



Désinformation, microciblage et IA : quel avenir pour les démocraties?

Mise en contexte

Alors que le Canada vient de vivre sa première élection fédérale à l'ère de l'IA, les questions sont nombreuses quant aux impacts concrets des nouvelles technologies sur le débat public et les processus démocratiques. Les premières analyses de la campagne électorale canadienne suggèrent que peu d'électeurs auraient été trompés par des contenus générés par l'IA¹. Néanmoins, quelques incidents survenus durant cette campagne appellent à un examen de la transformation du politique par le numérique.

En contexte électoral, la dégradation de la qualité de l'information en ligne et la polarisation politique amplifiée par les algorithmes sont deux menaces parfois invisibles, mais bien réelles. Ces risques associés au numérique s'ajoutent aux enjeux politiques de cybersécurité les plus courants. Les techniques utilisées par les partis politiques pour gagner des appuis sont aussi en pleine transformation, soulevant leur lot de défis respectifs.

Les préoccupations envers la santé démocratique des États face à la place croissante que prend l'IA dans nos sociétés ne sont toutefois pas sans solution. Une [lettre ouverte](#) cosignée par Lyse Langlois, directrice générale de l'Obvia, propose d'ailleurs des actions que les gouvernements et les partis politiques devraient mettre en œuvre pour se doter de remparts solides contre les effets négatifs de l'IA sur la démocratie.

Cette note de breffage fait état des principaux enjeux liés à l'IA et au numérique pour les démocraties, particulièrement en contexte électoral, et présente des recommandations aux législateurs et aux stratèges politiques pour assurer une coexistence durable entre l'IA et un débat politique sain et inclusif.

Définitions

Désinformation : La désinformation est une information fautive ou inexacte dont la diffusion vise à nuire ou manipuler l'opinion publique. Elle peut toucher des contextes variés, tels que les changements climatiques, la santé, l'économie, les relations internationales, etc.²

Mésinformation : La mésinformation est une information fautive ou inexacte. Contrairement à la désinformation, la personne qui partage une mésinformation ne le fait pas de manière malveillante : elle n'a pas l'intention de nuire ou de tromper les autres.³



Dans un sondage d'Abacus Data réalisé en juillet 2024, plus de **70 %** de la population canadienne s'est dite très préoccupée par la question de la désinformation en ligne à cause de sa possible influence sur le débat politique⁴.

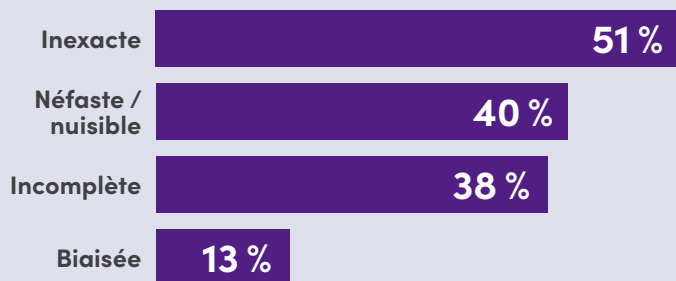
1 De Rosa, N. (2025, 6 mai). Désinformation électorale : impact limité de l'IA générative au Canada. Radio-Canada. <https://ici.radio-canada.ca/nouvelle/2162445/intelligence-artificielle-election-canada-2025>
2 Obvia. (2025). Glossaire de l'Obvia. <https://www.obvia.ca/ressources/glossaire/>
3 Ibid.
4 Poisson, M. (2024, 29 juillet). L'UdeM utilisera l'intelligence artificielle pour repérer les fausses nouvelles en ligne. Le Devoir. <https://www.ledevoir.com/societe/817282/udem-utilisera-intelligence-artificielle-reperer-fausses-nouvelles-ligne>

Résumé des connaissances

Un cyberspace de moins en moins fiable?

