



Disinformation, Microtargeting, and AI: What Future for Democracies?

Context

Canada has recently experienced its first federal election in the age of AI, and many questions remain about the concrete impacts of new technologies on public debate and democratic processes. The first analyses of the Canadian electoral campaign suggest that few voters were misled by AI-generated content¹. Nevertheless, a few incidents during this campaign call for an examination of how politics are being transformed by digital technologies.

In an electoral context, the degradation of online information quality and the amplification of political polarization by algorithms are very real threats. These digital risks add to the more common political issues of cybersecurity. The techniques used by political parties to win support are also undergoing significant transformations, raising their own set of challenges.

Concerns about the democratic health of states in the face of growing AI use in our societies are not without solutions. For instance, an open letter co-signed by Lyse Langlois, Executive Director of Obvia, proposes actions that governments and political parties should implement to build strong safeguards against the negative effects of AI on democracy.

This briefing note outlines the main issues related to AI and the digital sphere for democracies—particularly in electoral contexts—and presents recommendations to legislators and political strategists to ensure a sustainable coexistence between AI and a healthy, inclusive political debate.

Definitions

Disinformation: False or inaccurate information disseminated with the intent to harm or manipulate public opinion. It can affect various contexts such as climate change, health, the economy, international relations, etc.²

Misinformation: False or inaccurate information which, unlike disinformation, is not shared maliciously; there is no intention to harm or mislead others.³



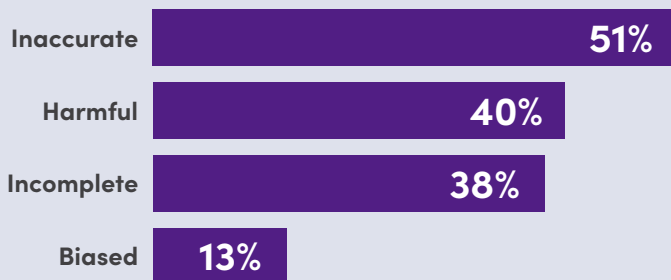
In a July 2024 Abacus Data survey, more than **70%** of Canadian respondents said they were very concerned about online disinformation because of its potential influence on political debate⁴.

Knowledge Overview

A Less Reliable Cyberspace?

Disinformation, fake news, and deepfakes are making it increasingly difficult for many to discern truth from falsehood online and on social media. This concern is shared by experts surveyed for the 2025 edition of the [Global Risks Report](#), who, for the second consecutive year, ranked **disinformation and misinformation** as the top short-term global risks⁵. The massive volume of AI-generated content contributes to the spread of false information in two main ways: first, through possible “hallucinations” or confabulations of AI systems—that is, when the system generates fictitious answers and presents them convincingly⁶—and second, by repeating false information found in cyberspace. It is important to remember that as sophisticated as they may seem, conversational agents like ChatGPT, Grok, or Meta AI do not possess “critical thinking” and are not trained to detect false information. A study found that half of the answers provided by such tools to political questions were inaccurate:

Evaluation of 130 AI model responses to election information queries⁷



This vulnerability of popular conversational agents is exploited by malicious actors seeking to spread false information, notably for political purposes. A March 2025 report⁸ revealed the “infection” of the most used conversational agents in the West by a Russian propaganda network, which created hundreds of websites sharing fake news in more than 46 languages. These sites are rarely visited by humans; their aim is to contaminate AI models with false information by flooding cyberspace—at a rate of 3.6 million fake articles in 2024. **The investigation revealed that the ten most popular conversational agents in Western countries repeated false information from the Russian network 33% of the time.**

The Canadian electoral campaign was not immune to AI-amplified disinformation incidents. At the end of March, a rumor claiming Conservative candidate Pierre Poilievre’s personal fortune exceeded \$20 million—an assertion later debunked—spread widely on social media. As revealed by the *Les Décrypteurs* team⁹, these figures came from the *Pierre Poilievre News* website, which publishes AI-generated articles filled with unverified information. This little-known site managed to make this false claim go viral because it was picked up by other AI-generated news sites and by popular conversational agents, which cited Pierre Poilievre News as a source. Thus, these AI systems end up in a feedback loop, reusing and redistributing AI-generated information without verification, potentially leading to real political consequences.

