



**RÉPONSE AU DOCUMENT DE CONSULTATION *POUR UNE NOUVELLE
VISION DE LA LOI ÉLECTORALE***

Mémoire présenté à
Élections Québec

Par la
Commission de l'éthique en science et en technologie

2024

Commission de l'éthique en science et en technologie

888, rue Saint-Jean, bureau 555

Québec, QC

G1R 5H6

Document préparé par

François Boucher, conseiller en éthique

Luc Bégin, président de la CEST

Coordination

Nicolas Bernier, secrétaire général par intérim

Ce mémoire a été préparé par le secrétariat de la Commission de l'éthique en science et en technologie et par son président. N'ayant pas fait l'objet d'une résolution lors d'une réunion officielle des membres, ce mémoire n'est pas une publication officielle de la Commission de l'éthique en science et en technologie.

© Gouvernement du Québec, 2024

Table des matières

Présentation de la CEST	1
Introduction.....	2
1. Les nouveaux risques pour la démocratie à l'ère de l'IA et du numérique	4
1.1. L'approche fondée sur les risques en gouvernance de l'IA et les interrogations soulevées par Élections Québec.....	4
1.2. Désinformation assistée par l'IA et marketing politique numérique.....	6
2. L'accès au vote et le droit de se présenter aux élections. Commentaire sur les chapitres 1 et 2.....	10
2.1. Accès au vote et fracture numérique.....	10
2.2. IA et accès au vote	11
2.3. IA, égalité et droit de se présenter aux élections	12
3. L'utilisation de l'IA et des données massives dans le cadre de l'information électorale et politique : commentaires sur le Chapitre 4 L'information électorale et politique	14
3.1. La mission d'information d'Élections Québec	14
3.2. Encadrer l'utilisation de l'IA générative dans l'information politique et électorale .	16
3.3. Mieux encadrer les pratiques de microciblage.....	20
4. Enjeux de gouvernance électorale. Commentaires sur le chapitre 5	23
4.1. Révision périodique de la Loi électorale	23
4.2. Renforcer les capacités d'Élections Québec en incluant des experts de l'IA et du numérique dans différents comités visant à épauler Élections Québec	24
Bibliographie.....	26

Présentation de la CEST

Créée en 2001, la Commission de l'éthique en science et en technologie (CEST) a pour mission de conseiller le gouvernement du Québec sur toute question relative aux enjeux éthiques liés à la science et à la technologie et de susciter la réflexion sur ces enjeux. Ses activités visent à informer, à sensibiliser et à émettre des recommandations pour favoriser une plus grande prise en compte de l'éthique, notamment par les décideurs et les milieux de pratique, afin de les accompagner dans leurs processus décisionnels. La CEST est composée de treize membres, dont un président, tous nommés par le gouvernement et issus de milieux variés afin que ses travaux misent sur l'interdisciplinarité.

Depuis quelques années, la CEST s'intéresse fortement aux enjeux éthiques soulevés par les transformations des communications et de la circulation de l'information à l'ère numérique. Elle a notamment rendu récemment deux avis sur la numérisation du système de santé¹ et produit des mémoires sur la *Loi favorisant la transformation numérique de l'administration publique*² et sur la *Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives*³. La CEST s'est aussi penchée sur les enjeux éthiques découlant des avancées récentes en matière d'intelligence artificielle (IA), en publiant notamment des avis sur la gestion algorithmique du travail⁴ et en effectuant des travaux sur les impacts de l'IA et du numérique sur la démocratie. La CEST a exploré les défis et enjeux éthiques qui accompagnent la cyber citoyenneté dans un contexte où une grande part de l'information circule sur les médias sociaux et grandes plateformes numériques, lesquels s'imposent par ailleurs à l'heure actuelle comme des forums⁵. La CEST s'est penchée plus spécifiquement sur les questions soulevées par l'impact de l'IA sur la démocratie en prenant part au processus de réflexion collective sur l'encadrement de l'IA au Québec orchestré par le Conseil de l'Innovation du Québec (CIQ)⁶, lequel a mené à la publication par le CIQ du rapport *Prêt pour l'IA*, en février 2024. Conjointement avec l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) et le Centre d'expertise International de Montréal en intelligence artificielle (CEIMIA), la CEST a remis au CIQ un « État de la situation » et un « Rapport d'experts » portant tous deux sur les impacts de l'IA⁷. Le présent mémoire s'inscrit dans la foulée de cette réflexion et l'approfondit en répondant à certaines questions soulevées par Élections Québec dans son document de consultation *Pour une nouvelle vision de la Loi électorale*.

¹ Commission de l'éthique en science et en technologie 2022, 2023a.

² Commission de l'éthique en science et en technologie 2019.

³ Commission de l'éthique en science et en technologie 2021.

⁴ Commission de l'éthique en science et en technologie 2023b.

⁵ Commission de l'éthique en science et en technologie 2018.

⁶ Conseil de l'innovation du Québec, 2024.

⁷ Centre d'expertise international de Montréal en intelligence artificielle (CEIMIA), Commission de l'éthique en science et en technologie (CEST) et Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) 2023a, 2023b.

Introduction

Dans ce mémoire, nous commentons le document d'Élections Québec *Pour une nouvelle vision de la Loi électorale* en nous penchant sur les passages de ce document qui concernent les défis qui confrontent les démocraties à l'ère du numérique et de l'intelligence artificielle. Nous nous intéresserons notamment à la désinformation assistée par l'IA, laquelle peut impliquer des robots conversationnels qui amplifient certains messages ou encore l'utilisation d'hypertrucages (*deepfakes*). Nous porterons aussi notre attention aux pratiques de campagnes électorales faisant appel à l'analyse de données massives, notamment au microciblage dans les communications politiques. Notre réponse au document de consultation d'Élections Québec fait principalement écho à son quatrième chapitre, portant sur l'information électorale et politique. Cela dit, nous nous pencherons aussi sur l'impact du numérique et de l'IA sur l'accès au vote et sur le droit de se présenter aux élections. Enfin, nous soulignerons brièvement comment ces préoccupations peuvent être mises en relation avec les questions de gouvernance posées par Élections Québec.

Le document de consultation *Pour une nouvelle vision de la Loi électorale* reconnaît l'importance des enjeux soulevés par la désinformation et le marketing politique à l'ère du numérique et de l'IA. Ainsi, d'une manière générale, la CEST accueille très favorablement l'ensemble des propositions faites par Élections Québec. Celles-ci, en somme, visent à modifier la Loi électorale de sorte à bonifier les capacités d'Élections Québec à lutter contre la désinformation et à favoriser la transparence dans les communications politiques tout en considérant la possibilité d'imposer de nouvelles obligations aux partis politiques et aux plateformes en ligne.

Élections Québec souligne par ailleurs l'importance de valeurs telles que la capacité des citoyens à voter de manière éclairée, la transparence des plateformes numériques et des systèmes d'IA, la nécessité de préserver la liberté d'expression, bien que celle-ci ne soit pas absolue, la nécessité de protéger la vie privée et les renseignements personnels des électeurs. Dans ses travaux, la CEST a identifié des valeurs tout à fait similaires devant être mises de l'avant pour penser l'exercice responsable de la citoyenneté démocratique à l'ère des plateformes en ligne et des médias sociaux. Elle souligne l'importance de l'exercice responsable de la liberté d'expression et lie celle-ci à la qualité et la diversité de l'information disponible sur les plateformes numériques. Elle met aussi de l'avant l'importance de la transparence, laquelle joue un rôle clé, car il est souvent difficile pour les utilisateurs de bien saisir l'étendue des pratiques de collecte et d'analyse de données, de comprendre le fonctionnement des algorithmes ainsi que les processus décisionnels qui sous-tendent le fonctionnement des plateformes. Elle reconnaît aussi que le respect de la vie privée et de la dignité des individus est une préoccupation éthique fondamentale, alors que les plateformes en ligne collectent souvent d'énormes quantités de données personnelles, parfois sans que les utilisateurs en soient pleinement conscients. Enfin, elle

souligne l'importance de l'équité et de l'accessibilité en contexte de fracture numérique au sein de la population.⁸

Élections Québec pose plusieurs questions relatives à la force des obligations qui devraient encadrer l'usage de l'IA dans les campagnes électorales et les communications politiques en ligne. Comme la réponse que l'on donne à ces questions dépend de la manière dont on conçoit les risques associés à ces pratiques, nous commençons, dans une première section, par rappeler les principaux risques que la montée de l'IA et des communications politiques en ligne fait peser sur le processus électoral. Ensuite nous commentons directement certaines propositions faites dans les chapitres 1, 2, 4 et 5 du document de consultation *Pour une nouvelle vision de la loi électorale*. Une section est dédiée aux chapitres 1 et 2 du document d'Élections Québec, une autre est consacrée au chapitre 4 et la dernière section concerne le chapitre 5.