Désinformation, fausses nouvelles, hypertrucages : pour plusieurs, il est de plus en plus difficile de distinguer le vrai du faux sur l'Internet et les médias sociaux. Cette impression est partagée par les experts sondés dans l'édition 2025 du [Global Risks Report](#), qui ont classé pour la deuxième année consécutive la **désinformation et la mésinformation** au premier rang des risques mondiaux à court terme⁵. Le volume phénoménal de contenu généré par l'IA contribue à la propagation de fausses informations de deux manières principales : premièrement, en raison des possibles hallucinations ou confabulations des systèmes d'IA, c'est-à-dire lorsque le système génère une réponse fictive et la présente de manière convaincante⁶, et deuxièmement, en répétant de fausses informations trouvées dans le cyberspace. Il est important de rappeler qu'aussi sophistiqués qu'ils puissent paraître, les agents conversationnels comme ChatGPT, Grok ou Meta AI n'ont pas de « pensée critique » et ne sont pas entraînés pour être capables de détecter les fausses informations. Une étude a d'ailleurs trouvé que la moitié des réponses de ces outils sur des questions politiques étaient inexactes :

Évaluation de 130 réponses d'agents conversationnels sur des questions électorales⁷



Cette vulnérabilité des agents conversationnels populaires est exploitée par des acteurs malveillants cherchant à propager de fausses informations, notamment à des fins politiques. Un rapport de mars 2025⁸ a dévoilé « l'infection » des agents conversationnels les plus utilisés en Occident par un réseau de propagande russe, qui a mis sur pied des centaines de sites Web partageant de fausses nouvelles, et ce dans plus de 46 langues. Or, ces sites sont très peu fréquentés par les humains : leur but est de contaminer les modèles d'IA avec de fausses informations en inondant le

cyberspace, au rythme de 3,6 millions de faux articles en 2024. **L'enquête a révélé que les 10 agents conversationnels les plus utilisés dans les pays occidentaux répètent les fausses informations provenant du réseau russe 33 % du temps.**

La campagne électorale canadienne n'a pas été exempte d'incidents de désinformation amplifiée par l'IA. À la fin mars, une rumeur selon laquelle la fortune personnelle du candidat conservateur Pierre Poilievre aurait été de plus de 20 millions de dollars, une information qui a été démentie, a considérablement circulé sur les réseaux sociaux numériques. Comme l'a révélé l'émission *Les Décrypteurs*⁹, ces chiffres étaient issus du site Web Pierre Poilievre News, qui diffuse des articles générés par l'IA comprenant une panoplie d'informations non validées. Ce site, dont presque personne n'avait entendu parler jusqu'alors, a réussi à rendre virale cette fausse information puisqu'elle a été reprise par d'autres sites utilisant l'IA générative pour partager des nouvelles et par des agents conversationnels populaires, qui citent Pierre Poilievre News comme source. Ainsi, ces systèmes d'IA se retrouvent dans une boucle de rétroaction en reprenant et en rediffusant des informations initialement générées par l'IA, sans processus de vérification, pouvant entraîner des répercussions politiques bien réelles.

La vérification des faits mise à mal

La libre circulation des fausses informations en ligne est exacerbée par la perte de confiance envers les médias traditionnels et les vérificateurs de faits. Le rapport [Freedom on the Net 2024](#) a recensé de nombreux exemples à l'échelle mondiale où des organisations indépendantes vouées à la vérification des faits ont elles-mêmes fait l'objet de campagnes de désinformation visant à les délégitimer, souvent instiguées par des partis politiques et des gouvernements¹⁰. Ce rapport classe le Canada au 3^e rang des 72 pays étudiés en matière de liberté de l'Internet, décelant peu d'obstacles à l'accessibilité, de limitations au contenu ou de violations des droits des usagers. Malgré cette donnée encourageante, le pays n'est pas à l'abri des attaques envers les vérificateurs de faits, comme ce fut le cas pour une [journaliste de CTV News](#) durant la campagne électorale.

