INSTITUT D'ÉTUDES INTERNATIONALES DE MONTRÉAL
UQÀM
WWW.IEIM.UQAM.CA

LES DONNÉES À CARACTÈRE PERSONNEL À L'ÈRE DE L'IA GÉNÉRATIVE : ENTRE ALLIANCES TECHNOLOGIQUES ET RÉSISTANCES RÉGLEMENTAIRES

Regards de l'IEIM par Michael Bilukidi| novembre 2025

Introduction

On le sait, lorsqu'un utilisateur explore Internet, il laisse derrière lui des empreintes. Ces traces peuvent être des informations qu'il partage de ses achats en ligne ou encore de son consentement au stockage de témoins (*cookies*) sur son appareil[1]. Mais cette question devient plus préoccupante lorsqu'il s'agit des interactions avec l'intelligence artificielle (IA) générative, au moyen d'outils aussi sophistiqués que sont les robots conversationnels.

« Cet essai examine de quelle manière l'intelligence artificielle générative redéfinit l'économie des données personnelles grâce à des partenariats technologiques et étatiques, ainsi qu'à une collecte massive, tout en soulignant les menaces pour la confidentialité et la propriété intellectuelle. »

En demandant à ChatGPT, par exemple, de résumer ses notes, l'utilisateur ignore souvent qu'il contribue involontairement à redessiner les rapports de force géopolitiques. Ces simples interactions, multipliées par des millions d'utilisateurs à travers le monde, alimentent une bataille silencieuse, mais décisive pour le contrôle des données personnelles[2]. Dans ce contexte, les entreprises technologiques nouent des alliances pour dominer ce marché émergent; les régulateurs, eux, tentent d'imposer des garde-fous. Se dessine alors une tension entre l'impératif d'innovation et l'exigence de protection des droits fondamentaux.

Dès lors, comment la bataille pour nos données personnelles révèle-t-elle les nouvelles alliances et résistances dans un monde en recomposition ? En analysant les politiques de confidentialité des géants technologiques et les cadres réglementaires existants, nous explorerons dans quelle mesure nos données sont exploitées lorsque nous utilisons ces

[1] Lire Radio-Canada, « Les navigateurs de TikTok, Instagram et Facebook vous traquent plus que vous le croyez » (19 août 2022), en ligne : <https://urlr.me/2DMNnu>.
[2] Kathleen Desveaud, « Chapitre 3. Une course à l'IA vers un oubli de la morale ? » dans *L'intelligence artificielle décryptée. Comprendre les enjeux et risques éthiques de l'IA pour mieux l'appréhender*, Caen, EMS Éditions, 2024.

modèles et analyserons comment ces outils redessinent les équilibres de pouvoir mondiaux, entre coopération nécessaire et affirmation de souveraineté.

1. Alliances technologiques : quand les géants à la course aux données s'allient

Avant d'aborder les alliances qui se tissent autour du partage des données et le rôle d'appui que leur accordent les pouvoirs publics, il importe d'examiner d'abord la manière dont les entreprises façonnent un régime de captation des données personnelles sous couvert de leurs politiques de confidentialité

1.1 Les données personnelles, carburant de l'IA générative

Comment savoir à quoi vos données, quand elles sont utilisées pour entraîner des modèles IA, peuvent servir ? À repérer des chats dans des vidéos YouTube ? À nourrir les algorithmes de l'armée américaine ? À faciliter l'oppression de la minorité ouïghoure en Chine ? Impossible de le savoir, mais le sujet devient de plus en plus sensible[3].

