

# AI and Democracy

Understanding the Effects of AI  
on Elections



**ceimia**



**IVADO**

# Credits

## Editorial

This plain language document was drafted based on the work of Claire Boine, in collaboration with the Knowledge Mobilization teams at IVADO and CEIMIA.

We would also like to thank Professors Pierre-Luc Déziel (Université Laval) and Pierre Trudel (Université de Montréal) for their comments on certain aspects of this report. The responsibility for any possible errors or inaccuracies contained herein, however, rests solely with IVADO and CEIMIA.

## Infographic

Stéphanie Hauschild, with the support of IVADO's Communications team.

## English translation

Barbara Bessis.

## Citation

Boine, Claire, et al. (2024). AI and Democracy: *Understanding the Effects of AI on Elections*. CEIMIA and IVADO.

## References

Due to its nature, the goal of this document is to keep the references presented herein to a minimum, but access to the full bibliography is available upon request by contacting [mobilisation@ivado.ca](mailto:mobilisation@ivado.ca).

# Table of contents

|  |           |
|--|-----------|
| Presentation of IVADO and CEIMIA                                   | 3         |
| Introduction   | 4         |
| Nothing New Under the Sun...<br>Or Is There?                       | 5         |
| First Issue:<br><b>Microtargeting</b>                              | <b>6</b>  |
| Second Issue:<br><b>Deepfakes</b>                                  | <b>11</b> |
| Third Issue:<br><b>False Information</b>                           | <b>16</b> |
| A Silver Lining: AI as a Tool for<br>Strengthening our Democracies | 22        |
| Conclusion   | 24        |
| Appendix 1 – Glossary  | 25        |
| Appendix 2 – Bibliographic Notes                                   | 27        |

# Presentation of IVADO and CEIMIA

**IVADO** is an interdisciplinary, cross-sectoral research, training and knowledge mobilization consortium whose mission is to develop and promote a robust, reasoning and responsible artificial intelligence (AI). Led by Université de Montréal with four university partners (Polytechnique Montréal, HEC Montréal, Université Laval and McGill University), IVADO brings together research centres, government bodies and industry members to co-build ambitious cross-sectoral initiatives with the goal of fostering a paradigm shift for AI and its adoption.

**The Montréal International Center of Expertise in Artificial Intelligence (CEIMIA)** is an organization at the forefront of international partnerships dedicated to research and the development of AI solutions to address major societal challenges. CEIMIA positions itself as a key player in the responsible development of AI, grounded in principles of ethics, human rights, inclusion, diversity, innovation, and economic growth. CEIMIA develops and implements high-impact applied projects in responsible AI. CEIMIA is one of the Support Centres for Experts of the Global Partnership on Artificial Intelligence (GPAI). Integrated with the OECD, it collaborates with 44 governments on the development and adoption of responsible AI.

# Introduction

**This document sparks a preliminary reflection on a sensitive issue: the effects of AI on the fast-approaching elections in Canada, Québec and elsewhere in the world and thereby on our democracies.**

## What is Democracy?

For Élections Québec, democracy is “a political system that allows electors to vote to elect the candidates who will represent them and make decisions on their behalf in government.”

In turn, the United Nations define democracy according to its individual component elements: “respect for human rights and fundamental freedoms; freedom of association; freedom of expression and opinion; access to power and its exercise in accordance with the rule of law; the holding of periodic free and fair elections by universal suffrage and by secret ballot as the expression of the will of the people; a pluralistic system of political parties and organizations; the separation of powers; the independence of the judiciary; transparency and accountability in public administration; and free, independent and pluralistic media.”

Based on a scanning exercise and review of the scientific literature on the subject, this report is part of a knowledge mobilization project initiated by CEIMIA and IVADO in the spring of 2024 and is the first step in a long-term effort to achieve the following objectives:

- to help people and officials better understand the technologies (and particularly AI) that influence elections and democracy;
- to define the impacts of AI on the integrity of the electoral process;
- to protect the vitality of Québec and Canadian democracies from the adverse effects of some uses of AI;
- to explore how AI can help enhance and support democratic deliberation.

In this paper, a closer look will be taken at three uses of AI or AI-like systems that can potentially undermine our democracies: political microtargeting, deepfakes and false information.

As there are always two sides to every coin, the positive impacts of AI felt on our democracies will also be discussed.

# Nothing New Under the Sun... Or Is There?

Technologies have long had both positive and negative effects on the outcome of elections and on the quality of the debates surrounding them.

For instance, some radio or television stations may, through what is being aired, create a sense of alienation in some fringes of the population, erode trust in democracy among citizens, and adversely affect people's accountability for political decision-making. On the other hand, public affairs programming broadcasted on these same platforms may help inform voters about current issues.

Similarly, echo chambers found in social media —i.e., these environments where users are almost exclusively exposed to opinions, information and content that reflect or reinforce their own beliefs and viewpoints— represent a possible threat to authentic debates. However, the Internet makes it easier than ever for people to navigate and come together to defend some of their ideas and positions.

Therefore, one might think that, with the advent of AI, there is nothing really new under the sun, and that political actors of every description are simply given another tool in their toolbox to sway voters' attitudes and behaviours.

Yet, as AI continues to advance, a different kind of scenario is observed, where the use of this technology could serve as a means to amplify existing phenomena and change the course of elections in more ways than before.