5 World Economic Forum (2025). *The Global Risks Report 2025: 20th Edition, Insight Report*. <https://www.weforum.org/publications/global-risks-report-2025/>

6 Obvia. (2025). *op. cit.*

7 Angwin, J., Nelson, A. & Palta, R. (2024). Seeking Reliable Election Information? Don't Trust AI. *Proof*. <https://www.proofnews.org/seeking-election-information-dont-trust-ai/>

8 Sadeghi, M. & Blachez, I. (2025). *The Infection of Western AI Chatbots by a Russian Propaganda Network*. NewsGuard. <https://www.newsguardtech.com/wp-content/uploads/2025/03/March2025PravdaAIMisinformationMonitor.pdf>

9 Yates, J. (2025, 29 mars). Comment la désinformation générée par IA a déjà infecté l'élection fédérale. *Radio-Canada*. <https://ici.radio-canada.ca/nouvelle/2151457/fortune-investissements-ia-carney-poilievre-désinformation>

10 Freedom House (2024). *Freedom on the Net 2024: The Struggle for Trust Online*. <https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online>, p.12

Que ce soit par méfiance envers les médias traditionnels ou par désintérêt, les réseaux sociaux sont une source importante de nouvelles pour bien des Canadiens. Or, depuis 2023, les médias traditionnels sont bannis de toutes les plateformes Meta¹¹, comme Facebook, Instagram et Threads, toujours populaires au pays. L'intégrité de l'information sur ces plateformes a connu un recul encore plus important dans les derniers mois avec la fin de la vérification des faits par des tierces parties, suivant maintenant l'approche de X avec des vérifications « par la communauté »¹². Cette décision est justifiée par Mark Zuckerberg sur la base d'une plus grande liberté d'expression en ligne et des « biais politiques » allégués des vérificateurs de tierces parties, dans la foulée de son rapprochement avec le gouvernement fédéral américain.

« Plusieurs compagnies de médias sociaux ont licencié les équipes dédiées à améliorer la confiance, la sécurité et les droits humains en ligne »¹³ – Freedom House

En l'absence d'une vérification des faits indépendante et crédible, les médias sociaux deviennent un terrain de jeu en période électorale pour des acteurs cherchant à influencer les électeurs avec de fausses informations et pour l'ingérence étrangère, souvent à l'aide de robots informatiques (bots). Récemment, des élections présidentielles en Roumanie ont dû être annulées puis reprises après que la Russie ait mené une campagne d'influence massive et néfaste sur TikTok¹⁴. « Ces robots [bots] sont utilisés par une multitude d'acteurs, souvent pour amplifier et manipuler des récits partisans, ou pour répandre des rumeurs ou de fausses nouvelles avec notamment l'objectif d'attaquer ou de soutenir des politiciens pour influencer l'opinion publique. »¹⁵

La polarisation politique et les algorithmes, un mélange explosif

Le Global Risks Report 2025 souligne l'interrelation entre la désinformation et la mésinformation et la polarisation sociale et politique¹⁶. La polarisation du discours tend à déformer la vérité, ce qui donne de l'impulsion à la circulation de fausses informations. Pour maximiser l'engagement de leurs utilisateurs, les médias sociaux utilisent **des algorithmes qui favorisent le partage de contenus extrémistes : plus le contenu fait réagir les utilisateurs, plus il est valorisé par l'algorithme**¹⁷. Ce sont également les algorithmes qui contribuent aux « chambres d'écho » en

ligne, en proposant aux utilisateurs du contenu susceptible de leur plaire et provenant d'individus avec des points de vue similaires.

« Le concept de chambre d'écho fait référence à un espace virtuel où peuvent pénétrer seulement des informations et des opinions qui correspondent à celles de l'utilisateur ou d'un groupe. »¹⁸

Non seulement ces « bulles » informationnelles en ligne limitent l'exposition à des opinions variées, mais elles constituent aussi un terrain fertile pour les théories du complot et la mobilisation politique, parfois violente, de leurs adhérents. Avant leur pardon présidentiel en 2025, trois émeutiers de l'assaut du Capitole à Washington le 6 janvier 2021 rejetaient la faute sur la mésinformation et les théories du complot en ligne comme défense en cour¹⁹.