Avant de s'offrir des services IA, les fournisseurs réclament aux futurs utilisateurs d'accepter des conditions d'utilisation qui sont très longues et difficiles à lire. Et dans ces conditions bien souvent, le concepteur demande à ces derniers de partager leurs données personnelles. Dans la dernière version des conditions d'utilisation d'OpenAI, maison mère de ChatGPT, en date du 11 décembre 2024, on peut notamment lire ceci à propos de sa politique de confidentialité :

« *Nous recueillons des renseignements personnels à votre sujet comme suit :*

1. ***Les Renseignements personnels que vous fournissez***

- *Renseignements sur le compte : Lorsque vous créez un compte auprès de nous, (…) y compris votre nom, vos coordonnées, les identifiants de votre compte, votre date de naissance, vos informations de paiement et l'historique de vos transactions (…)*
- *Contenu sur l'utilisateur : Nous recueillons les Renseignements personnels saisis dans les données d'entrée que vous soumettez à nos Services, y compris vos requêtes et d'autres contenus que vous téléversez, comme des fichiers, des images, et de l'audio (…)*

2. ***Notre utilisation des Renseignements personnels* (*…)***

- *Pour fournir, analyser et entretenir nos Services (…)*
- *Pour améliorer et développer nos Services et mener des recherches, par exemple pour développer de nouvelles fonctionnalités produit (…)*

[3] Remy Demichelis, « Le mariage explosif de nos données et de l'IA » (2019), Les Echos, en ligne: <https://urlr.me/RrhGap>.

3. Divulgation des Renseignements personnels

- *Afin de répondre à nos besoins opérationnels et d'offrir divers services et fonctionnalités, nous pouvons divulguer des Renseignements personnels à des prestataires et fournisseurs de services (…) ».*[4]

Pour être précis, dans une note publiée sur son site, ce géant de la tech clarifie sa politique en ces termes : « *Les modèles de fondation d'OpenAI, y compris les modèles qui alimentent ChatGPT, sont développés en utilisant trois sources de renseignements principales : (1) les renseignements accessibles au public sur Internet, (2) les renseignements auxquels nous avons accès dans le cadre de partenariats avec des tiers, et (3) les renseignements fournis ou générés par nos utilisateurs ou nos formateurs et chercheurs humains. »*[5]. Et d'en ajouter dans une autre note : « *Lorsque vous partagez votre contenu avec nous, vous aidez nos modèles à devenir plus précis et meilleurs pour résoudre vos problèmes spécifiques, tout en améliorant leurs capacités générales et leur sécurité (…) Par exemple, ChatGPT s'améliore grâce à un entraînement poussé sur les conversations que les gens ont avec lui, sauf dans l'hypothèse où vous choisissez de vous en retirer* ».[6]

L'entreprise précise en outre que « *dans certaines circonstances, [elle peut] fournir vos informations personnelles à des tiers sans préavis, sauf si la loi l'exige* ». C'est presque la même politique que celle de *Perplexity IA* du 04 juin 2024 qui va plus loin en précisant que « *si vous choisissez de synchroniser votre compte Google ou Gmail avec nos Services, nous aurons accès à vos contacts, e-mails et calendriers ».*[7]

En milieu universitaire, où l'originalité et la contribution à la connaissance constituent des exigences fondamentales de tout travail de recherche, le recours à l'IA soulève bien de risques : en confiant à ces outils des extraits de sa recherche dans un but de correction, de reformulation ou de synthèse, ce que l'IA mémorise d'emblée et de surcroît, l'utilisateur s'expose à la divulgation anticipée de ses travaux ou à sa réutilisation, avant même la soutenance ou la publication officielle.

En entreprise, que se passe-t-il si un employé saisit des notes d'une réunion et demande à ChatGPT de les corriger ? ChatGPT obtient des informations confidentielles sur cette entreprise, ses produits ou ses clients. Dans une étude publiée en février 2023, l'entreprise de cybersécurité Cyberhaven observe que 2,3 % des travailleurs qui utilisent

---

[4] OpenAI, « Politique de Confidentialité » (11 décembre 2024), en ligne: <https://urlr.me/jRta2r>

[5] OpenAI, « Comment ChatGPT et nos modèles de fondation sont développés - OpenAI Help Center », en ligne: <https://urlr.me/aRzWYx>