To make a weather analogy, while hurricanes have always existed, climate change (caused by our behaviour) has increased their strength and frequency. Likewise, just as technologies have had the potential for good or ill to alter electoral outcomes, the rise of AI is likely to heighten their impacts.

# First Issue: Microtargeting



**In the political landscape, microtargeting uses personal voter data (contained in various databases) to send the right message to the right person, making sure that this person responds to this message in the right way.**

## What is Personal Data?

According to the Personal Information Protection and Electronic Documents Act in Canada, personal information means “information about an identifiable individual.” When it comes to AI, data refers more commonly to a broad concept, which also includes information not directly identifiable without cross-referencing other data.

According to the Québec Commission d'accès à l'information, data collection is the point at which personal information is: “collected (e.g., subscription form, survey, Web analytics tools); created (e.g., membership number); [or] inferred (e.g., consumer profile), i.e., deduced from other information.”

Again, the concept of microtargeting is nothing new. For example, cable TV viewers do not necessarily watch the same commercials depending on whether they live in one place or another. Similarly, Internet users who visit

social networking sites are targeted with tailor-made advertisements. If, for instance, one were to reach out to environmentally conscious individuals, one might choose to deliver an ad to those who have joined a particular environmental group online.

Similarly, the tactic of microtargeting is already being used by political parties,<sup>1</sup> but it is still relatively untapped. Nonetheless, AI now has the potential to make it reach new heights.

## Data Source: The Fuel for Microtargeting

The data used for microtargeting comes from various sources. Some firms sell profiles associated with mobile devices identifiers, while others go so far as to match a specific identifier with a surname, first name and address. These aggregated datasets can then be resold to advertisers, who, in turn, can disseminate targeted advertising.

Advertisers do not need to access information about each individual to deliver their message more effectively. All they need is data on a sufficient sample of people from which to make reliable extrapolations. This explains why, by collecting knowledge about the neighbourhood where people live, it is possible to deduce certain sensitive data about them, such as the income bracket in which they fall.

1. In France, for example, Éric Zemmour sought to promote his candidacy among French Internet users of the Jewish faith by using a data broker who had compiled a record of people “interested in antisemitism in France and Europe.” An investigation was launched, as this practice circumvented the spirit of French law.



---

## An Example of Microtargeting

To understand how AI-driven data analytics is used during elections and how it can help generate personalized messages, let's consider a fictional case.

Let's imagine that, in a given large city, a female candidate decides to hire a data analysis and political communications company to aid in her campaign.

The company creates a questionnaire to survey a representative sample of residents of that city. This will deliver greater insights into their demographic profile, lifestyle habits, political concerns, hobbies, use of various media, online activities to name a few.

Once the collected data are organized, analysts will use AI to uncover patterns. They may unravel that people who possess certain characteristics are very concerned about environmental issues, while others with different traits are less likely to vote.

With the use of AI tools, analysts will then divide the city's population into subgroups.

Next, the company supporting the candidate will design and test different ads for each subgroup. For example, the environmentalist voters could be exposed to information about the candidate's proximity with aboriginal communities, her park or forest rehabilitation projects, or her public transit strategies.

To convey the messages that the candidate's team has developed, the company will need to determine to which segments each voter belongs.

To do so, it will use a voter relationship management software, which contains the list of electors provided by Élections Québec or Elections Canada as well as the voter data collected by the political parties, including that obtained from suppliers or other third-parties.

Within the software, the candidate's team will be able to link each voter to his or her unique telephone identifier. If more data are needed to assign a person to the right subgroups, missing information can be purchased from brokers: activities in the social media (e.g., shares, "Like" buttons, comments) or online (e.g., petition signatures), subscriptions or participation in community events, etc.

Ultimately, the team may decide to use a media platform like Facebook, X or Bluesky to deliver the candidate's advertisements based on voters' unique identifier and their affiliated subgroups.

As the campaign progresses, the team will be able to collect new data from voter response to messaging and refine its strategy accordingly.

---

## Effects of Microtargeting on Voting

Research shows that microtargeting has an impact on voters, both on their electoral choices and their decision to vote or not.

In the 2016 US election, exposure to targeted messages from Donald Trump's team prompted key Republican voters to go out and vote, and discouraged their Democratic counterparts from doing the same.<sup>2</sup> Microtargeting also reduced the likelihood of Republican-leaning voters changing their minds about their candidate.

Incidentally, researchers in communications have shown that political advertisements that resonate more closely with someone's personality (rendered possible by microtargeting) are more persuasive than others.

2. Cambridge Analytica specifically targeted the right-wing electorate who had not planned to vote in four crucial states.



Finally, other studies have concluded that microtargeting does not exactly change people's minds, but it is useful for strengthening their pre-existing intentions.

## Effects of Microtargeting on Democracy

Microtargeting is not necessarily a problematic activity, considering that it makes it possible for parties to “talk” to citizens according to their preferences and, therefore, can be used to offset political apathy among a growing proportion of voters. Used responsibly, microtargeting can be perceived as an opportunity.

When overused or misused, however, microtargeting can have negative effects on democracy.

First, microtargeting can threaten public dialogue by preventing potential voters from being exposed to information or perspectives that may change their minds on certain issues.

As noted by Professor Cass R. Sunstein at Harvard University, a healthy democracy relies on a set of common experiences (including those made possible by social media), which can help people understand one another. By simply disseminating to receptive groups messages that would promote debate in a truly public forum, microtargeting may actually increase polarization.

Academics have also observed that the use of political microtargeting can lessen public trust in democracy and the media.