⁸ La CEST a exploré ces grandes valeurs liées au développement et au déploiement responsables du numérique et de l'IA dans plusieurs publications et interventions. Néanmoins, on trouvera une présentation synthétique du cadre d'analyse éthique qui oriente les travaux de la CEST sur l'IA, le numérique et la démocratie dans le mémoire de la CEST sur les thèmes potentiels pour le programme d'étude *Éthique et culture religieuse* (maintenant remplacé par le programme *Culture et citoyenneté québécoise*) (CEST 2020). Ce cadre éthique articule les grands principes qui devraient encadrer l'exercice de la citoyenneté numérique et que nous avons brièvement mentionnés plus haut (exercice responsable de la liberté d'expression, qualité de l'information, transparence, respect de la vie privée, équité et sobriété numérique – nous avons omis de mentionner ce dernier principe, la sobriété numérique, car il a moins d'incidence directe sur une éventuelle refonte de la Loi électorale). En présentant ce cadre, ce mémoire s'inspire de l'avis *Éthique et cybercitoyenneté : un regard posé par des jeunes*, produit deux années plus tôt par la CEST-Jeunesse, un projet biannuel réalisé avec la participation de cégépiennes et cégépiens (CEST 2018).

1. Les nouveaux risques pour la démocratie à l'ère de l'IA et du numérique

1.1 L'approche fondée sur les risques en gouvernance de l'IA et les interrogations soulevées par Élections Québec

Les efforts les plus avancés et les plus ambitieux en matière d'encadrement de l'IA sont structurés par une approche fondée sur les risques posés par différents systèmes d'IA. C'est notamment le cas de la *Législation sur l'Intelligence artificielle de l'Union européenne (EU AI Act)*⁹ et du projet de *Loi sur l'intelligence artificielle et les données du gouvernement du Canada*¹⁰. Cette approche reconnaît que toutes les applications d'IA ne présentent pas les mêmes risques et que la réglementation doit être proportionnée au niveau de risque associé à une application d'IA spécifique¹¹. Plus le risque est élevé, c'est-à-dire, plus le potentiel de nuisance est élevé, plus le niveau adéquat d'encadrement législatif et réglementaire par l'État est élevé.

Ainsi, l'Union européenne (UE) considère quatre niveaux de risque dans sa législation. Les systèmes posant des « risques minimes ou négligeables », par exemple ceux utilisés pour le divertissement et pour usage personnel, peuvent être régulés par des codes de conduite volontaires. À l'autre bout du spectre, les systèmes présentant des « risques intolérables », notamment ceux qui bafouent la dignité humaine (comme un système de surveillance fondé sur la reconnaissance biométrique en continu dans les espaces publics) sont intégralement prohibés. Un cran plus bas dans l'échelle du risque, on retrouve les systèmes à « risque élevé », ceux qui posent des risques significatifs pour la sécurité, la santé et les droits fondamentaux (par exemple, un système de décision automatisé qui aurait un impact sur le recrutement ou sur certaines décisions judiciaires). Ceux-ci devraient être sujets, par exemple, à des obligations très strictes de contrôle de la qualité et de supervision humaine. À la différence, les systèmes posant un « risque limité » aux consommateurs, par exemple, le risque d'être floué ou induit en erreur, ne sont assujettis qu'à des obligations de transparence qui visent simplement à informer l'utilisateur à propos d'un système d'IA (notamment, à l'informer à propos du fait qu'il interagit avec un système d'IA et des paramètres encadrant l'interaction). Le projet de loi du gouvernement canadien contient une catégorie similaire à celle de « système à risque élevé » qui s'appliquerait aux « systèmes à incidence élevée », lesquels seraient assujettis à des obligations qui elles aussi iraient au-delà des exigences de transparence. Il se dégage aussi de ce projet une volonté

⁹ Voir <https://artificialintelligenceact.eu/fr/l-acte/>.

¹⁰ Voir <https://artificialintelligenceact.eu/fr/l-acte/>. Le Québec n'a pas encore de projet de loi équivalent, mais dans son rapport *Prêt pour l'IA*, le CIQ se prononce en faveur d'une approche fondée sur les risques. Voir notamment CIQ 2024, 5. L'approche de l'encadrement de l'IA fondée sur les risques est aussi mise de l'avant par l'OCDE (2024) et bien que les États-Unis aient une approche plus décentralisée, volontariste et pro-innovation, la logique de proportionnalité sous-jacente à l'approche des risques y joue un certain rôle, notamment depuis la publication du AI Risk Management Framework en 2023 par le National Institute of Standards and Technology (NIST).

¹¹ Holistic AI, 2024.

de prévoir des interdictions ciblant les usages malveillants ou insoucieux de l'IA qui pourraient causer des préjudices graves à certaines personnes.

Plusieurs des interrogations soulevées par Élections Québec dans le chapitre 4 de son document de consultation sur le renouveau de la Loi électorale reprennent l'idée, chère à l'approche fondée sur les risques, d'une gradation dans les niveaux d'intervention de l'État. On demande ainsi s'il faut imposer des obligations de transparence relatives à l'utilisation, dans les communications politiques et électorales, (1) d'agents conversationnels artificiels sur les réseaux sociaux, (2) d'hypertrucages produits grâce à différentes applications d'IA générative et (3) de techniques de microciblage. Faut-il plutôt laisser les développeurs d'IA et les plateformes numériques adopter des normes volontaires ou bien au contraire imposer des obligations plus strictes que des exigences de transparence, par exemple des interdictions ou des restrictions de ces usages de la technologie?

Il serait tentant de répondre hâtivement que l'UE a déjà tranché la question, du moins par rapport aux hypertrucages et aux robots conversationnels. Dans sa récente législation sur l'IA, l'UE a en effet créé une catégorie expressément dédiée à l'IA générative, laquelle est vue comme posant un simple risque d'être induit en erreur qui pourrait être neutralisé par des mesures de transparence qui rendent disponibles aux yeux de tous certaines informations. Or, on peut très bien considérer que cette manière de concevoir et réglementer l'IA générative convient pour les usages « ordinaires » et « généraux », « dans la vie de tous les jours », de cette technologie (dans les publicités commerciales, par exemple) sans que cela ne soit le cas pour le contexte spécial des élections. Celui-ci se caractérise, entre autres, par l'impact potentiellement énorme qu'a l'issue d'une élection sur la législation et la réglementation, le risque de crise sociale, voire de violence, en cas d'élections contestées, le caractère compétitif de la relation entre les partis et la portée symbolique du processus électoral. Il convient donc d'examiner de plus près les risques posés par l'IA générative (hypertrucages et robots conversationnels) et les techniques de microciblage en contexte électoral pour voir si des mesures spécifiques sont requises par ce contexte unique, lequel est d'ailleurs déjà source de multiples obligations spéciales, qu'on pense aux règles encadrant les dépenses électorales et les dons aux partis politiques ou encore à l'obligation qu'ont les employeurs d'accorder suffisamment de temps à leurs employés pour aller voter¹².

Dans le reste de cette section, nous rappelons les risques que l'IA générative et les pratiques de collecte et d'analyse de données massives font peser sur la qualité de l'information et de la délibération publique. Par contre, nous verrons dans les prochaines sections que ces usages de la technologie peuvent aussi occasionner d'importants préjudices personnels.

¹² L'UE n'a pas non plus tranché de manière définitive la question du microciblage, bien qu'on discute actuellement d'un projet de loi controversé qui aurait pour effet de rendre le microciblage impossible, en limitant sévèrement la collecte de données effectuée par les partis. Voir <https://www.europarl.europa.eu/news/fr/press-room/20230130IPR70208/le-parlement-vote-pour-renforcer-les-regles-en-matiere-de-publicite-politique>.

1.2 Désinformation assistée par l'IA et marketing politique numérique

Dans ses travaux sur l'impact de l'IA sur la démocratie et sur la citoyenneté à l'ère numérique, la CEST a identifié deux types d'usages de l'IA et des données massives qui soulèvent des préoccupations majeures quant à la capacité des citoyens à voter et à délibérer de manière éclairée et autonome, soit la désinformation assistée par l'IA (laquelle fait intervenir des robots conversationnels ou encore des contenus générés par des IA génératives) et les pratiques de microciblage des partis politiques.

Les risques que la désinformation fait peser sur l'intégrité des élections sont magnifiés par l'arrivée de l'IA générative. Une IA est dite « générative » lorsqu'elle possède la capacité de générer de nouveaux contenus en réponse à des propositions textuelles d'un utilisateur. On peut penser à des plateformes textuelles comme ChatGPT, mais aussi à des plateformes de génération d'images, comme DALL-E 2, Stable Diffusion ou Midjourney. Pour arriver à ces résultats, les IA génératives doivent être entraînées avec de grandes quantités de données : des textes, des photos ou des images.