[6] OpenAI, « Comment vos renseignements sont utilisés pour améliorer la performance des modèles - OpenAI Help Center », en ligne: <https://urlr.me/keP8pC>

[7] PerplexityAI, « Terms of Service » (4 juin 2024), en ligne: <https://www.perplexity.ai/fr/hub/legal/terms-of-service>

ChatGPT y partagent des informations confidentielles[8]. C'est ainsi que de nombreuses entreprises, y compris des banques, des hôpitaux et des géants du numérique tels qu'Apple, Samsung et Amazon, ont pour leur part interdit à leurs équipes d'utiliser les outils d'IA générative.

Cette situation a poussé OpenAI à revoir sa politique dans la version payante de ChatGPT, où les utilisateurs peuvent modifier les paramètres pour que leurs conversations ne soient pas utilisées dans l'entraînement des futurs modèles d'intelligence artificielle de *OpenAI*. Malgré cette possibilité, des erreurs peuvent toujours survenir, et aucune entreprise n'est à l'abri d'une fuite informatique ou anomalie technique. D'ailleurs, plusieurs incidents montrent que des systèmes d'IA ont déjà, involontairement, divulgué des informations sensibles[9].

Par ailleurs, la vie privée n'est pas le seul enjeu à prendre en compte dans ce contexte. Il y a également des défis importants concernant la propriété intellectuelle qu'il faut considérer. En effet, sur Internet les utilisateurs mettent également en ligne des productions protégées par les droits d'auteurs et qui peuvent être récupérées par des algorithmes qui vont s'entraîner dessus[10]. C'est exactement ce qu'a fait Microsoft avec son IA *GitHub Copilot* qui, pour atteindre sa redoutable performance, a puisé dans l'intégralité du contenu public de *GitHub*, une plateforme rachetée par l'entreprise, et qui permet aux développeurs d'héberger publiquement leur code informatique. Leur *IA Copilot* s'est ainsi entraînée sur tout ce contenu hébergé sur *GitHub*, et cela sans tenir compte des licences et des *copyrights*[11]. Ainsi, à leur insu, des développeurs peuvent voir leur nom apparaître ou d'autres informations sous *copyright* lorsque *Copilot* propose et complète du code de manière autonome.

Un développeur a par ailleurs signalé sur le réseau social X (Twitter) en 2022 avoir constaté que *Copilot* suggérait du code informatique issu de son propre projet sous *copyright*[12].

1.2 Alliances public-privé et reconfiguration du pouvoir dans l'économie des données

L'exemple du partenariat Microsoft-OpenAI illustre bien cette situation : après avoir injecté 13 milliards de dollars depuis 2019, Microsoft a récemment négocié une

---

[8] Cyberhaven, « 11% of data employees paste into ChatGPT is confidential », (28 février 2023), en ligne : <https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt>

[9] Nicholas Carlini et al, *Extracting Training Data from Large Language Models*, USENIX Association, 2021, p. 2633

[10] Amanda Levendowski, « How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem » (2018), 93:2 *Washington Law Review*.

[11] Kathleen Desveaud, « Chapitre 4. Des remises en question sociétales importantes » dans *L'intelligence artificielle décryptée Comprendre les enjeux et risques éthiques de l'IA pour mieux l'appréhender*, Caen, EMS Éditions, 2024, 161.

[12] *Ibid*, Tim Davis sur X https://x.com/DocSparse/status/1581461734665367554?s=20

participation de 30% dans la future structure d'OpenAI, désormais valorisée à 500 milliards de dollars.

L'objectif est, estimons-nous, de comprendre, d'anticiper et d'orienter les comportements individuels et collectifs : habitudes de consommation, opinions politiques, émotions, choix culturels, voire décisions électorales, en vue d'instaurer une dépendance. Ainsi, la donnée n'est plus seulement un moyen : elle devient une ressource financiarisée, un actif stratégique qui attire les investisseurs, alimente les valorisations boursières et légitime des levées de fonds massives.