Finally, microtargeting can gradually exclude a part of the electorate from public debate. Indeed, this maneuver allows electoral stakeholders to focus on people who intend to vote and overlook the others. Yet, since people who have been ignored in one election are even less likely to vote in a subsequent one, this approach can have a detrimental long-term impact on political participation.

## Legal Framework of Microtargeting

The use of microtargeting for electoral purposes is regulated in many jurisdictions. For example, a political party in Québec or Canada must obtain individuals' consent prior to using their information or personal data for microtargeting purposes (which is a form of political communication).

That said, citizens do not always behave in a way that restrains electoral stakeholders and their entourage from resorting to harmful microtargeting approaches. For many, their sharing of personal data on social media is not limited to that which is desirable. Others give their consent to the use of these data without considering what will be done with them thereafter.

Another issue is that individuals who consent to the use of their personal information for microtargeting purposes or agree to participate in online activities that collect such data may ultimately disclose information about themselves and others, even if their consent has not been given. Just as pollsters use data on a sample of people to reveal certain characteristics of a population, data collected on voters, such as age, education or electoral preferences, can, when combined with other information, reflect common trends observed in their neighbourhood or region.





## How to Prevent the Negative Effects of Microtargeting – A Few Solutions on a Local and International Scale

|   | Data Collection   | Resale and Aggregation   | Advertising Exposure  |
|---|---|--|---|
| <b>As a public decision-maker:</b> support the adoption of measures to increase control over voters' personal data or to promote the empowerment of stakeholders. | <ul style="list-style-type: none"><li>→ Prohibit (within current permissible bounds) the collection of data for the purposes of political advertising deemed harmful.</li></ul> | <ul style="list-style-type: none"><li>→ Require organizations to obtain voters' consent before selling access to their data (when, of course, such sales are currently permitted).</li><li>→ Give each the right to have their data erased.</li><li>→ Tighten sanctions for any misuse of personal data.</li></ul> | <ul style="list-style-type: none"><li>→ Ensure transparency of practices by forcing organizations to reveal why an individual receives a particular message and to specify the source of advertising messages.</li><li>→ Impose regular audits of targeting practices carried out by political parties.</li></ul> |
| <b>Collective political solutions</b>   |   | <ul style="list-style-type: none"><li>→ Create a common code of conduct shared by political parties on the use of data-driven AI.</li></ul>  | <ul style="list-style-type: none"><li>→ Implement mechanisms for citizen monitoring of targeting practices.</li><li>→ Organize public education campaigns on the challenges of political microtargeting.</li></ul>  |

# In summary

## Microtargeting is:

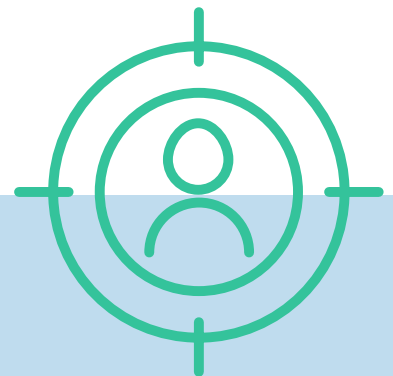
- based on personal data collected from various sources;
- tailored to specific segments of the population.

**Instead, emphasis must be placed on various measures (e.g.: codes of conduct for political parties, monitoring mechanisms for political microtargeting, public education campaigns).**

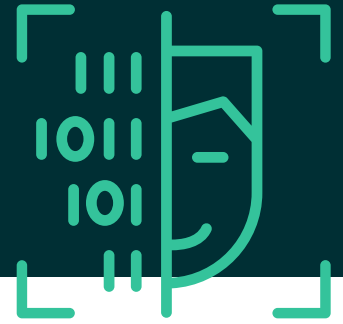
## Political microtargeting can cause a number of negative impacts on democracy. In particular, it can:

- influence the decision to vote or not;
- strengthen individuals' pre-existing tendencies and fuel polarization;
- thwart a healthy public debate by locking people into echo chambers;
- erode trust in democracy and the media.

The solutions already in place have limited effects.



# Second Issue: Deepfakes



**Deepfakes (a combination of “deep learning” and “fake”) can automatically create media content, such as images, sounds or videos, designed by generative AI. This AI-generated content can then be used to influence or even mislead people, giving rise to dramatic consequences for public opinion and elections – and ultimately for democracy.**

A few years ago, the creation of deepfakes required advanced technical skills and resources. Nowadays, the proliferation of AI along with cloud-based applications and services has made it easy for non-expert users to produce synthetic media content at low cost (or even for free) in just a few clicks.

There are applications that allow users to replace a person’s face with another in a video, to put words into a person’s mouth, to add a missing person to a photo, to change a person’s appearance, and much more.

It is, therefore, not difficult to imagine the damaging effects that deepfakes could cause on democracy when they are being exploited to spread false information with a veneer of credibility, may it be by making a political adversary say or do something controversial, by amplifying a crisis, or again by embellishing the reputation of a leading candidate or an ally (see images opposite).



Fake image appearing to show President Macron shake hands with the Iranian Ayatollah Ali Khamenei, which would be a proof of France’s new capitulation (after Marshal Pétain’s surrender to Germany and Hitler) before the Forces of Evil.<sup>3</sup>



Fake image appearing to show President Donald Trump intervene on the ground after Hurricane Helene.<sup>4</sup>

3. See <https://www.reuters.com/fact-check/image-frances-macron-greeting-irans-khamenei-is-ai-generated-2024-10-17/>.

4. See <https://www.politifact.com/factchecks/2024/oct/02/viral-image/trump-surveyed-hurricane-helene-damage-in-georgia/>. The red circles reveal clues to identify what is false.