Bien entendu, ce phénomène n'est pas nouveau et les dernières années (depuis l'élection américaine de 2016 et la pandémie de COVID-19) ont donné lieu à des travaux sur la désinformation et dissémination de fausses nouvelles via les plateformes numériques¹³. Cependant, l'arrivée de l'IA générative permettant de produire facilement du texte, des images ainsi que des clips audios et vidéos propulse la désinformation à une tout autre échelle¹⁴. En effet, l'usage de ce type d'IA est maintenant largement accessible depuis que plusieurs plateformes permettent de générer du contenu synthétique à partir de commandes exprimées dans des langues naturelles (français, anglais, etc.), ce qui accentue fortement les impacts négatifs potentiels de la désinformation sur la délibération publique. L'usage de ces technologies entraîne des gains en efficacité par le fait d'automatiser la création de tout type de contenus (écrit, audio, image, vidéo), ce qui ouvre la porte à la circulation d'un très haut volume de contenus synthétiques, notamment sur les médias sociaux, où la vitesse de propagation de l'information (et de la désinformation ou de la mésinformation) est très rapide, surtout lorsqu'elle est propulsée par des robots conversationnels. Enfin, combinés à des techniques de microciblage, les hypertrucages deviennent d'autant convaincants qu'ils sont faits sur mesure pour susciter l'adhésion de publics cibles¹⁵.

L'arrivée des hypertrucages, des créations visuelles et audios synthétiques prétendant représenter des personnes et des événements réels¹⁶, suscite un degré particulièrement élevé d'inquiétude chez les observateurs¹⁷. D'une part, ces hypertrucages sont très difficiles à détecter, tant pour les êtres humains¹⁸ que pour les algorithmes de détection¹⁹. D'autre

¹³ Brown 2021, Chambers et Kopstein, 2022; Dumbrava, 2021.

¹⁴ Buchanan et al., 2021; Goldstein et al., 2023; Paris et Donovan, 2019.

¹⁵ Cohen et Fung, 2021.

¹⁶ Helms, 2022.

¹⁷ Voir notamment Schick 2020; Citron & Chesney, 2019; Macdonald 202; Rini et Cohen 2022.

¹⁸ Köbis et al., 2021.

¹⁹ Thompson et Hsu, 2023.

part, notre faible capacité à détecter ces hypertrucages remet en question la confiance que nous pouvons placer dans les sources audios, vidéos et photographiques, normalement considérées comme des éléments solides de preuves empiriques permettant de vérifier les faits²⁰. Certains commentateurs soulignent par ailleurs que le risque le plus sérieux par rapport aux hypertrucages ne consiste pas tant dans la production par l'IA de fausses nouvelles ponctuelles ou à la pièce, mais bien dans la production d'« histoires synthétiques » consistant en des ensembles de fausses nouvelles synthétiques de différents types se soutenant mutuellement et supportant de faux récits²¹.

Comme l'IA générative arrive facilement à créer des contenus pouvant duper les usagers²², elle exacerbe considérablement les risques de manipulation politique par la désinformation²³. La manipulation est une forme d'influence insidieuse sur autrui qui ne fait pas appel aux capacités réflexives des personnes et fonctionne en partie parce qu'elle demeure cachée aux personnes ciblées²⁴. La désinformation dans les médias numériques alimentée par l'IA est une forme de manipulation puisqu'elle vise à modifier les croyances de manière insidieuse en exploitant les asymétries de connaissances relatives au fonctionnement de l'IA et des médias numériques. Elle porte ainsi atteinte à la capacité des électeurs de faire des choix autonomes et à prendre part de manière éclairée à la délibération publique.

Un second type de risque démocratique à l'ère numérique découle de nouvelles pratiques de marketing politique en ligne et de campagnes électorales alimentées par les données (*data-driven campaigns*).²⁵ Ainsi, le microciblage en marketing politique numérique est une stratégie qui vise à personnaliser les messages politiques en fonction des données personnelles des individus, telles que leur démographie, leur style de vie ou leurs habitudes de consommation. Cette personnalisation permet de cibler les besoins spécifiques des électeurs afin de maximiser l'impact du message et d'encourager leur soutien pour un parti politique donné ou leur participation à son financement. Les techniques de microciblage permettent de segmenter la population en groupes de personnes partageant certains traits les rendant plus susceptibles de réagir d'une manière donnée à certains messages. Plus précisément, le microciblage est « une technique de marketing politique visant la création de messages conçus spécifiquement pour un individu, au moyen d'analyses produites à partir des données personnelles de cette personne en fonction de critères tels que les caractéristiques démographiques, le style de vie, les habitudes de consommations et bien d'autres. »²⁶ Ces techniques permettraient notamment aux partis de mieux interpellier les électeurs sur des sujets qui les intéressent vraiment et de diversifier leur discours de sorte

²⁰ Paris et Donovan, 2019.

²¹ Horvitz, 2022.

²² Spitale et al., 2023.

²³ Christiano, 2022; Coeckelbergh, 2022.

²⁴ Christiano, 2022; Sunstein, 2016.

²⁵ Dommert, Barclay et Gibson 2024.

²⁶ Borgesius et al., 2018; Caron, 2023; Kreiss, 2017; Lavigne, 2022.

à rendre l'offre des partis plus inclusive et plus représentative de la population.²⁷ Aux États-Unis, ces techniques sont omniprésentes dans les campagnes présidentielles depuis 2004 et, au Canada, elles le sont depuis 2006 dans les campagnes fédérales.²⁸ Elles le sont aussi dans les campagnes électorales au Québec depuis au moins 2018.²⁹

Cependant, cette pratique soulève plusieurs préoccupations quant à ses impacts sur la démocratie. Premièrement, le microciblage peut entraîner une distorsion de la sphère publique en rendant invisibles certains aspects des programmes politiques à différents segments d'électeurs.³⁰ En personnalisant les messages pour correspondre aux préférences individuelles, les partis politiques peuvent limiter la diversité des informations accessibles à tous, ce qui compromet la qualité du débat public et la transparence.

Deuxièmement, le microciblage peut fragmenter le débat politique en polarisant les électeurs et en renforçant leurs positions existantes. En voyant des messages qui confortent les croyances et les valeurs des individus, cette stratégie peut renforcer les chambres d'écho et les bulles de filtres, qui sont elles-mêmes déjà fortement encouragées par les algorithmes de recommandation de contenus sur les plateformes en ligne.³¹ Dans cette situation, seules les opinions similaires sont renforcées, ce qui réduit la possibilité d'un débat démocratique robuste et inclusif.

Troisièmement, le microciblage risque d'accentuer les inégalités de participation liées à la fracture numérique en concentrant les ressources des partis politiques sur des segments spécifiques d'électeurs. Les électeurs qui produisent moins de données se retrouvent moins bien représentés dans l'offre des partis politiques taillée sur mesure pour certains profils constitués à partir de données numériques. Les électeurs moins ciblés peuvent avoir moins d'accès à l'information et moins d'incitations à participer politiquement, ce qui crée un déséquilibre dans le processus démocratique et nuit à l'égalité de participation.

Enfin, si l'on situe le microciblage dans le cadre plus large des campagnes alimentées par les données (*data-driven campaigns*)³², on peut redouter que cette forme de communication politique réduise en quelque sorte l'électeur à un rôle passif dans lequel il est perçu comme une simple source de données qu'on peut étudier afin de mieux l'influencer.

On doit finalement reconnaître que certains chercheurs avancent qu'il faut nuancer cette vision plutôt sombre des campagnes alimentées par les données massives.³³ Ils suggèrent que ces pratiques sont beaucoup plus utiles pour mobiliser l'action, comme faire sortir le vote et améliorer les taux de dons, que pour atteindre des objectifs persuasifs, comme amener quelqu'un à soutenir un candidat. À la différence, d'autres avancent que, tout comme la désinformation, le microciblage peut constituer une forme de manipulation qui

²⁷ Pour des discussions critiques sur l'efficacité du microciblage politique, voir Gorton, 2016; Tappin et al., 2023.

²⁸ Caron 2023.

²⁹ Montigny, Dubois et Giasson, 2019.

³⁰ Gorton 2016.

³¹ Arguedas et al. 2022, Nguyen 2020.

³² Dommet Barclay et Gibson 2024.

³³ Voir notamment Baldwin-Philippi 2019.

constitue une entrave à l'autonomie. Ils soutiennent que le microciblage et l'offre de contenus adaptés aux profils personnels peuvent être si efficaces qu'ils constituent une forme d' « *hypernudging* », notamment lorsque le ciblage est constamment réactualisé en fonction de l'activité des usagers d'outils numériques³⁴. Dans cette optique, le manque de transparence dans les pratiques de microciblage est particulièrement problématique. L'électeur qui ignore qu'il reçoit des communications politiques ciblées et selon quels critères il est ciblé peut en effet être influencé de manière insidieuse.