« S'alignant dans une course mondiale aux données, les géants du numérique et les autres acteurs spécialisés multiplient les alliances capitalistiques et technologiques afin de partager les coûts très élevés liés au développement des modèles d'IA et de mutualiser les ressources (données, infrastructures, ingénieurs, brevets). »

Cependant, au-delà des acteurs privés, cette dynamique s'accompagne d'un soutien étatique massif. Le projet « *Stargate* » annoncé par Donald Trump en janvier 2025 avec 500 milliards de dollars d'investissements publics privés sur quatre ans, en est l'exemple parfait.

La Chine, face à cette offensive américaine (61% du financement mondial des start-ups IA), a répondu par d'énormes investissements (environ 17% du financement mondial) tandis que l'Europe, avec seulement 6% investis, est accusé d'un grand retard selon Mario Draghi, ancien président de la Banque centrale européenne et ancien premier ministre italien, qui alerte : « *l'Europe [...] est en recul* »[13]. Une telle configuration appelle dès lors à analyser comment les tentatives de régulation se heurtent aux réalités d'un écosystème désormais caractérisé par des alliances technoétatiques qui dépassent les cadres juridiques traditionnels.

2. Résistances réglementaires et limites du droit

2.1 Le RGPD européen

L'Europe a mis en place un cadre « robuste » pour assurer la protection des données personnelles de ses citoyens. Il s'agit du Règlement général sur la protection des données (RGPD), pionnier du genre dans le monde, entré en vigueur le 25 mai 2018. Cette

[13] Lire Mario Draghi, *L'avenir de la compétitivité européenne Partie A | Une stratégie de compétitivité pour l'Europe*, commission européenne éd, Luxembourg, 2024, p 15.

législation constitue une résistance importante face aux alliances d'extraction massive de données personnelles orchestrées par les géants technologiques.

Mais sept ans après son entrée en vigueur, le bilan reste partagé entre actions répressives et initiatives de contournement. L'année 2024 marque un record d'amendes prononcées à travers l'Europe avec 1,2 milliard d'euros, portant le montant total cumulé à 5,88 milliards d'euros depuis 2018[14]. En France, la CNIL confirme cette tendance avec 87 sanctions (contre 42 en 2023) et 55,2 millions d'euros d'amendes[15]. Et les entreprises américaines concentrent 80% du montant total des amendes prononcées, avec des sanctions record : Amazon à hauteur de 746 millions d'euros, Meta cumulant 2,7 milliards d'euros dont 1,2 milliard pour transferts illégaux de données vers les États-Unis et ce, au grand dam de Donald Trump, qui dénonce un « protectionnisme européen » et menace d'imposer des droits de douane contre les pays appliquant des réglementations « discriminatoires »[16].

Par ailleurs, certaines entreprises mettent sur pied des interfaces trompeuses, appelées « *dark patterns* », des pratiques d'interfaces numériques qui orientent, trompent, contraignent ou manipulent les consommateurs pour les amener à faire des choix qui ne sont souvent pas dans leur intérêt[17]. Ces techniques amènent souvent les utilisateurs à partager davantage de données personnelles qu'ils ne le souhaitent, contournant ainsi l'esprit du RGPD. Selon une étude de la Commission européenne de 2022, 97% des sites e-commerce et des applications les plus populaires au sein de l'Union contiennent des *dark patterns*[18].

Exemple de bannière cookie où la possibilité de « refuser » est entravée, requérant plus de clics et étant dissimulée dans le texte.