Transformation de la participation politique

Depuis de nombreuses années, le numérique transforme l'action politique et les manières dont les partis tentent de gagner des votes. L'arrivée de l'IA accélère cette transition vers des techniques plus sophistiquées et reposant moins sur l'appui de militants sur le terrain. Des activités traditionnelles comme le porte-à-porte sont graduellement remplacées par du microciblage publicitaire en ligne :

« Les traces numériques des internautes constituent des informations précieuses pour les stratèges des partis. Ces données granulaires permettent des opérations de segmentation et de microciblage afin de déterminer quel message (quoi) devrait être communiqué à quels électeurs (qui). »²⁰

Cette technique soulève plusieurs préoccupations éthiques, notamment parce que les électeurs ne sont pas exposés de manière égale à tous les messages politiques, mais aussi parce que leurs préférences politiques peuvent être inférées à partir de leur activité en ligne, à leur insu. Même si les réseaux sociaux numériques obligent leurs utilisateurs à accepter des conditions d'utilisation, l'usage réel des données personnelles peut être difficile à saisir pour l'utilisateur moyen. Comme le soulève une recherche récente auprès des partis politiques québécois, « la tendance à la professionnalisation et au recours accru "aux spécialistes en intelligence artificielle et de lecture du big data" n'est pas près de disparaître »²¹.

11 En raison du litige autour de la loi C-18

12 McMahon, L., Kleinman, Z. & Subramanian, C. (2025, 7 janvier). Facebook and Instagram get rid of fact checkers. *BBC News*. <https://www.bbc.com/news/articles/cly74mpy8klo>

13 Freedom House (2024). *op. cit.*, p. 6 [traduction libre]

14 Radio-Canada (2025, 25 janvier). *Ingérence électorale en Roumanie, quels risques pour le Canada ?* <https://ici.radio-canada.ca/decrypteurs/site/episodes/999776/>

15 Thibault, S. (2024). La désinformation en ligne. Dans Lalancette, M., Bastien, F., Greffet, F., & Giasson, T., *Médiatisation de la politique : logiques et pratiques*.

Presses de l'Université du Québec, p.228

16 World Economic Forum (2025). *op. cit.*, p. 35

17 Dufresne, Y., Dumouchel, D. & Ouellet, C. (2024). Des opinions publiques? Dans Lalancette, M., Bastien, F., Greffet, F., & Giasson, T., *Médiatisation de la politique : logiques et pratiques*.

Presses de l'Université du Québec, p.279

18 Durand, F., Gramaccia, J., Thiboutot, J., Brin, C. & Naffi, N. (2021). *Portrait d'une infodémie: Retour sur la première vague de COVID-19*. Obvia. <https://doi.org/10.61737/UQAN6464>

19 *Ibid.*, p.302

20 Dufresne, Y., Dumouchel, D. & Ouellet, C. (2024). *op. cit.*, p.275

21 Montigny, M. (2024). L'organisation électorale et la transformation interne des partis à l'ère numérique. Dans Lalancette, M., Bastien, F., Greffet, F., & Giasson, T.,

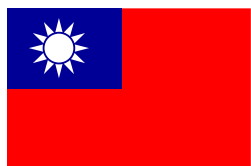
Médiatisation de la politique : logiques et pratiques. Presses de l'Université du Québec, p.33

Des garde-fous possibles

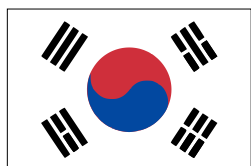
Les risques de l'IA envers la démocratie énumérés dans cette note peuvent être atténués avec des mesures ciblées. Plusieurs pays ont d'ailleurs commencé à légiférer sur l'utilisation des technologies comme l'IA en période électorale ou soutiennent des initiatives visant à contrer la désinformation²² :



En amont des élections de mai 2024, la Commission électorale d'Afrique du Sud (IEC) et le groupe de la société civile Media Monitoring Africa (MMA) ont mis sur pied un portail permettant au public de signaler des cas de fausses informations, de harcèlement, de discours haineux et d'incitation à la violence. Des cas évalués par un comité d'experts pouvaient ensuite être soumis au tribunal électoral du pays.



La plateforme de vérification des faits Cofacts, propulsée par la société civile taïwanaise, a permis de renforcer la confiance des citoyens envers les informations en ligne dans l'ensemble du spectre politique et parmi les diverses circonscriptions durant l'élection présidentielle de janvier 2024.



En Corée du Sud, les législateurs ont interdit l'utilisation d'hypertrucages dans les communications politiques à partir de 90 jours avant le scrutin, les contrevenants s'exposant à des peines pouvant aller jusqu'à sept ans de prison ou à des amendes de 50 millions de wons (48 000 CAD). La loi exige également l'étiquetage de tous les contenus politiques générés par l'IA.