Fact-checking Undermined

The free flow of false information online is exacerbated by the loss of trust in traditional media and fact-checkers. The [Freedom on the Net 2024](#) report documented many global cases where independent fact-checking organizations themselves became targets of disinformation campaigns aiming to delegitimize them—often orchestrated by political parties and governments¹⁰. This report ranked Canada 3rd out of 72 countries studied in terms of internet freedom, detecting few obstacles to access, content limitations, or violations of user rights. Despite this encouraging data, Canada is not immune to attacks on fact-checkers, as seen during the electoral campaign when a [CTV News journalist](#) faced such harassment.

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-ja-carney-poilievre-desinformation>

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

Whether due to distrust of traditional media or simple disinterest, social media remains a major news source for many Canadians. However, since 2023, traditional media have been banned from all Meta platforms¹¹—including Facebook, Instagram, and Threads—which remain popular in the country. Information integrity on these platforms has suffered further in recent months with the end of third-party fact-checking, now replaced by a “community notes” approach, similar to X’s policy¹². Mark Zuckerberg justified this decision on the grounds of increased online freedom of expression and alleged political bias by third-party fact-checkers, in the context of his ties with the U.S. federal administration.

“Many social media companies have laid off the very teams that were dedicated to advancing trust, safety, and human rights online”¹³ — Freedom House

Without independent and credible fact-checking, social media becomes a playground during elections for actors seeking to influence voters with false information, as well as for foreign interference, often using bots. Recently, presidential elections in Romania had to be annulled and rerun after Russia conducted a massive, harmful influence campaign on TikTok¹⁴. “These bots are used by a variety of actors, often to amplify and manipulate partisan narratives, or to spread rumors or fake news, particularly to attack or support politicians in order to influence public opinion”¹⁵.

Political Polarization and Algorithms: An Explosive Mix

The Global Risks Report 2025 highlights the link between disinformation and misinformation and social and political polarization¹⁶. Polarized discourse tends to distort the truth, fueling the spread of false information. To maximize user engagement, social media algorithms prioritize extremist content: the more content provokes reactions, the more the algorithm gives it visibility¹⁷. Algorithms also contribute to “echo chambers” by showing users content likely to appeal to them from individuals with similar viewpoints.

“An echo chamber is an environment where a person only encounters information or opinions that reflect and reinforce their own. Echo chambers can create misinformation and distort a person’s perspective so they have difficulty considering opposing viewpoints and discussing complicated topics. They’re fueled in part by confirmation bias, which is the tendency to favor info that reinforces existing beliefs.”¹⁸

Such online “information bubbles” limit exposure to varied viewpoints and foster fertile ground for conspiracy theories and, at times, violent political mobilization. Before their presidential pardons in 2025, three rioters from the January 6, 2021, U.S. Capitol attack blamed online misinformation and conspiracy theories in their court defense¹⁹.

Transformation of Political Participation

For many years, the digital realm has been transforming political action and how parties seek votes. The arrival of AI accelerates this shift toward more sophisticated techniques, relying less on grassroots activism. Traditional activities like door-to-door canvassing are gradually being replaced by online political microtargeting:

“Internet users’ digital traces constitute valuable information for party strategists. This granular data enables segmentation and microtargeting operations to determine what message should be communicated to which voters.”²⁰

This practice raises ethical concerns, notably because voters are not equally exposed to all political messages and because their political preferences can be inferred from their online activity—without their knowledge. Even though social media users must accept terms of use, the actual use of personal data can be difficult to grasp for the average user. Recent research on Quebec political parties notes that “the trend toward professionalization and increased reliance on AI and big data analytics specialists will not be stopping soon”²¹.