Source : DGCCRF/DITP, 2023

En outre, le RGPD se heurte également à des résistances géopolitiques, notamment avec le *NUAGE Act* américain, qui avec son

[14] Louise Costa, « Malgré les amendes, les autorités en charge du RGPD jugées trop timides », *Le Monde* (4 février 2025), en ligne : <https://urlr.me/JHmscP>
[15] Jeanne Breton et al, « Données personnelles », *La voix* (21 juillet 2025), en ligne : <https://urlr.me/UFBQfH>
[16] Vincent Lequeux, « Numérique : Donald Trump menace de sanctions les pays qui "discriminent" la tech américaine », *Toute l'Europe* (26 août 2025), en ligne : <https://urlr.me/3UZxW9>
[17] DGCCRF/DITP, *Lutter contre les pratiques commerciales déloyales en ligne - Rapport de diagnostic*, 2023 à la p 6.
[18] European Commision, *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation : final report*, Publications Office of the European Union, 2022

extraterritorialité entre en collision directe avec l'article 48 du RGPD, et crée une zone d'incertitude pour les entreprises européennes utilisant des services d'infonuagique (*cloud)* américains.

2.2 La Loi 25 québécoise

Avec l'omniprésence et la généralisation du *cloud*, l'extra-territorialité est devenue une préoccupation majeure pour les entreprises, les gouvernements et les individus. À ce titre, en septembre 2021 le gouvernement du Québec a adopté la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, aussi appelée la Loi 25.

Celle-ci « *modernise l'encadrement applicable à la protection des renseignements personnels dans diverses lois, dont la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels dans le secteur privé ».*[19] Une de ses caractéristiques notables est l'*Évaluation d'impact sur la vie privée*, un outil d'évaluation obligatoire que les organisations doivent utiliser lors du traitement des données personnelles de certaines manières et dans certains contextes. Une autre concerne les règles strictes relatives au transfert transfrontalier de données, exigeant que les données quittant le Québec soient protégées à un niveau équivalent à celui à l'intérieur de la province.

Cependant, comme nous l'avons abordé ci-haut, entraîner des modèles d'IA peut entraîner la mémorisation des données par le modèle, ce qui signifie que les informations personnelles contenues dans les données peuvent être divulguées de manière imprévisible. À ce sujet, la Loi 25, en son article 28 stipule :

> « *La personne concernée par les informations personnelles a le droit d'exiger de toute entité exerçant une activité commerciale de cesser la diffusion de ces informations ou de déréférencer tout lien hypertexte lié à son nom permettant l'accès à ces informations par des moyens technologiques, si la diffusion enfreint la loi ou une ordonnance judiciaire. »*

En d'autres termes, si un modèle d'IA divulgue des informations personnelles présentes dans ses données d'entraînement sans le consentement de l'individu, la présente disposition donne droit à la personne concernée d'introduire une requête auprès de la structure concernée pour demander le retrait ou la cessation de diffusion de ses informations. Dans la pratique, il est déjà difficile qu'une personne soit au courant que ses

[19] Notes explicatives de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021, c 25.

informations sont divulguées dans un autre contexte. Même si cela lui parvenait par chance, techniquement il est difficile, voire impossible, de procéder à un tel retrait ou modification :

> « *Mettre en œuvre les droits des personnes concernées sur leurs données est difficile. Les LLMs stockent les données qu'ils apprennent sous forme de milliards ou de trillions de paramètres, plutôt que dans une base de données traditionnelle. Pour cette raison, rectifier, supprimer ou même demander l'accès aux données personnelles apprises par ces modèles, qu'elles soient exactes ou issues d'hallucinations, peut s'avérer difficile, voire impossible* ».[20]

Dans un entretien accordé au quotidien *Le Devoir*, Anne-Sophie Hulin reste sceptique quant à ChatGPT de se conformer à la Loi 25 : « *On ne peut toutefois pas garantir que ChatGPT sera obligé de s'y conformer, puisque le critère de rattachement pour une entreprise étrangère à la loi 25 n'est pas si certain que ça* », prévenait-elle en 2023[21]. La loi qui encadre la politique de confidentialité de ChatGPT a été construite conformément au *California Privacy Rights Act,* soit la loi californienne qui assure une protection des renseignements personnels. Comparativement au RGPD et à législation québécoise, la législation californienne est un peu moins protectrice[22].