Rôles que peuvent jouer les acteurs publics

Partis politiques :

- 1 Adopter des codes de conduite en matière d'IA en période électorale, notamment en s'engageant à ne pas utiliser l'IA de manière dénigrante ou pour diffuser de fausses informations²³;
- 2 Faire preuve d'une transparence accrue envers l'utilisation du microciblage politique en ligne et l'exploitation de « l'empreinte numérique » des citoyens à des fins partisans;

Gouvernements :

- 3 Renforcer les dispositions des lois électorales face à l'utilisation de l'IA et des hypertrucages en période électorale, par exemple en interdisant l'utilisation, la publication et la propagation de contenus trompeurs à l'aide de l'IA²⁴;
- 4 Soutenir et faire la promotion des initiatives d'éducation au numérique pour mieux outiller la population à reconnaître les hypertrucages et les fausses nouvelles en ligne;
- 5 Renforcer les enseignements relatifs au développement de l'esprit critique dans les cursus scolaires, surtout par rapport aux contenus en ligne;
- 6 Appuyer les initiatives de la société civile visant à contrer la désinformation et la mésinformation en ligne et faire la promotion de ces outils, particulièrement en période électorale;
- 7 Encourager les citoyens à consulter des sources de nouvelles fiables et à favoriser les réseaux sociaux proposant une vérification des faits indépendante.

22 Freedom House (2024). *op.cit.*

23 Régis, C. & Martin-Bariteau, F. (2025, 1^{er} avril). *Il faut agir pour protéger nos démocraties*. La Presse. <https://www.lapresse.ca/dialogue/opinions/2025-04-01/intelligence-artificielle-et-ingerence-electorale/il-faut-agir-pour-protoger-nos-democraties.php>

24 *Ibid.*

1 Les systèmes d'IA, notamment les agents conversationnels, sont imparfaits et peuvent véhiculer de fausses informations. Cette vulnérabilité peut être exploitée par des acteurs cherchant à influencer l'électorat avec des campagnes de désinformation.

3 Les partis politiques sont de plus en plus « professionnalisés » et ont tendance à remplacer les activités militantes traditionnelles par du microciblage politique en ligne, rendu possible grâce aux traces numériques que produisent les internautes.



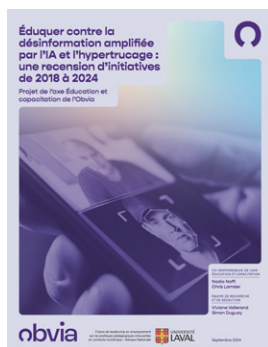
2 Les algorithmes favorisent la circulation de contenus polarisants et les chambres d'écho, ce qui peut nuire à un débat politique sain et limite l'exposition aux points de vue divergents.

4 Les gouvernements et les entités responsables des élections peuvent et doivent renforcer l'encadrement de l'usage des nouvelles technologies comme l'IA en contexte électoral, à l'instar des initiatives en ce sens à l'international.

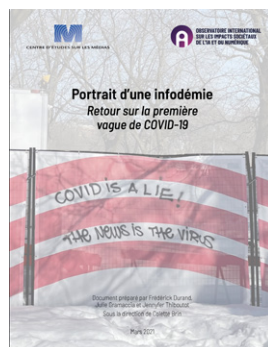
Pour aller plus loin :



Consulter le rapport



Consulter le rapport



Consulter le rapport



L'Obvia, au service des acteurs publics et de la société

L'Obvia identifie les enjeux sociétaux de l'intelligence artificielle et du numérique, et contribue à des solutions qui placent les êtres vivants et la biosphère au centre de leur cycle de développement et d'utilisation. Notre communauté de recherche produit des connaissances ouvertes qui renforcent les capacités individuelles et collectives, en collaboration avec la société civile, les acteurs publics, l'industrie et les développeurs.

Pour nous contacter :

Observatoire international sur les impacts sociétaux de l'IA et du numérique

Pavillon Charles-De Koninck, local 2489
1030, avenue des Sciences-Humaines
Université Laval
Québec (Québec) G1V 0A6

collaboration@obvia.ca
418.656.2131 poste 401234

Pour consulter les autres notes de breffage :



obvia.ca