³⁴ La notion de « *nudge* », issue de l'économie comportementale, réfère à des interventions sur l'architecture des choix qui s'offrent aux personnes (la manière dont différentes options leur sont présentées) qui visent à orienter la conduite de celles-ci sans recourir à la coercition et sans imposer de pénalités (Thaler & Sunstein, 2008). Un site web, par exemple, peut organiser le contenu qu'il présente de sorte à promouvoir un comportement (ne pas quitter le site web sans y faire d'achat, par exemple), de la même manière qu'un supermarché peut choisir l'emplacement physique de certains items de sorte à rendre plus probable leur achat par des consommateurs (en les plaçant à une certaine hauteur sur les étagères, ou près des caisses, etc.). Il s'agit donc d'une forme « douce » de contrôle et d'influence basée sur la conception de l'architecture de choix qui modifie le comportement des gens de manière prévisible sans interdire aucune option ni modifier de manière significative leurs incitations économiques. Certains avancent qu'avec l'analyse des données massives, il est possible de considérablement raffiner ces techniques pour les rendre extrêmement puissantes, d'où la notion de « *hypernudge* »; c'est notamment le cas dans les environnements numériques où les *nudges* sont omniprésents et où il est possible de collecter des données en continu et de recalibrer en continu le message ou le contenu présenté à l'utilisateur. Voir Christiano 2022; Morozovaité 2024.

2. L'accès au vote et le droit de se présenter aux élections. Commentaire sur les chapitres 1 et 2

Dans les chapitres 1 et 2 de son document de réflexion, *Pour une nouvelle vision de la loi électorale*, Élections Québec s'intéresse à l'accès au vote et au droit à se présenter à une élection. Dans le premier chapitre, il est question de l'égalité dans l'accès au vote ainsi que de l'intégrité du processus électoral, alors que le chapitre 2 aborde les conditions de l'égalité dans la diversité ainsi que la protection des droits politiques.

Bien que ces deux chapitres contiennent des éléments qui situent l'accès au vote et le droit de se présenter aux élections dans le cadre des grandes transformations numériques, la réflexion sur l'impact des nouvelles technologies d'information de communication sur ces deux enjeux nous semble pouvoir être davantage développée, de sorte à mieux prendre en compte les inégalités numériques de même que les bénéfices potentiels de l'IA ainsi que les risques qu'elle pose.

2.1 Accès au vote et fracture numérique

Le chapitre 1, sur l'accès au vote, fait notamment cette proposition :

Proposition 1

Convertir l'inscription et la modification de l'inscription sur la liste électorale en service numérique

Depuis l'entrée en vigueur de la Loi modifiant la Loi électorale, en 2022, les électrices et les électeurs peuvent faire une demande en ligne auprès de la commission de révision de leur circonscription pour s'inscrire ou pour modifier leur inscription sur la liste électorale en période électorale. Nous proposons de pousser ce changement plus loin afin que le processus d'inscription s'effectue principalement en ligne auprès d'Élections Québec³⁵.

S'il est vrai qu'une telle modification offre un fort potentiel inclusif en facilitant l'inscription et la modification de l'inscription sur la liste électorale, il ne faut pas négliger la prise en compte de la fracture numérique et les inégalités d'accès aux technologies numériques. Certains citoyens ont une littéracie numérique plutôt faible de même qu'un accès restreint aux outils numériques (ordinateur, connexion internet, etc.). D'une manière générale, ce sont surtout les personnes connectées qui bénéficient des opportunités offertes par les solutions numériques et la transition numérique tend à délaisser les personnes se situant involontairement de l'autre côté du fossé numérique. Par ailleurs, ceci peut créer une pression sur des personnes qui souhaitent, de manière tout à fait légitime, mener une existence moins connectée et moins dépendante des technologies de l'information. S'il devient nécessaire d'utiliser des objets connectés ou de partager des données personnelles afin de bénéficier de services publics ou afin de participer à la vie publique, ces pressions

³⁵ Élections Québec 2023, 20.

peuvent s'apparenter à une forme de discrimination désavantageant certains modes de vie légitimes. D'ailleurs, dans sa *Stratégie de Transformation Numérique Gouvernementale 2019-2023*, le gouvernement du Québec reconnaît l'importance de prendre ce point en considération : « (...) bien qu'une part grandissante de la population utilise le numérique au quotidien, il est primordial de tenir compte des personnes qui, par choix ou en raison de contraintes, interagissent avec l'administration publique par des modes plus traditionnels, comme le téléphone ou le point de service »³⁶. Dans son rapport *Prêt pour l'IA*, le CIQ va dans le même sens et affirme : « Personne ne devrait être exclu parce qu'il maîtrise mal le numérique. Le gouvernement du Québec doit donc s'assurer de mettre en place des mesures qui permettent à chaque citoyen de s'informer, de voter, de délibérer et de contester le pouvoir au Québec sans avoir à interagir avec des systèmes d'IA ou des plateformes numériques »³⁷.

Dans de telles circonstances, il importe de reconnaître un droit à la non-connexion et de s'assurer que les électeurs disposent d'avenues non numériques accessibles et de qualité pour s'inscrire ou modifier leur inscription sur la liste électorale. La CEST a d'ailleurs fait la recommandation suivante dans le cadre de la consultation sur l'encadrement de l'IA au Québec orchestré par le CIQ :

Droit à la non-connexion

31. Il est recommandé au gouvernement du Québec d'adopter des mesures pour s'assurer qu'il soit possible pour tous les citoyens de voter, délibérer et contester sans avoir à interagir avec des SIA et des plateformes numériques. En particulier, il est recommandé :

31.1 De maintenir et soutenir des canaux d'information traditionnels pour la diffusion d'informations relatives aux élections.³⁸

2.2 IA et accès au vote

Élections Québec demande « comment rendre le vote encore plus accessible à toutes les électrices et à tous les électeurs sans compromettre l'intégrité du processus électoral? » et « comment mettre à profit les possibilités qu'offrent les technologies dans ce domaine tout en tenant compte des risques qui leur sont associés? »

Face à ces questions, il serait intéressant d'examiner dans quelle mesure des systèmes d'IA pourraient favoriser l'accès au vote. Certains commentateurs soulignent que des outils alimentés par l'IA pourraient aider à augmenter le taux de participation aux élections. Depuis 2016, dans les élections présidentielles américaines, on a largement eu recours à des robots conversationnels, tels que HelloVote, pour solliciter, avec un certain succès, la participation électorale par le biais d'envois automatisés de rappels et d'information

³⁶ Secrétariat du Conseil du Trésor, 2019, 4.

³⁷ Conseil de l'Innovation du Québec, 2024, 41.

³⁸ CEIMIA, CEST et OBVIA, 2023.

relative aux modalités du vote (où voter, comment s’inscrire, etc.)³⁹. On peut raisonnablement s’attendre à ce que l’automatisation de ces efforts pour solliciter le vote, avec, par exemple, l’usage de robots conversationnels alimentés par de grands modèles de langage (*Large Language Models*), augmente l’efficacité de ces campagnes.⁴⁰

Toutefois, une mise en garde s’impose. D’une part, il convient de rappeler qu’à l’heure actuelle, les agents conversationnels artificiels alimentés par de grands modèles de langage ont tendance à fabuler et à fournir des informations fausses. Étant donné l’impact tout à fait capital que pourrait avoir une fausse information sur les modalités du vote pour un électeur, la fiabilité d’un tel agent conversationnel devrait être totale et il n’est pas clair que l’état actuel de la technologie nous permette d’avoir une telle confiance. Notons aussi que les grands modèles de langage qui alimentent les robots conversationnels collectent très souvent des « données de conversation » (à savoir, l’ensemble de ce que les utilisateurs écrivent ou disent en interagissant avec ces agents), ce qui peut soulever des enjeux de protection de la vie privée des électeurs.⁴¹

2.3 IA, égalité et droit de se présenter aux élections

Le harcèlement et l’intimidation peuvent faire obstacle au droit de se présenter comme candidat aux élections et cet obstacle a un effet disproportionné sur certains groupes sociaux, comme les femmes. Élections Québec reconnaît à juste titre cette triste réalité en faisant ce constat dans le chapitre 2 de *Pour une nouvelle vision de la Loi électorale* :

Constat no. 3

Des phénomènes comme le harcèlement, l’intimidation et les menaces envers les personnalités publiques, notamment les personnes candidates et les personnes élues, ont pris de l’ampleur au cours des dernières années. Ces comportements peuvent dissuader des citoyennes et des citoyens de présenter leur candidature. Les femmes et les personnes issues de la diversité sont plus susceptibles d’en être la cible.