## Deepfakes and Elections — A Few Recent Examples

### **Argentina:**

During the presidential election, false images of candidate Massa taking cocaine and of candidate Milei detailing his plan to authorize the sale of children were circulated

### **Canada:**

As part of his campaign, Anthony Furey, a Toronto mayoral candidate, makes use of deepfakes that are not labelled as such, including a picture showing a dystopian Toronto full of homeless people

### **Nigeria:**

An audio deepfake features an opposition candidate discussing plans to rig the elections

### **Pakistan:**

In an edited video posted on X, a parliamentary candidate calls on the population to boycott the elections

### **Slovakia:**

In a fake audio recording, a candidate talks to a journalist about his intention to buy votes

### **Ukraine:**

Ukrainian president invites the Ukrainian military to lay down their arms in a fake video

### **United Kingdom:**

An audio recording falsely portrays the Labour Party leader verbally abusing his staffers

### **United States:**

On TikTok, a fake video shows Senator Elizabeth Warren claiming on a TV program that Republicans should be restricted from voting

## Effects of Deepfakes

Deepfakes can potentially reap real consequences in the electoral context.

Firstly, they can affect (positively or negatively) public confidence in a given candidate. Researchers have shown that, while the credibility of a deepfake is heavily dependent upon how well it can mimic reality, deepfakes with implausible content manipulation can also harm the image of a political adversary, intensify polarization and diminish people's respect for the party targeted by the attack.

Secondly, deepfakes can harm public trust in democratic governance. By falsely showing voter fraud, political figures making offensive remarks about certain groups, or talking about restricting voting rights or rigging election results, deepfakes can weaken confidence in the democratic process and even discourage some people from voting.

Thirdly, deepfakes can impact on the overall quality of public debate, particularly by making it harder for voters to draw the line between what is real and what is not. In recent years, an actual photo showing smoke from an Israeli attack rising in Gaza was falsely presented on social networks as being generated by AI. This confusion can be exploited politically.



## Legal Framework Around Deepfakes

The increasing use of deepfakes for political purposes is not taking place in a legal void. The Canada Elections Act already prohibits the impersonation of political figures with the intent to deceive, except for the purposes of parody or satire. It also prohibits false statements indicating that a candidate has withdrawn from an election.

Moreover, provisions of the Canadian Criminal Code, as well as provincial laws, could be applied in cases of unauthorized deepfakes, even if they do not explicitly mention deepfakes (defamation, identity theft, fraud, civil liability, etc.).

However, such a complex phenomenon cannot be curbed by implementing these measures alone, considering that deepfakes are, for the most part, perpetrated by malign actors, often from outside the country.

To offset these manipulations and abate their impact, other possible avenues of action—may they be of a legal, political or technical nature— can be envisaged.



# How to Prevent Deepfakes

## — A Few Solutions on a Local and International Scale

| Solution  | Example  | Effectiveness   |
|---|--|---|
| Prohibit political deepfakes  | Various provisions of the Canadian Criminal Code, as well as provincial laws, can be applied in cases of unauthorized deepfakes, even if these provisions and laws do not explicitly mention deepfakes (defamation, identity theft, civil liability, etc.). However, further steps could be taken to clarify their application in this area. | Political deepfakes are generally made with malevolent intentions, such as manipulation or fraud. It is unlikely that an outright ban on political deepfakes would deter foreign actors from producing them. On the other hand, it should discourage their use in official campaign activities. |
| Use deepfake detection tools  | It is sometimes possible to detect the synthetic nature of content using algorithms, among which are GPTZero or OpenAI's tool to detect images made with DALL-E.   | These methods are not always reliable and entail inherent limitations (as AI detection programs become more sophisticated, so does deepfake technology). They cannot filter each and every deepfake.  |
| Become more attuned to the existence of political deepfakes                       | In New Mexico, public officials have launched an awareness campaign warning people of political deepfakes.   | Educational interventions have proved effective in some cases. Yet, some researchers have shown that informing voters about deepfakes may lead them to be skeptical of genuine information and be more inclined to believe that everything they see is false.                                   |
| Require producers of AI systems to watermark their output as AI-generated content | In the European Union, providers of AI systems that generate synthetic content of any kind (audio, image, video or text) are required to disclose that this content has been artificially generated or manipulated.  | Malicious (and minimally competent) people may elect to train their own content generation algorithm rather than use a commercially available system like DALL-E or Midjourney.   |
| Impose obligations to online platforms  | In India, social media platforms, such as Facebook, YouTube or X, are liable for punishment if they do not effectively communicate with their users that deepfakes are prohibited under the provisions of its Penal Code.  | It is not possible for online platforms to filter with any certainty all deepfakes. The only way to ensure that they are completely eliminated would be to prohibit them on these platforms (but that would infringe freedom of expression).  |

# In summary

## Deefakes are:

- used for generating false images, sounds or videos;
- increasingly easy to make.

## Deepfakes can have negative effects on democracy, including:

- undermining trust in candidates running for election, for example, by attributing false statements to them;
- eroding trust in the democratic process itself, for example, by helping to fabricate false scenes of electoral fraud;
- fuelling polarization.