Par ailleurs, au niveau fédéral, une tentative ambitieuse de résistance réglementaire s'est soldée par un échec. Le projet de loi C-27, déposé en juin 2022 et incluant la *Loi sur l'intelligence artificielle et les données*, avait comme objet de « *renforcer la confiance des Canadiens envers les technologies numériques qu'ils utilisent au quotidien* ».[23] La prorogation du Parlement annoncée le 6 janvier 2025 a cependant sonné le glas de cette initiative qui, après plus de deux ans et demi de débats parlementaires, d'audiences en comité et de consultations, est « mort au feuilleton ».

Conclusion

Ce texte est écrit alors que se dessinent les contours du Pacte numérique mondial porté par les Nations Unies, dont l'ambition affichée est de construire un cadre global capable d'orienter la gouvernance du numérique vers la justice, la durabilité et le respect des droits fondamentaux. Ce projet, né d'un consensus international rare, se veut une réponse aux déséquilibres croissants provoqués par la concentration du pouvoir technologique.

---

[20] European Data Protection Supervisor, *TechSonar: 2023-2024 report*, Luxembourg, European Union, 2023, p 8

[21] Sandrine Vieira, « Les risques de trop en dire à ChatGPT », *Le Devoir* (30 mars 2023), en ligne : <https://www.ledevoir.com/societe/787321/que-fait-chatgpt-avec-nos-donnees-personnelles>

[22] *Ibid*.

[23] ISDE Canada, « La Loi sur l'intelligence artificielle et les données (LIAD) – document complémentaire », *ISDE Canada* (31 janvier 2025), en ligne : <https://urlr.me/zSw2tf>

Pourtant, ses limites apparaissent déjà : absence de mécanismes contraignants, dépendance aux bonnes volontés, influence des grandes plateformes dans la formulation même des principes. Ainsi, le Pacte risque de rejoindre la longue liste des textes symboliques qui, à défaut de coercition, peinent à transformer la réalité.

Pourtant, ce Pacte pourrait devenir un véritable levier de résistance s'il osait franchir le pas vers des mesures coercitives radicales et briser la logique de « partenariat » avec les géants technologiques pour retrouver une posture de régulation par la contrainte. Car ce n'est pas un hasard si, en 2023, plus de 30 000 personnalités — dont les « pères fondateurs » de l'IA moderne Yoshua Bengio et Geoffrey Hinton, aux côtés d'Elon Musk, Steve Wozniak et Yuval Noah Harari - ont signé une tribune appelant à un moratoire sur le développement incontrôlé de l'IA[24]. Leur alerte n'était pas celle d'esprits technophobes, mais d'observateurs rappelant que l'humanité s'est déjà montrée incapable de prévenir d'autres crises majeures (guerres incessantes, dérèglement climatique, pandémies, etc.) face auxquelles nous avons multiplié les déclarations, chartes et engagements volontaires — sans réelle prise sur le terrain.

« Nous devons affronter ce défi avant qu'il ne soit trop tard, avant que la créativité algorithmique ne façonne le monde à notre place, avant que la régulation n'arrive une fois de plus après la catastrophe. Peut-être faut-il, pour la première fois, agir avant de comprendre entièrement. »

Or, avec l'IA, le risque est d'une autre nature : la vitesse de création dépasse notre capacité d'encadrement, et la frontière entre l'humain et la machine devient chaque jour plus poreuse. Ce n'est plus simplement une question de gouvernance ou d'éthique, c'est une question de survie symbolique. Nous devons affronter ce défi avant qu'il ne soit trop tard, avant que la créativité algorithmique ne façonne le monde à notre place, avant que la régulation n'arrive une fois de plus après la catastrophe. Peut-être faut-il, pour la première fois, agir avant de comprendre entièrement. Car si l'intelligence artificielle nous dépasse déjà, serons-nous encore capables demain de reconnaître ce qui relève de notre propre humanité ?