Le harcèlement et l’intimidation ont une forte composante en ligne et plusieurs discours pouvant faire obstacle au droit de se présenter aux élections y circulent. De plus, les outils d’IA générative sont utilisés à de telles fins d’intimidation. En effet, une grande part des hypertrucages sont en réalité des hypertrucages non consensuels, bien souvent à caractère pornographique, et ceux-ci ciblent dans une vaste majorité de cas des femmes. Ce type d’hostilité en ligne à l’égard des femmes peut faire en sorte que certaines remettent en question leur participation à la vie publique.⁴²

Plusieurs États américains ont déjà légiféré pour interdire la publication de tels hypertrucages, c’est notamment le cas de la Virginie et de la Californie. Au Canada, le

³⁹ Scola 2016.

⁴⁰ Sanders 2023.

⁴¹ Sur les risques éthiques liés à l’usage de robots conversationnels, voir Cortés et al. 2023.

⁴² Moreau et Rourke 2024.

gouvernement fédéral considère aussi la possibilité d'adopter une législation contenant une interdiction similaire qui forcerait les plateformes numériques à retirer rapidement de tels hypertrucages. Le projet de loi 63, *Loi sur les méfaits en ligne*, déposé le 26 février 2024 à la Chambre des communes du Canada, contient en effet une disposition interdisant la diffusion de contenu à caractère sexuel non consenti, ce qui inclut les hypertrucages pornographiques réalisés sans consentement.

Il importe de souligner qu'une telle approche de la régulation des hypertrucages ne considère pas uniquement ce phénomène sous l'angle de la désinformation, elle considère aussi le préjudice subi par les victimes. Lorsque les hypertrucages sont uniquement abordés du point de vue de la désinformation, il n'est pas rare qu'une des pistes de solutions envisagées consiste simplement à identifier les contenus synthétiques comme tels, par exemple en leur apposant un filigrane (*watermark*), comme certaines plateformes numériques proposent déjà de le faire volontairement en vue des élections présidentielles américaines.⁴³ Or, cette mesure ne peut mitiger que la composante informationnelle des hypertrucages : elle remet les pendules à l'heure et informe l'électeur du caractère irréel des images, les protégeant ainsi contre la manipulation. Toutefois, l'entrave à la vie privée et la crainte d'être la prochaine victime, sur lesquelles se fonde le caractère dissuasif des hypertrucages pornographiques, restent intactes. En revanche, l'interdiction ciblée qu'on trouve dans le PL63 permet véritablement de protéger les femmes sans non plus bannir toute forme de contenu synthétique.

Dans le cadre de la réflexion sur la mise à jour de la loi électorale du Québec, il conviendrait de se demander si d'autres formes d'interdiction de diffusion de contenus synthétiques, ou d'autres mesures sont nécessaires pour mitiger les obstacles à l'entrée en politique d'autres groupes sociaux marginalisés, tels que les minorités culturelles et les minorités visibles. Il conviendrait aussi de se demander si le potentiel nocif des hypertrucages porte atteinte au droit de se présenter aux élections de tous les citoyens et citoyennes. Nous reviendrons sur ce point dans nos commentaires portant sur le chapitre 4.

⁴³ Voir : <https://about.fb.com/news/2023/11/how-meta-is-planning-for-elections-in-2024/>.

3. L'utilisation de l'IA et des données massives dans le cadre de l'information électorale et politique : commentaires sur le Chapitre 4 L'information électorale et politique

3.1 La mission d'information d'Élections Québec

Une saine démocratie implique que les citoyens et citoyennes votent de *manière éclairée*. Élection Québec, citant l'arrêt *Harper c. Canada*, reconnaît l'importance de voter de manière éclairée et en fait même une composante intégrale du droit de vote.⁴⁴ L'éducation à la démocratie joue un rôle important pour promouvoir cette capacité de voter de manière éclairée. Nous accueillons donc très favorablement l'idée que le système scolaire n'est pas le seul acteur devant prendre part à l'éducation à la démocratie et qu'Élection Québec a un rôle à jouer en la matière. Cette mission d'information et, plus largement, d'éducation civique, est une composante essentielle de la fonction de prévention du Directeur général des élections du Québec qui elle-même découle du rôle de gardien institutionnel du DGEQ. Nous accueillons aussi favorablement la proposition no. 1 du chapitre 4 de *Pour une nouvelle vision de la Loi électorale*, laquelle vise à étendre le mandat d'information d'Élections Québec en lui permettant d'informer le public sur les partis politiques, les personnes candidates et leur programme :

Proposition 1

Mettre à la disposition des électrices et des électeurs une vitrine d'information sur les personnes candidates ou les partis politiques

Comme les compétences informationnelles nécessaires pour participer de manière éclairée au processus électoral et à la vie démocratique se complexifient depuis l'arrivée des plateformes numériques et de l'IA, le rôle bonifié d'Élections Québec en matière d'information électorale pourrait aller encore plus loin qu'une mission d'informer sur les partis politiques et les personnes candidates. Une mise à jour de la fonction de prévention d'Élections Québec à l'ère du numérique et de l'IA générative pourrait, par exemple, consister à s'engager sur la voie de l'éducation à la cyber citoyenneté en faisant la promotion de la littéracie numérique et de la pensée critique.⁴⁵

La littéracie numérique se définit par la capacité d'une personne à trouver, comprendre, évaluer, utiliser et créer de l'information au moyen des technologies numériques. Elle comprend à la fois des compétences techniques et des habiletés dans le traitement de l'information et l'organisation des idées⁴⁶. La littéracie numérique inclut également la littéracie algorithmique. Celle-ci se traduit par la capacité des utilisateurs d'être conscients de la présence d'algorithmes dans l'environnement numérique, de comprendre leur

⁴⁴ Élections Québec, 2023, 94.

⁴⁵ D'une manière plus générale, la désinformation politique et électorale a aussi une dimension non numérique et indépendante des avancées en IA qui soulève des enjeux de prévention pouvant être abordés dans le cadre d'activités visant à promouvoir la pensée critique et certaines compétences informationnelles.

⁴⁶ Tinmaz *et al.* 2022.

fonctionnement puis d'être capables d'évaluer de manière critique la prise de décision et la génération de contenus par des algorithmes.

Le gouvernement du Québec reconnaît déjà l'importance de cultiver la littéracie numérique à travers le système d'éducation. Le *Plan d'action numérique en éducation et en enseignement supérieur* du gouvernement du Québec vise notamment à soutenir le développement des compétences numériques des étudiantes et étudiants tout au long de leur parcours éducatif. Les dimensions essentielles de la compétence numérique sont identifiées dans le Cadre de référence de la compétence numérique. Elles incluent entre autres le développement et la mobilisation d'habiletés technologiques (ex. s'approprier les nouvelles technologies; sécuriser ses données personnelles; développer une compréhension globale à l'égard de l'intelligence artificielle et de ses impacts) ainsi que le développement d'une culture personnelle informationnelle (ex. sélectionner et utiliser adéquatement l'information en tenant compte, par exemple, des bulles de filtres; faire preuve de jugement dans la détermination de la crédibilité et de la fiabilité des sources d'information et des contenus).

Outre la littéracie numérique, la pensée critique est essentielle pour renforcer l'autonomie des citoyens dans leurs rapports à l'information et pour voter de manière éclairée. En France, la Commission Bronner, qui avait le mandat de « mesurer et comprendre les dangers que le numérique fait peser sur la cohésion nationale et la démocratie afin de mieux y faire face », a produit un rapport intitulé *Les Lumières à l'ère numérique* qui met fortement de l'avant l'idée que le développement de la pensée critique est un des principaux remèdes aux problèmes de la désinformation et de la mésinformation. Le rapport définit la pensée critique comme « la capacité à évaluer correctement les contenus et les sources des informations à notre disposition afin de mieux juger, mieux raisonner, ou prendre de meilleures décisions »⁴⁷. Or, certains biais cognitifs et inclinaisons de l'esprit humain peuvent être exploités ou amplifiés par l'IA de manière à entraîner des erreurs de raisonnement ou l'adhésion à de fausses informations. Par exemple, la tendance à tenir pour vraies des informations répétées fréquemment (effet de répétition) ou encore celles nous portant à privilégier les informations qui confirment nos idées préconçues et convictions (biais de confirmation/validation) peuvent être amplifiées par les algorithmes de recommandation et les phénomènes de chambres d'écho et de bulles de filtre en ligne.

L'éducation à la pensée critique et à la littéracie numérique est propre à sensibiliser les individus à leurs propres biais cognitifs, à la manière dont ceux-ci sont amplifiés sur les plateformes numériques et à mieux identifier les fausses informations⁴⁸. Elle permet une forme de capacitation (*empowerment*) des citoyens qui leur permet de voter de manière éclairée dans un contexte marqué par la centralité des plateformes numériques pour la

⁴⁷ Bronner 2022 : 90.