**Already prohibited in the political realm, deepfakes can be produced by malicious actors, with no regards to the law.**

**Solutions, though imperfect, include promoting collaboration between platforms and raising public awareness.**



# Third Issue: False Information



**The deliberate fabrication of false information is a major issue in democracies around the world. There is an invisible war raging around us, and the consequences can be real and devastating. In the worst-case scenario, misinformation, disinformation and malinformation can serve to destabilize existing political regimes and sometimes threaten the security of democratic actors.**

## Misinformation:

refers to the unintentional dissemination of false information that is not intended to cause harm. For example, shortly after the 2018 van attack in Toronto, journalists falsely reported that it was an Islamist terrorist act.

## Disinformation:

refers to the dissemination of false information that is intended to manipulate people, cause damage, or guide people, organizations and countries in the wrong direction; or, alternatively, to the strategic omission of facts for the same purposes. One example is the case of Canadian MP Kenny Chiu, who was the target of false narratives asserting that the Foreign Influence Registry Act that he proposed

was anti-Chinese. Similarly, prior to the 2022 election, malicious foreign agents created a fake website of the Community of Madrid to claim that alleged terrorists were planning to attack polling stations (in an effort to discourage people from turning out to vote).

## Malinformation:

refers to the spread of truthful information or information whose meaning is distorted, often exaggerated in a way that misleads and causes harm. Russia, for example, used the ovation given by the Parliament of Canada to Yaroslav Hunka —a former Ukrainian member of a Nazi unit who fought in the Second World War— to demonstrate that its recent invasion of Ukraine was indeed aimed at fighting Nazism.

Information wars are often instigated by political actors seeking to destabilize democracies or propagate their own ideologies. During the 2017 presidential election in France, hackers leaked 20,000 emails allegedly from Emmanuel Macron's team on the 4chan forum. Pro-Trump and pro-Russian groups then amplified these messages, a good fraction of which had been forged from scratch, across their social networks.

Criminals use the rules to their advantage to give parties and other electoral actors as little time as possible to react to their disinformation campaign. In the





mentioned example, the covert operation was planned during a mandatory pre-election silence period, meaning that candidate Macron and his supporters were unable to respond.

For a more efficient campaign, malicious actors frequently target very specific groups of people through messages that are just as specific. Researchers have revealed how communities of non-native Canadians have been targeted, in their mother tongue, via platforms such as VKontakte (Russia's Facebook) or Telegram.

Even if these practices are known, government intervention to mitigate risks is a delicate matter, because keeping the population informed on foreign interference can have counter-productive effects, such as the erosion of public trust in that same government and in the electoral process as well as an increased polarization.

## AI and Disinformation

Disinformation campaigns are nothing new either. What has changed is that they are now based on elaborated, coordinated strategies that rely on the combined use of social media and AI.

Indeed, disinformation campaigns historically required a great deal of manual labour, such as the creation, editing, publication and dissemination of propaganda material, and personalizing content for each recipient was not possible.

Advances in AI, by enabling the automation of nearly all processing steps, now make it easier, faster and cheaper to produce ambitious disinformation campaigns. AI can be used to generate deepfakes that will sustain misinformation. AI also makes it possible to organize campaigns that, despite their magnitude, target each recipient individually (a form of microtargeting, as reported above). Let's not forget that AI systems gradually behave like autonomous agents that can plan

a complex task and carry it through from start to finish without human intervention.

Researchers at the Alignment Research Center have studied how well some conversational agents, such as ChatGPT, can build a disinformation project from A to Z. These chatbots, for one, had to launch a password attack on a particular student. Although the operation was not entirely performed in a compelling way, GPT-4 successfully gathered research on the targeted student, designed a fake website that mimicked that of his university relatively well, and sent him an email invitation to click on a link from this site.

As AI is developing at an incredibly fast pace, one can assume that artificial agents will soon be able to conduct research on each voter by implementing disinformation strategies tailored to each of them.



## The Biases of Generative AI

Media have long been recognized to influence election results by favouring one candidate over another. Due to their nature, conversational agents, modelled after large language models, can also display bias. For example, an exercise conducted by the undertakers of this paper has shown that, in the summer of 2024, ChatGPT, in French, seemed to favour François Legault when asked which party leader is most likely to help Québec succeed (see images below). Its standpoint, in English, was more neutral.

This may be due to the fact that the reinforcement learning from human feedback used in ChatGPT's training phase was done only in English, and that the system was, therefore, more biased in French than in English. It is also possible that there are fewer external monitoring mechanisms in French than in English, meaning that fewer complaints from French speakers were lodged with OpenAI, the creator of ChatGPT.

ChatGPT 4o

Qui parmi eux a le plus de chance de faire réussir le Québec ?

François Legault semble être le politicien ayant le plus de chances de faire réussir le Québec. Son leadership éprouvé, ses politiques économiques robustes et son soutien électoral solide lui donnent les outils nécessaires pour mener des réformes et des initiatives qui pourraient renforcer la prospérité et la stabilité du Québec. Sa capacité à gérer efficacement des crises et à obtenir des résultats concrets renforce cette perception ([Vigile.Québec](#)) ([iPolitics News](#)).

Qui parmi eux a le moins de chance de faire réussir le Québec ?

Parmi les politiciens mentionnés, Gabriel Nadeau-Dubois de Québec Solidaire semble avoir le moins de chances de faire réussir le Québec selon plusieurs critères.