[24] Future of Life Institute, « Pause Giant AI Experiments: An Open Letter » (2023).

BIBLIOGRAPHIE

———, « Chapitre 4. Des remises en question sociétales importantes » dans *L'intelligence artificielle décryptée Comprendre les enjeux et risques éthiques de l'IA pour mieux l'appréhender*, ems éditions éd, Caen, EMS Éditions, 2024. https://urlr.me/7e6gP8

———, « Comment vos renseignements sont utilisés pour améliorer la performance des modèles | OpenAI Help Center », en ligne: <https://urlr.me/FHc7eY>.

———, « Politique de Confidentialité » (11 décembre 2024), en ligne: <https://urlr.me/fAn6G2>.

Carlini, Nicholas et al, *Extracting Training Data from Large Language Models*, USENIX Association, 2021. https://urlr.me/9G2ra8

Desveaud, Kathleen, « Chapitre 3. Une course à l'IA vers un oubli de la morale ? » dans *L'intelligence artificielle décryptée Comprendre les enjeux et risques éthiques de l'IA pour mieux l'appréhender*, ems éditions. éd, Caen, EMS Éditions, 2024. https://urlr.me/7e6gP8

DGCCRF/DITP, *Lutter contre les pratiques commerciales déloyales en ligne - Rapport de diagnostic*, 2023. https://urlr.me/pVWT79

European Commision, *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation : final report*, Publications Office of the European Union, 2022. https://urlr.me/pNwjVW

European Data Protection Supervisor, *TechSonar: 2023-2024 report*, Rapport, Luxembourg, European Union, 2023. https://urlr.me/guk8Hx

Future of Life Institute, « Pause Giant AI Experiments: An Open Letter » (2023). https://urlr.me/aNswmF

Levendowski, Amanda, « How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem » (2018) 93:2 Washington Law Review. https://urlr.me/SEHTeZ

Mario Draghi, *L'avenir de la compétitivité européenne Partie A - Une stratégie de compétitivité pour l'Europe*, Commission européenne éd, Luxembourg, 2024. https://urlr.me/9zpDXU

OpenAI, « Comment ChatGPT et nos modèles de fondation sont développés - OpenAI Help Center », en ligne: <https://urlr.me/5e8yWU>.

PerplexityAI, « Terms of Service » (4 juin 2024), en ligne: <https://urlr.me/WdskPr>.

Vieira, Sandrine, « Les risques de trop en dire à ChatGPT », *Le Devoir* (30 mars 2023), en ligne : <https://www.ledevoir.com/societe/787321/que-fait-chatgpt-avec-nos-donnees-personnelles>.

Note : *Les sites IA (ChatGPT et Perplexity AI) ont été consultés uniquement dans l'objectif de cette recherche : prendre connaissances de leurs politiques de confidentialité et conditions d'utilisations, afin de comprendre la manière dont ces plateformes récupèrent et utilisent les données de leurs utilisateurs.*

Auteur

Michael Bilukidi est candidat au doctorat en droit à l'Université du Québec à Montréal (UQAM). Ses intérêts de recherche portent sur la responsabilité sociale des entreprises, ainsi que sur les enjeux émergents liés à l'utilisation responsable et à la régulation de l'intelligence artificielle. Il est impliqué dans le projet « IA générative en droit » au Département des sciences juridiques de l'UQAM.

Ce texte a été retenu dans le cadre de l'appel à propositions 2025-2026 de l'Institut d'études internationales de Montréal sur le thème des alliances et des résistances.

Institut d'études internationales de Montréal
Université du Québec à Montréal
400, rue Sainte-Catherine Est
Bureau A-1540, Pavillon Hubert-Aquin
Montréal (Québec) H2L 3C5
514 987-3667
ieim@uqam.ca
www.ieim.uqam.ca