⁴⁸ Certaines études empiriques démontrent par exemple que ceux qui ont un niveau de littéracie numérique plus élevé ont moins tendance à partager de fausses nouvelles. Voir Ali 2022.

circulation de l'information et le développement rapide de l'IA générative qui transforme les formes de communication en ligne.⁴⁹

Ainsi, une vitrine d'information politique, ou un ensemble de campagnes de sensibilisation en période électorale pourraient, par exemple, inclure des informations sur :

- Les phénomènes de bulles de filtres et de chambres d'écho en ligne
- La manière dont les biais cognitifs amplifient le potentiel de mésinformation de ces phénomènes en ligne
- L'utilisation de l'IA générative pour produire de faux contenus sous forme d'image, de vidéo ou de faux enregistrements audio qui clonent la voix de personnes (hypertrucages)
- La manière dont les partis politiques ont recours aux données massives pour effectuer, notamment, du microciblage.

3.2 Encadrer l'utilisation de l'IA générative dans l'information politique et électorale

Dans un contexte où l'usage de l'intelligence artificielle (IA) prend de l'ampleur dans les communications politiques, il est impératif d'établir des obligations de transparence pour garantir l'intégrité du processus démocratique. Nous supportons ainsi fortement les propositions 2 et 3 du chapitre 4 de *Pour une nouvelle vision de la Loi électorale* :

Proposition 2

Envisager la création d'obligations destinées aux plateformes numériques en matière de transparence et de respect de la Loi électorale

Proposition 3

Accroître la transparence des communications à caractère politique et encadrer l'utilisation de certaines pratiques en ligne

Nous nous accordons aussi avec l'analyse d'Élections Québec qui identifie deux usages de l'IA qui soulèvent des risques pour la démocratie : l'usage de robots conversationnels pour amplifier certains messages et l'usage de l'IA générative pour créer des hypertrucages visant à discréditer des élus ou des personnes candidates ou à détourner l'issue d'une élection. Nous soulignons aussi la justesse de l'analyse des mesures d'encadrement proposées par Élections Québec. Cette analyse distingue à juste titre, d'une part, une approche fondée sur la transparence, laquelle exige d'informer l'électeur qu'il est en

⁴⁹ CEST 2023.

présence d'un système d'IA et, d'autre part, une approche qui s'appuie sur l'interdiction de certaines pratiques.

La CEST est d'avis que les obligations de transparence relatives à l'usage de l'IA dans l'information électorale et politique représentent des obligations minimales nécessaires pour protéger l'autonomie des électeurs et garantir leur droit de voter en toute connaissance de cause. Ainsi, nous supportons fortement l'idée proposée par Élections Québec de s'inspirer de la Colombie-Britannique pour exiger que « les comptes de médias sociaux automatisés qui diffusent de la publicité électorale divulguent leur nature automatisée de manière claire. » De même, nous estimons que le Québec pourrait s'inspirer de l'article 52 de la Législation sur l'Intelligence artificielle de l'Union européenne (*EU AI Act*), lequel exige la divulgation de l'utilisation d'IA générative dans la conception de publicités politiques, qu'il s'agisse de la production d'images, de vidéos ou de contenus audio. Ces obligations de transparence pourraient, dans l'optique où l'État québécois dispose de plus de leviers pour s'assurer que ces entités respectent la loi qu'il n'en a face aux géants des nouvelles technologies localisés à l'étranger, être directement imposées aux partis politiques, mais idéalement elles devraient pouvoir s'appliquer aux plateformes en ligne de sorte à encadrer tous les acteurs produisant de l'information politique et électorale.

Cependant, on constate que certaines voix s'élèvent pour remettre en question la suffisance des obligations de transparence axées sur la divulgation du caractère synthétique des contenus en ligne⁵⁰. En effet, les risques de désinformation associés aux hypertrucages et à l'utilisation malveillante des robots conversationnels pour amplifier certains messages mettent en lumière les limites de ces mesures. On peut par exemple penser qu'elles auraient peu d'effet sur les personnes dont la littéracie numérique est peu développée (celles-ci pourraient par exemple ignorer la signification d'un filagramme visant à identifier un contenu synthétique⁵¹). Cette insuffisance devient particulièrement évidente lorsqu'on considère les préjudices personnels pouvant résulter de certains hypertrucages, notamment ceux à caractère pornographique. Ainsi, certaines juridictions, dont plusieurs États américains, ont déjà légiféré, ou envisagent de légiférer, de sorte, par exemple, à interdire la diffusion d'hypertrucages en temps de campagne électorale ou à interdire la diffusion d'hypertrucages malicieux qui portent atteinte aux droits de certaines personnes⁵².

Face à ces défis, il est nécessaire d'envisager des mesures allant au-delà de la simple transparence, tout en évitant de porter atteinte à la liberté d'expression. Une approche prometteuse consisterait à introduire des interdictions ciblées, de portée limitée ou accompagnées d'exemptions spécifiques pour préserver des formes légitimes d'expression artistique, journalistique et humoristique usant de l'IA générative et s'assurer de minimiser l'impact de la régulation sur les droits. Si, en droit canadien, l'objectif de préserver l'intégrité du processus électoral peut être considéré comme étant suffisamment important pour justifier certaines restrictions aux droits inscrits dans la *Charte canadienne des droits et libertés* (et dans la *Charte des droits et libertés de la personne du Québec*), encore faut-

⁵⁰ Van der Sloot et Wagensfeld 2022, Gandhi 2024.

⁵¹ Weiner et Norden 2023.

⁵² Voir Lawson 2023, Holistic AI 2024.

il pouvoir établir que les mesures prises pour atteindre cet objectif sont proportionnelles.⁵³ Ceci implique, entre autres, de démontrer que ces mesures permettent de poursuivre l'objectif en question en portant une atteinte minimale aux droits (aucune autre mesure ne permet d'atteindre cet objectif tout en constituant une moindre restriction aux droits). Voici quelques modalités à considérer pour limiter la portée de telles interdictions et s'assurer qu'elles représentent des atteintes minimales.

- Interdiction avec exemption prévue dans la loi pour la satire et l'humour: toute interdiction devrait explicitement inclure une exemption ciblant les médias et les artistes pour que ceux-ci puissent produire et diffuser des contenus satiriques et humoristiques synthétiquement générés, préservant ainsi la liberté d'expression dans les arts et les pratiques journalistiques.⁵⁴ En général, les lois interdisant la production et la dissémination d'hypertrucages mises en place par différents États américains depuis quelques années contiennent de telles exemptions explicites et assez larges (et elles continuent néanmoins d'inquiéter certains observateurs comme la American Civil Liberties Union, ACLU).⁵⁵
- Interdiction des hypertrucages malveillants: Une interdiction spécifique pourrait viser les hypertrucages ayant pour dessein de nuire à des élus ou des candidats, ou de détourner insidieusement l'issue d'une élection. C'est une des routes empruntées par certaines chambres législatives américaines qui ont (en partie) banni les hypertrucages.⁵⁶ Une telle interdiction pourrait aussi cibler l'usage de robots conversationnels en vue d'amplifier des points de vue, des fausses informations électorales et politiques ou tout simplement de gonfler artificiellement la popularité des élus et des personnes candidates.⁵⁷
- Interdiction ciblant des usages spécifiques de l'IA générative: Des interdictions pourraient être établies pour certains usages spécifiques de l'IA générative, tels que

⁵³ Au sens établi dans l'arrêt de la Cour Suprême *R. c. Oakes*, [1986] 1 R.C.S. 103.

⁵⁴ Voir par exemple *Weiner et Norden 2023*.

⁵⁵ *Ibid.*

⁵⁶ C'est notamment le cas de la Californie qui a banni l'usage de tels hypertrucages malicieux ciblant les personnes candidates en période de campagne électorale (60 jours avant l'élection). C'est aussi le cas de législations qui ne visent pas spécifiquement à sécuriser les élections, comme le *Malicious Deep Fake Prohibition Act* de 2018 du Congrès américain et du Projet de loi 63 sur les méfaits en ligne, déposé à la chambre des communes d'Ottawa.

⁵⁷ Il faut ici noter que ce type d'interdiction ciblée repose parfois sur une distinction entre, d'un côté, les torts, disons, « directs » qui suivent un schéma clair et simple de responsabilité criminelle : un acteur bien identifiable pose une action qui nuit à un acteur (ou un groupe) bien identifié (par exemple : une personne candidate diffuse un hypertrucage qui porte sévèrement atteinte à la réputation d'une autre personne candidate); et, de l'autre côté, des torts qu'on pourrait qualifier de « structurels », lesquels résultent du cumul de plusieurs actions posées par différents acteurs qui se combinent pour produire un effet macro sur les conditions sociales facilitant ou compliquant la poursuite de certains biens collectifs, tels que l'accès à un environnement informationnel fiable. L'idée est ainsi que les préjudices individuels sont plus graves (ils affectent directement des personnes et non pas des processus sociaux) ou que la responsabilité pour les torts structurels est plus difficile à établir étant donné leur caractère cumulatif et diffus, de sorte que les prohibitions ancrées dans le droit criminel ne sont appropriées que pour les premiers.

la création d'agents conversationnels ayant cloné la voix de personnes sans leur consentement.⁵⁸ Les États-Unis ont rapidement emprunté cette voie après un incident impliquant des appels automatisés qui utilisaient la voix clonée de Joe Biden.

