l'UE, on avait prévu quatre systèmes d'IA inacceptables dans des situations précises dans le projet de règlement (la notation sociale, la reconnaissance faciale en temps réel par les forces de l'ordre, la manipulation subliminale en sont des exemples). Au cours des négociations du texte, quatre autres cas ont été ajoutés, soit huit interdictions d'utilisation de l'IA. En face, la Canada en a aucune et c'est regrettable.

[7] Quant à l'approche par les risques en tant que tels, le projet de loi C-27 publié en juin 2022, prévoyait simplement que les responsables et les opérateurs devaient évaluer les risques : les risques de préjudice et les risques de résultats biaisés des

systèmes d'IA. Les risques de préjudices sont définis dans la loi de manière très proche du droit de la responsabilité civile classique contractuelle ou extracontractuelle. Tous les préjudices moraux, économiques ainsi que les pertes de chance sont visés. Quant aux résultats biaisés, ils sont renvoyés à la loi canadienne sur les droits fondamentaux, sur les droits humains. Finalement, cela laisse un certain flou. On prévoyait aussi des obligations à la charge des opérateurs, c'est-à-dire les concepteurs, les utilisateurs, les fournisseurs de systèmes, toute la chaîne de l'IA. On exigeait de leur part une évaluation des risques (sur la base des risques de préjudice ou de biais) et on exigeait une minimisation de ces risques, ainsi que la mise en œuvre de mesures de contrôle de ces mesures de minimisation. Cela correspond à trois catégories d'obligations.

[8] Les critiques importantes formulées contre le texte ont conduit à clarifier ce que peut-être un système d'IA à « incidence élevée », une approche par les risques. Finalement, le Ministre Champagne, lors de son audition au Comité INDU, a ajouté une classification des risques avec sept cas qui ressemblent énormément au droit européen, mais avec des formulations différentes. On retrouve l'idée de l'utilisation de système d'IA dans le domaine de l'emploi et du recrutement, dans le cas des données biométriques pour l'identification et l'évaluation de comportement, dans le cadre de la santé, mais uniquement dans les hypothèses de triages des patients et non dans les dispositifs médicaux, dans la fourniture de services, que ce soient des services publics ou privés, dans la prise de décisions dans le domaine pénal et dans la prise de décision par un tribunal ou un organisme administratif. Il y a un septième cas qui concerne la création des contenus qui est quand même un petit peu à part, puisqu'il porte sur la modération des contenus régulée en droit de l'Union européenne par le règlement Digital Services Act (DSA). Grâce à cette classification, on sait dans quel domaine on peut avoir des systèmes à incidence élevée. Dans ces domaines, les opérateurs sont tenus d'évaluer les risques, de les minimiser et de prendre des mesures de contrôle. Ils doivent aussi conserver des preuves de cette minimisation et des mesures mises en œuvre et de faire preuve d'un certain nombre de mesures de transparence pour informer le public de l'utilisation des systèmes d'IA. Et si ces dispositions ne sont pas respectées, des sanctions pénales vont être adoptées. Évidemment, les sanctions pénales peuvent paraître un peu excessives et disproportionnées par nature, mais le choix des sanctions pénales se justifie par les règles de partage de compétences entre le fédéral et les provinces, donc les sanctions criminelles sont très certainement liées à ces contraintes de partage de compétence, en vertu de l'article 91 de la Constitution. Il en est de même du champ d'application du texte lui-même qui concerne les échanges et le commerce international et interprovincial, ce qui relève également de la compétence fédérale. Mais là, il va falloir réfléchir entre le fédéral et les provinces. L'IA est partout, il va donc falloir que les différents paliers de gouvernements travaillent ensemble.

[9] Je voudrais ajouter deux choses : dans les amendements, on a ajouté une prise en considération des modèles d'IA à usage général, suivant un même phénomène qu'en Europe avec Chat GPT. Il faut tenir compte de ces modèles qui ne se définissent pas par l'usage. On vise aussi le respect de la loi par l'instauration d'un commissaire à l'IA et aux données qui n'a malheureusement pas beaucoup de pouvoir. Par amendements, on ajoute des pouvoirs qui ressemblent à ceux du Commissariat à la protection de la vie privée. Il y a trois jours, le budget fédéral a indiqué quel montant d'argent il voulait

donner à ce commissaire, soit 5 millions de dollars pour l'année 2024-2025, ce qui n'est pas énorme. Ce que nous apprenons aussi dans ce budget fédéral est l'investissement du budget fédéral, soit 50 millions de dollars pour 5 ans, 10 millions par an pour de nouvelles institutions, ce qui n'est pas énorme non plus.

[10] L'effet Bruxelles est quand même limité en raison des questions de compétences différentes dans un contexte fédéral et des partenaires avec lesquels on veut s'aligner. À l'évidence, les Américains font partie du jeu et ont une approche différente de celle de l'Europe, notamment à travers l'*Executive Order* du président Biden, qui privilégie une approche axée sur la sécurité, notamment la sécurité nationale contre les attaques par l'IA.

RÉFÉRENCES BIBLIOGRAPHIQUES (SS TITRE DU TEXTE)

Anu BRADFORD*, The Brussels Effect : How the European Union Rules the World*, Oxford University Press, 2020, 404 p. L'"effet Bruxelles" se réfère à l'habileté unilatérale de l'Union européenne à réguler le marché global.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), *AI Risk Management Framework*, janvier 2023, en ligne : <https://www.nist.gov/itl/ai-risk-management-framework>.