11 Because of the dissent around Bill 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/clj74mpy8klo>

13 Freedom House (2024). *op. cit.*, p. 6

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

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 GCFGlobal.org. *What is an echo chamber?* <https://edu.gcfglobal.org/en/digital-media-literacy/what-is-an-echo-chamber/1/>

19 *Ibid.*, p.302

20 Dufresne, Y., Dumouchel, D. & Ouellet, C. (2024). *op.cit.*, p.275 [author’s translation]

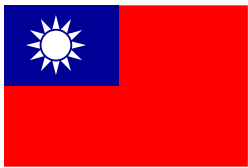
21 Montigny, M. (2024). *L’organisation électorale et la transformation interne des partis à l’ère numérique*. Dans Lalancette, M., Bastien, F., Greffet, F., & Giasson, T., *Médiatisation de la politique : logiques et pratiques*. Presses de l’Université du Québec, p.33 [author’s translation]

Possible Safeguards

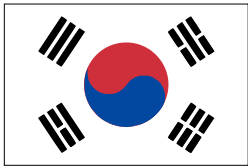
The AI-related risks to democracy outlined in this note can be mitigated with targeted measures. Several countries have begun legislating AI use during elections or supporting initiatives to counter disinformation²²:



South Africa: Ahead of the May 2024 elections, the Electoral Commission (IEC) and the civil society group Media Monitoring Africa (MMA) set up a portal for the public to report cases of fake news, harassment, hate speech, and incitement to violence. Cases assessed by an expert committee could be referred to the country's electoral court.



Taiwan: The Cofacts fact-checking platform, powered by civil society, strengthened citizen trust in online information across the political spectrum and constituencies during the January 2024 presidential election.



South Korea: Lawmakers banned the use of deepfakes in political communications starting 90 days before voting. Offenders face up to seven years in prison or fines of 50 million won (CAD 48,000). The law also mandates labeling all AI-generated political content.

Roles Public Actors Can Play

Political parties:

- 1 Adopt codes of conduct regarding AI during election periods, for instance by committing not to use AI for smear campaigns or to disseminate false information²³;
- 2 Increase transparency about the use of online political microtargeting and the exploitation of citizens' "digital footprint" for partisan purposes;

Governments:

- 3 Strengthen electoral laws regarding AI and deepfake use during campaigns, e.g., by banning the use, publication, and dissemination of misleading AI-generated content²⁴;
- 4 Support and promote digital literacy initiatives to help the public recognize deepfakes and fake news online;
- 5 Enhance critical thinking education in school curricula, especially concerning online content;
- 6 Support and publicize civil society initiatives aimed at countering disinformation and misinformation online, especially during election periods;
- 7 Encourage citizens to consult reliable news sources and to opt for social networks with independent fact-checking.

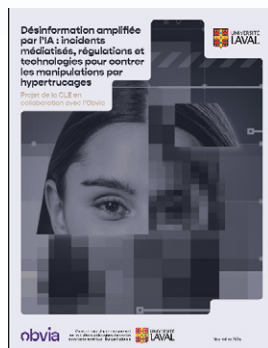
²² Freedom House (2024). *op.cit.*

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>

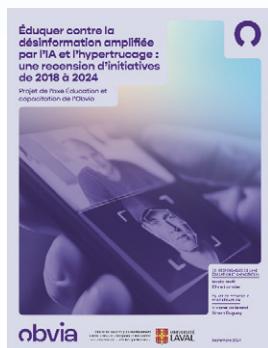
²⁴ *Ibid.*



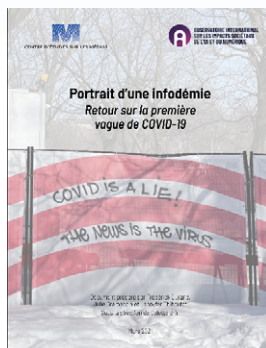
Further reading:



Read the report



Read the report



Read the report



About Obvia

Obvia identifies the societal issues of AI and digital technology and contributes to solutions that place living beings and the biosphere at the center of development and use. Our research community produces open knowledge that strengthens individual and collective capacities, working with civil society, public-sector actors, industry, and developers.

Contact us:

The International Observatory on the Societal Impacts of AI and Digital Technologies

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

collaboration@obvia.ca
418.656.2131 extension 401234

To read our other briefing notes:



obvia.ca

The translation of this briefing note was produced with the help of AI tools (ChatGPT and DeepL) and then reviewed and edited for accuracy and clarity.