- Interdiction pour les partis politiques: Une interdiction spécifique pourrait être imposée aux partis politiques, limitant leur recours aux robots conversationnels et à l'IA générative dans leurs communications politiques (en période électorale). Bien que cette avenue ait le désavantage de ne cibler qu'une partie des acteurs qui peuvent produire et faire circuler de la désinformation, elle a un avantage non négligeable qu'il convient de considérer. Celle-ci pourrait en effet se justifier du point de vue des obligations et responsabilités spéciales qui découlent du rôle d'élus en démocratie ou encore du rôle des partis politiques. Cette justification part d'une distinction entre les responsabilités générales qui incombent à toute personne en raison de sa simple humanité ou de sa qualité d'agent moral (devoir de ne pas nuire à autrui) et les responsabilités spéciales qui découlent d'un acte spécifique (une promesse) ou d'une relation spécifique (comme l'asymétrie de pouvoir entre un professionnel, comme un médecin, et le public). On pourrait ainsi exiger des personnes candidates qu'elles soient particulièrement dévouées à l'égard de l'idéal démocratique et soucieuses de préserver un environnement informationnel sain. Comme certains professionnels suivent, dans le cadre de leurs fonctions, des normes plus serrées qui ne s'appliquent pas aux autres membres de la société (comme le devoir de confidentialité des médecins et avocats), on pourrait demander aux élus, dont on estime déjà qu'ils occupent une position particulière justifiant l'imposition d'obligations spéciales qui vont au-delà des obligations générales (en matière de divulgation des conflits d'intérêts, par exemple), d'observer des normes plus strictes régissant leurs communications en ligne et leur usage de l'IA.
- Interdiction générale en période électorale: en période de campagne électorale ou dans une période déterminée précédant une élection (les États américains empruntant cette voie oscillent entre 60 jours, à l'instar de la Californie, et 90 jours, à l'instar du Minnesota)⁵⁹, une interdiction générale, ou ciblant les partis, de recourir à des hypertrucages ou des robots conversationnels dans les communications politiques pourrait être mise en place pour prévenir toute manipulation de l'opinion publique. Il est fort douteux que la circulation d'un hypertrucage, ou que l'amplification d'un message, 3 ans avant une élection ait une forte incidence sur l'issue de celle-ci. Du point de vue de la proportionnalité, une

⁵⁸ Voir les règles adoptées par la Federal Communications Commission suite à un incident d'appels automatisés ayant cloné la voix de Joe Biden plus tôt en 2024, <https://www.fcc.gov/document/fcc-makes-ai-generated-voices-robocalls-illegal>.

⁵⁹ Pour le Minnesota, voir : <https://www.cbsnews.com/minnesota/news/new-minnesota-law-regulates-deepfakes-to-curb-influence-on-elections/>; pour la législation californienne, voir <https://legiscan.com/CA/bill/AB730/2019>

interdiction non ciblée dans le temps de l'usage de l'IA générative risquerait fortement de ne pas respecter le critère d'atteinte minimale.

Notons que des pistes de solutions de nature informationnelle pourraient aussi être poursuivies. Élections Québec pourrait tenir un registre en ligne des incidents impliquant des hypertrucages ou des agents conversationnels artificiels pour amplifier des messages. Les États-Unis ont établi un tel protocole en vue de sécuriser les élections présidentielles de 2024.⁶⁰ Il pourrait aussi se doter d'une obligation de documenter de tels incidents dans des rapports postélectorales, en s'inspirant notamment d'Élections Canada. On pourrait également envisager la création d'une cellule de veille visant à détecter des incidents où l'IA est utilisée d'une manière qui remet en question l'intégrité d'une élection. Le Canada s'est notamment doté d'une telle structure, le Protocole public en cas d'incident électoral majeur. Celle-ci vise surtout à se protéger des influences étrangères, une menace qu'on peut penser moins présente à l'échelle provinciale, mais à laquelle il convient néanmoins d'être attentif.

3.3 Mieux encadrer les pratiques de microciblage

Comme on l'a vu dans la première section de ce document, le microciblage peut entraîner une distorsion de la sphère publique en rendant invisibles certains aspects des programmes politiques à différents segments d'électeurs, fragmenter le débat politique en polarisant les électeurs et en renforçant leurs positions existantes, accentuer les inégalités de participation liées à la fracture numérique et contribuer à renforcer une vision passive de l'électorat. Pour ces raisons, nous accueillons très favorablement la proposition qu'Élections Québec fait relativement à l'imposition d'obligations de transparence dans les communications politiques en ligne :

Exiger des plateformes numériques qu'elles répertorient les publicités relatives aux élections dans un registre⁶¹

Il serait par ailleurs tout à fait adéquat d'exiger, comme le suggère Élections Québec, que les plateformes divulguent aussi les critères de microciblage utilisés pour diffuser les publicités. De telles mesures sont un minimum nécessaire pour assurer aux électeurs d'avoir un portrait global de ce que disent les partis politiques et de la manière dont ceux-ci utilisent des stratégies visant à influencer leur vote. Notons toutefois qu'il s'agit là aussi de mesures de transparence et que des mesures plus fortes pourraient être envisagées pour limiter les pratiques de microciblage, comme certains le proposent maintenant dans le cadre de l'Union européenne.⁶² L'argument en faveur de telles mesures d'encadrement du microciblage plus fortes que les exigences de transparence n'est toutefois pas identique à

⁶⁰ Gandhi 2024.

⁶¹ Élections Québec 2023, 111.

⁶² Voir <https://www.europarl.europa.eu/topics/fr/article/20230202STO71504/l-importance-des-nouvelles-regles-de-l-ue-en-matiere-de-publicite-politique>.

l'argument qui vise à établir une conclusion analogue par rapport au cas de l'utilisation de l'IA générative en contexte électoral.

Tout d'abord, on peut estimer que les hypertrucages ont le potentiel de flouer une partie de l'électorat au point tel qu'ils peuvent directement porter atteinte à leur droit à voter de manière éclairée. Il n'est cependant pas clair que le microciblage porte directement atteinte à la capacité de voter d'une manière éclairée. Plusieurs articles scientifiques et tribunes dans les journaux et magazines soulignent l'effet de fragmentation du microciblage, ou encore sa contribution au renforcement des chambres d'écho et bulles de filtres.⁶³ Par contre, comme on l'a vu, ceux qui estiment que cette forme de publicité a le potentiel d'influencer le public d'une manière insidieuse qui minerait l'autonomie parlent d'une forme poussée à l'extrême de marketing personnalisé. Celle-ci impliquerait par exemple une technique d'hypernudging qui consiste à collecter des données en continu de sorte à constamment réajuster l'architecture de choix qui est présenté aux destinataires de publicités. Dans le domaine du marketing politique, il faudrait imaginer un parti qui, par exemple, suit les lectures, les écoutes et les visionnements d'un électeur, de même que ses publications sur les médias sociaux, afin de réagir en temps réel par l'envoi de messages adaptés aux activités d'information et d'expression de cet électeur (par exemple, en s'assurant qu'il reçoive un contre-discours, taillé sur mesure en fonction de son profil, chaque fois qu'il est exposé aux opinions contradictoires d'un autre parti). Il n'est pas du tout clair que les partis politiques aient atteint ce niveau intensif de ciblage, du moins ce n'est pas la conclusion qui se dégage des études empiriques existantes qui nuancent l'efficacité de ces pratiques.⁶⁴

Cela ne veut toutefois pas dire que le microciblage n'implique que des risques liés à la qualité de l'environnement informationnel sans comporter de risques de préjudices personnels et d'atteintes aux droits. En effet, lorsqu'elles sont non réglementées, ces pratiques font peser des risques importants sur la protection de la vie privée étant donné l'ampleur des données collectées et le fait que les pratiques de collecte des données des partis sont mal connues, notamment lorsqu'elles impliquent des méthodes indirectes, comme l'achat de données ou bien la production de données inférées.⁶⁵

Les travaux de la CEST qui abordent la question de la protection de la vie privée fondent celle-ci sur la valeur de l'autonomie informationnelle, laquelle implique que chaque personne « doit se voir reconnaître un droit non absolu, mais étendu de décider quels sont les aspects de sa vie privée qu'elle souhaite partager et dans quelles circonstances. Par exemple, une personne peut vouloir que certaines informations la concernant demeurent confidentielles.⁶⁶ » Bien que ce droit soit non absolu, les pratiques qui l'entravent doivent, pour être légitimes, servir des intérêts importants et passer le même test de proportionnalité qui s'applique, comme on l'a vu, à la restriction de la liberté d'expression et des autres droits et libertés fondamentaux. Or, il est douteux que l'objectif de protéger une technique

⁶³ Lavigne 2022, Caron 2023, Gorton 2016.