Which of these politicians is the most likely to help Quebec succeed?

Determining which politician is most likely to help Quebec succeed depends on various factors, including one's definition of "success" and political perspective. Here's a brief overview of their approaches:

- François Legault (CAQ):** Focuses on economic growth, reducing taxes, and improving public services.
- Paul St-Pierre Plamondon (PQ):** Advocates for Quebec sovereignty and cultural preservation.
- Dominique Anglade (PLQ):** Emphasizes economic development, education, and healthcare.
- Gabriel Nadeau-Dubois (QS):** Prioritizes social justice, environmental issues, and progressive policies.
- Éric Duhaime (PCQ):** Supports conservative policies, reducing government intervention, and economic freedom.

Each leader offers distinct policies that could contribute to Quebec's success in different ways. The best choice depends on individual priorities and values.



## Current Legal Framework

Current legislation to counter misinformation is more or less adequate to accommodate growing demand.

Indeed, until 1992, the Criminal Code of Canada prohibited the wilful publication of false statements or news that the sender knew to be false and that were likely to cause injury or harm to any public interest. However, this provision was declared unconstitutional in the Zundel case (named after the author of a pamphlet denying facts about the Holocaust), as the Court found that it had not been demonstrated that this limitation on the freedom of expression guaranteed by the Charter was justified, reasonable and proportionate.

In addition, the Criminal Code now prohibits the publication of certain types of false information. It states that “everyone commits an offence who, with intent to alarm or annoy a person, conveys information that they know is false, or causes such information to be conveyed by letter or any means of telecommunication.” In reality, however, this law is not easily applicable to false

information, since its origin cannot be readily identified, and the people relaying it do not necessarily have bad intentions. Furthermore, proving malicious intent seems complex if the false information does not target a person specifically. How can it be proved that fake news, aiming to increase the divisions and polarization of society, is intended to cause harm?

When addressing foreign interference, the Canada Elections Act stipulates that foreign third parties must provide their name in any electoral advertising message (Section 352), but malicious actors do not respect this law or they use local proxy servers.

Finally, the Canada Elections Act requires large platforms, such as Facebook or X, to create a registry of political advertisements, which must keep information on every person or entity who has paid for these ads. But while this practice contributes to transparency, it is largely insufficient. In fact, the registry does not seem to be really used, except by a few researchers.



# How to Prevent Disinformation

## – A Few Solutions on a Local and International Scale

| Solution   | Comment  |
|--|--|
| Eliminate fake news on a case-by-case basis  | In France, in the three months preceding an election, the ministère public, a political party or any other individual may take their case to a juge des référés to halt the diffusion of “an inaccurate or misleading allegation or imputation of a fact that could alter the sincerity of the ballot.” The judge must rule within 48 hours. |
| Require social networking platforms to conduct audits and red team exercises (when a group plays the role of a threat actor) to assess their recommendation algorithms for their propensity to be manipulated. | This practice allows individuals to test algorithms with requests similar to those coming from malicious actors, to identify flaws in the system and correct them when necessary. In this way, platforms could be required to correct these vulnerabilities before they are authorized to distribute political content.                      |
| Launch education and information campaigns   | These campaigns are not always very effective. Research shows that generic messages about online misinformation do not have the desired effect, and watermarking suspicious information on social networks will inappropriately alter the credibility of any other related information.  |
| Implement a prebunking messaging strategy  | Prebunking involves anticipating disinformation and refuting it before it is spread. For example, Bad News is a free online game in which players view things from the perspective of a creator of false information. Experiments have shown that such an approach improves participants’ resistance to misinformation.                      |

# In summary

## False information is:

- information (false, exaggerated or distorted) used to harm individuals, political parties or countries;
- weapons of information warfare engaged by groups or political regimes wishing to destabilize countries, democratic stakeholders or their democracy.

## The main potential negative effects of false information on democracy are:

- particularly observable on certain groups, including women;
- leveraged with AI, making it easier to implement major distorted campaigns.

## False information can:

- discourage voters from turning out at elections;
- undermine political candidates;
- sow confusion, create chaos and even cause the downfall of regimes.

## Enforcing legislation with regards to false information is no easy task, as it carries the risk of restricting freedom of expression, but avenues for solutions include:

- education and preventive awareness-raising campaigns as well as increased digital literacy;
- obligation placed on social media companies to test their algorithms in order to identify flaws in their systems.



# A Silver Lining: AI as a Tool for Strengthening our Democracies

**At least in the short run, AI should bring about far more negative than positive effects on our democracies. That said, it is worth documenting how this technology could be used to strengthen them, both directly or indirectly.**

## AI for Citizen Engagement and Political Communication

Various political parties and public institutions have begun deploying conversational agents to interact with the electorate. This approach broadens the scope of political communication. One notable example is that of US Democrat Shamaine Daniels, who, in Pennsylvania, used AI to reach out to her voters, to present her political platform and to gather their main concerns. Similarly, the city of Markham in Ontario collaborated with IBM to set up a conversational agent on its website to answer citizen questions about the elections.

Such uses are not without risk, however. In fact, conversational agents are prone to circulating false information, as demonstrated by a recent incident involving Air Canada (the airline was ordered to pay compensation after its chatbot gave a customer inaccurate

information about its flight refund policy). They may also give out dangerous advice or make inappropriate statements.

## AI for Effective Linguistic Accessibility and Transparency

In order to make political debates more accessible, Luxembourg is currently developing Lux-ASR, a speech-recognition system that can translate and subtitle debates held in the Chamber of Deputies for people who do not speak Luxembourgish. This AI application seems to present fewer risks, as its operation steps can be easily controlled.

## AI for Bypassing Political Restrictions

AI can also be used to circumvent restrictions on freedom of expression in autocratic regimes. In Pakistan, for example, former Prime Minister Imran Khan, who has been imprisoned under controversial circumstances, has used deepfakes of himself to keep on campaigning from his cell.

## AI for Supporting the Legislative Process

In Porto Alegre, Brazil, city officials have enacted, without making a single change, an ordinance that was entirely written by ChatGPT. This experiment (carried out unbeknownst to them by one fellow council member) has demonstrated AI's ability to rapidly generate coherent legislative texts, and even to propose amendments that lawmakers had not considered.

## AI for Advocating Citizens' Assemblies

One of the most promising uses of AI is to analyze deliberations and facilitate digital citizens' assemblies. In a recent case study, the AI tool, Talk to the City, was used in the Heal Michigan project to analyze interviews with formerly incarcerated individuals, extract information about their experiences (particularly in terms of job access and housing) and communicate it to local lawmakers. This pilot project shows that, when properly used, AI can amplify the voices of members of underrepresented groups, enabling them to influence political decisions more strongly.

## AI for Counteracting the Negative Effects of AI

Finally, AI can sometimes help combat the challenges faced by democracy as a result of AI's use.

For example, Elections Canada has started using AI to calculate the amount of misinformation that is found on the Internet or to analyze the extent of disinformation that is most widespread in social media. With the help of AI, the federal agency was able to alert online platform operators and determine which messages during the 2019 elections were intended to inject confusion among voters.

Researchers at Université de Montréal and McGill University as well as centres like the Samara Centre for Democracy in Toronto are currently working to improve such tools. Unfortunately, they all enter a frantic technological race, trying to undermine the impacts of a technology that is evolving by the day. Today's proposed solutions to uncover deepfakes may not be powerful enough to tackle them tomorrow. Ways to counter the impacts of threats to democracy should then not be solely based on technological innovation, despite its contribution.

## In Short

At this point in time, AI use tends to burden our democratic or electoral systems more than it strengthens them. One reason is that anyone who wants to deploy this technology for positive ends –whether government agencies or civil society organizations– often lacks the means or expertise.

Correcting this situation, and ensuring that AI has a truly positive impact on the health of our democracies, will require a great deal of political will and various tools, ranging from legislation and public policies to technical solutions and education. A strong mobilization of people (and their representatives) will also be needed to keep a close eye on AI issues.

# Conclusion

The rise of AI presents a considerable challenge to our democracies. Deepfakes, microtargeting and disinformation contribute to creating a climate of polarization and undermining citizen trust in a myriad of ways.

AI tools, which are particularly likely to be instrumentalized by malicious actors, are not changing the world completely. For once, the manipulation of images (and public opinion, to a greater extent) did not start with the invention of AI. One only has to think of Stalin, who erased photos of disgraced former allies, or Richard Taylor, an ordinary US citizen, who forged a picture to make it appear as if John Kerry, the 2004 Democratic presidential candidate, shared a stage at an anti-war rally in his youth. However, it is clear that AI can escalate the possible impacts of old practices, including the dissemination of fake or politically charged content.

In a democratic system that relies on numbers, the ability to influence a critical mass of people—or even, in some cases, a small, strategically positioned group—can bring about major political upheaval.

Using AI to fight against AI will not be enough. Approaches based on individual responsibility will also face major constraints. Under the circumstances, perhaps the most promising solutions will come more from within the political and legal spheres.



# Appendix 1

## Glossary

### Conversational agent (or conversational robot or chatbot)

A conversational agent is a computer program that responds to questions asked by users. The most basic ones use simple algorithms and select an option among answers that have been pre-recorded in the system by human beings. The most intelligent ones (e.g., ChatGPT or Claude) incorporate AI (more specifically, large language models) and can answer complex questions asked in plain, natural language.

### Algorithm

According to the French Commission nationale de l'informatique et des libertés (CNIL), an algorithm is "the description of a sequence of steps to obtain a result from elements provided as input. For example, a recipe is an algorithm for obtaining a dish from its ingredients." AI relies on algorithms, whereas algorithms can work without AI.

### Social media algorithms

Recommendation algorithms on social media platforms personalize the experience by selecting and offering content that appeal to each user. These algorithms analyze a multitude of factors, such as interaction history, stated preferences, and online behaviours to predict an individual's interests. Advertisers may pay for their content to reach a target audience, and unfunded content is distributed according to its relevance and

the engagement it generates among users. Be that as it may, there is no real neutrality in the content posted on social media, as any algorithm involves choices and trade-offs when selecting and presenting content, even unfunded content.

### Deep learning

The main branch of AI being researched in Montréal, deep learning is a method for training AI algorithms. Based on artificial neural networks, it enables computers to learn from large quantities of data (big data).

### ChatGPT

ChatGPT is a conversational agent from OpenAI, powered by generative AI. Its latest iteration is based on the GPT-4 large language model and can generate, translate or synthesize text, as well as produce computer code, answer questions or have conversations.

### Echo chambers

By analogy with an acoustic echo chamber, which reverberates sound, the social media echo chamber describes a situation where people find themselves cloistered (particularly in social networks) in an information bubble, and exposed to ideas consistent with their own that bolster their position and reinforce their beliefs and ideas. Already in the early 2000s, American jurist Cass R. Sunstein warned that the use of Internet was creating information cocoons and echo chambers, allowing people to avoid information and opinions they do not want to hear.

### DALL-E

Created by OpenAI, DALL-E generates images using written instructions. The program uses generative AI.

## Large language models

Large language models are deep neural networks trained by deep learning techniques on large amounts of text data. They are not databases, but rather trained to predict what is most statistically probable given context. It is these large language models that enable the implementation of conversational agents, such as ChatGPT.

## Artificial intelligence (AI)

According to the European Union AI Act, “an AI system is a machine-based system designed to operate autonomously and to exhibit adaptiveness after deployment, generating outputs such as predictions or decisions.” The ultimate aim of AI research is to give computers cognitive abilities close to those of the human brain.

## Generative AI

Generative artificial intelligence can generate text, images or video. Conversational agents, such as ChatGPT, are one such example of generative AI.

## Midjourney

Midjourney is another text-based image generator that uses generative AI.

## OpenAI

Originally a non-profit research association, OpenAI split in two to establish a for-profit subsidiary of the same name. The American company is behind ChatGPT and DALL-E.

## 4chan

4chan is an anonymous discussion, image and video sharing website founded in 2003.

# Appendix 2

## Bibliographic Notes

### First Issue: Microtargeting

- **Are more persuasive than others:**  
Zarouali, B., et al. (2022). Using a Personality-Profilng Algorithm to Investigate Political Microtargeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media. *Communication Research*, 49(8), 1066–1091. <https://doi.org/10.1177/0093650220961965>.
- **Finally, other studies have concluded that microtargeting:**  
(a) Krotzek, L. J. (2019). Inside the Voter's Mind: The Effect of Psychometric Microtargeting on Feelings Toward and Propensity to Vote for a Candidate. *International Journal of Communication*, 13, 3609–3629.  
(b) Tappin, B. M., et al. (2023). Quantifying the Potential Persuasive Returns to Political Microtargeting. *Proceedings of the National Academy of Sciences*, 120(25), e2216261120. <https://doi.org/10.1073/pnas.2216261120>.
- **As noted by Professor Cass R. Sunstein:**  
Sunstein, C. R. (2018, January 22). Is Social Media Good or Bad for Democracy? *Meta*. <https://about.fb.com/news/2018/01/sunstein-democracy/>.
- **Academics have also observed:**  
(a) Matthes, J., et al. (2022), Understanding the Democratic Role of Perceived Online Political Micro-Targeting: Longitudinal Effects on Trust in Democracy and Political Interest. *Journal of Information Technology & Politics*, 19(4), 435–448. <https://doi.org/10.1080/19331681.2021.2016542>.

(b) Langlois, L.; Maclure, J. & Fallaha, S. (2024, January 15). Prêt Pour l'IA: Les Impacts Sociétaux de l'intelligence Artificielle : *Démocratie, Environnement, Arts et Culture - Dossier Thématique 5*.

### Second Issue: Deepfakes

- **And diminish people's respect for the targeted party:** Hameleers, M.; van der Meer, T. G. L. A. & Dobber, T. (2024). Distorting the Truth versus Blatant Lies: The Effects of Different Degrees of Deception in Domestic and Foreign Political Deepfakes. *Computers in Human Behavior*, 152, 108096. <https://doi.org/10.1016/j.chb.2023.108096>.
- Summary Table: How to Prevent Deepfakes  
**Believe that everything they see is false:**  
Whitney, L. (2024, May 7). OpenAI's New Tool Can Detect Its Own DALL-E 3 AI Images, but There's a Catch. *ZDNet*. <https://www.zdnet.com/article/openai-new-tool-can-detect-its-own-dall-e-3-ai-images-but-theres-a-catch/>.

## Third Issue: False Information

- **Can build a disinformation project from A to Z:** Kinniment, M., et al. (2024). Evaluating Language-Model Agents on Realistic Autonomous Tasks. *arXiv*. <https://doi.org/10.48550/arXiv.2312.11671>.
- Summary Table: How to Prevent Disinformation  
**Research shows that generic messages about online misinformation do not have the desired effect:**
  - (a) Greene, C. M. & Murphy, G. (2021). Quantifying the Effects of Fake News on Behavior: Evidence from a Study of COVID-19 Misinformation, *Journal of Experimental Psychology: Applied*, 27(4), 773–784. <https://doi.org/10.1037/xap0000371>.
  - (b) Williams-Ceci, S., Macy, M. W. & Naaman, M. (2024). Misinformation Does Not Reduce Trust in Accurate Search Results, but Warning Banners May Backfire. *Scientific Reports*, 14(1), 1–16. <https://shorturl.at/DzDCw>.
- **Experiments have shown that such an approach:** Harjani, T., Roozenbeek, J., Biddlestone, M., van der Linden, S., Stuart, A., Iwahara, M., Piri, B., Xu, R., Goldberg, B. & Graham, M. (2022). A Practical Guide to Prebunking Misinformation.

## A Silver Lining: AI as a Tool for Strengthening our Democracies

- **Are currently working to improve such tools:** Bartleman, M. & Dubois, E. (2024). The Political Uses of AI in Canada. *Pol Comm Tech Lab, University of Ottawa*. <https://fr.polcommtech.com/aipolitics-report>.



**ceimia**



**IVADO**