⁶⁴ Baldwin-Philippi 2019.

⁶⁵ Dommett, Barclay et Gibson 2024.

⁶⁶ CEST 2022, 14.

de marketing politique qui mine les conditions sociales et informationnelles qui rendent possible l'exercice du vote de manière éclairée en vienne à être considéré comme un objectif législatif « dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique ⁶⁷ ». Une des raisons d'opter pour de telles mesures est que la tenue de registres de publicités sur les plateformes n'a d'effet que sur les citoyens qui ont de bonnes compétences informationnelles et numériques et qui savent comment (et prennent le temps de) naviguer d'une plateforme à l'autre pour consulter les différents registres propres à chacune d'elles. Certains ont par ailleurs proposé des mesures de transparence qui pourraient être plus efficaces : on pourrait exiger que les partis politiques eux-mêmes tiennent des registres de leurs publicités et de leurs critères de microciblage. La principale objection à cette solution est qu'elle pourrait être trop difficile à appliquer pour les petits partis politiques. On pourrait toutefois octroyer une exemption pour ces petits partis (ceux qui ne rencontrent pas les seuils minimums pour obtenir du financement, par exemple) sans que cela ne remette en question l'efficacité d'un tel régime (à eux seuls, on peut douter qu'ils aient la capacité de distordre le processus électoral via leur usage de publicités ciblées). Bien que cette solution simplifierait la tâche des citoyens désireux de mieux comprendre comment les partis communiquent avec l'électorat, elle mise encore sur la compétence numérique des citoyens, d'où l'importance de combiner de telles mesures avec des efforts d'éducation à la citoyenneté numérique.

Plutôt que de miser uniquement sur la responsabilisation des citoyens, il serait intéressant de poursuivre les efforts pour directement s'attaquer aux pratiques de collecte de données des partis politiques. Comme c'est l'analyse de données massives sur les électeurs qui rend possible le microciblage, des mesures limitant la capacité des partis politiques de collecter divers types de données, limitations qui n'incluent pas uniquement les renseignements personnels, s'attaqueraient plus directement à la source du problème. Ainsi, nous soutenons les efforts qu'Élections Québec fait depuis plusieurs années pour mieux protéger les données personnelles des électeurs.⁶⁸

⁶⁷ Article 1 de la Charte des droits et libertés canadienne, lequel balise les limitations légitimes des droits.

⁶⁸ Voir notamment Élections Québec 2023, 119.

4. Enjeux de gouvernance électorale. Commentaires sur le chapitre 5

En tant que gardien institutionnel, Élections Québec doit promouvoir et assurer l'intégrité du processus électoral, l'équité de ce processus ainsi que sa transparence. Ce rôle de gardien vient donc avec des responsabilités en matière de prévention d'incidents et d'activités qui remettent en cause ces principes fondamentaux, de surveillance et de détection de tels incidents et activités ainsi que de répression de tels incidents et activités. Dans cette section, nous discutons de certaines réformes en matière de gouvernance électorale visant à assurer ce rôle de gardien institutionnel doté de responsabilités de prévention, détection et répression à l'ère de l'utilisation des technologies numériques et de l'IA dans le cadre des élections et de la circulation de l'information politique et électorale.

4.1 Révision périodique de la Loi électorale

Les transformations des communications et de l'information entraînées par la montée des plateformes en ligne et le déploiement de l'IA sont profondes, mais elles sont également très rapides. Depuis quelques années, plusieurs gouvernements se sont engagés sur la voie de la régulation de l'IA dans tous les domaines d'activités, une tendance qui a explosé en 2023. Le CIQ, dans son rapport *Prêt pour l'IA* sur l'encadrement de l'IA au Québec, va aussi dans ce sens. Étant donné la rapidité de ces changements et l'imprévisibilité des lois qui seront nécessaires pour faire face à d'autres développements technologiques, nous sommes fortement d'accord avec la proposition 1 du chapitre 5 de *Pour une nouvelle vision de la Loi électorale* :

Proposition 1

Prévoir un processus de révision périodique de la Loi électorale

Pour favoriser la délibération et la prise de décision éclairée par l'Assemblée nationale et, d'une manière plus générale, le public québécois, ainsi que pour promouvoir la transparence concernant les risques éthiques liés au numérique et à l'IA en contexte électoral et les initiatives prises par le gouvernement du Québec et plus spécifiquement par Élections Québec, ce processus de révision périodique de la loi pourrait être articulé à une exigence qu'Élections Québec publie les résultats de ses activités de surveillance d'incidents et activités liés aux risques éthiques posés par le numérique et l'IA, par exemple en tenant un registre de ces incidents ou en les incluant dans des rapports post-électorales.⁶⁹

⁶⁹ Élections Canada a par exemple diffusé de tels rapports abordant certains aspects des risques éthiques liés à l'environnement informationnel. Voir Élections Canada 2022. Au Québec, des chercheurs de l'Observatoire de l'écosystème médiatique, du Centre pour les médias, la technologie et la démocratie de l'Université McGill et du Centre d'études sur les médias de l'Université Laval ont produit un rapport plus ciblé sur la désinformation dans la dernière élection provinciale québécoise, voir Lavigne et al. 2022.

4.2 Renforcer les capacités d'Élections Québec en incluant des experts de l'IA et du numérique dans différents comités visant à épauler Élections Québec

Ces dernières années, les démocraties occidentales ont été confrontées à une montée significative des opérations d'influence, qu'elles proviennent du pays ou de l'étranger, cherchant à manipuler les résultats des élections. L'usage croissant de l'intelligence artificielle dans ces campagnes se manifeste à travers une gamme diversifiée de stratagèmes, allant de la diffusion de fausses informations via des hypertrucages à l'utilisation de robots conversationnels et de faux comptes sur les réseaux sociaux pour promouvoir des causes spécifiques ou submerger les canaux de communication de messages préconçus. Cette menace est prise très au sérieux par de nombreux États. Par exemple, le gouvernement fédéral du Canada a mis en place un protocole pour faire face à d'éventuels incidents électoraux majeurs. Bien que la menace d'ingérence étrangère soit moins prononcée au Québec, les élections de 2022 ont révélé que des acteurs nationaux tentaient de propager de fausses informations sur le processus électoral. L'intelligence artificielle offre un potentiel redoutable pour renforcer l'impact, l'efficacité et l'accessibilité de ces campagnes d'influence. Pour contrer cette menace, Élections Québec mène une surveillance active des médias pendant les campagnes électorales, mais ses ressources limitées rendent nécessaire une mise à jour constante des connaissances sur les opérations d'influence automatisées, compte tenu de l'évolution rapide des technologies. Pour ces raisons la CEST a fait les recommandations suivantes dans son rapport remis au CIQ dans le cadre de la réflexion collective sur l'encadrement de l'IA :

1. Il est recommandé au gouvernement du Québec de renforcer les capacités d'Élections Québec en matière de détection d'ingérence électorale assistée par l'IA et d'opérations d'influence alimentées par l'IA.
2. Il est recommandé au gouvernement du Québec de créer un comité interdisciplinaire d'experts en IA visant à soutenir Élections Québec dans ses efforts de détection de l'ingérence dans le processus électoral.⁷⁰

Ces recommandations ont largement été reprises par le CIQ dans son rapport *Prêt pour l'IA*, lequel affirme :

En résumé, le Conseil encourage le gouvernement du Québec à renforcer la capacité d'Élections Québec pour :

- étudier les impacts de l'IA sur l'intégrité du processus électoral québécois et sur la participation des citoyens aux élections;
- protéger la vitalité de la démocratie québécoise contre les effets néfastes de certains usages de l'IA;

⁷⁰ CEST, OBVIA, CEIMIA 2023b.

- explorer comment l’IA pourrait éventuellement servir à bonifier et soutenir la délibération démocratique.

Il encourage aussi l’État à mettre sur pied un comité interdisciplinaire pour appuyer Élections Québec dans ses travaux (RC-7).⁷¹

Dans ce sens, nous soutenons la proposition 3 du chapitre 5 de *Pour une nouvelle vision de la Loi électorale* :

Proposition 3

Revoir la portée du mandat et la composition du comité consultatif

Le comité consultatif pourrait ainsi inclure des experts en IA et en médias numériques indépendants des partis politiques et provenant de la société civile de façon à faire en sorte que ce comité assume aussi un rôle de consultation sur les enjeux soulevés par le rôle de l’IA et des plateformes numériques dans la circulation de l’information électorale et politique, notamment sur les risques que posent ces technologies pour l’intégrité du processus électoral. Nous recommandons une inclusion des experts dans la composition du comité consultatif afin également d’assurer des discussions éclairées avec les représentants des partis politiques, déjà membres du comité consultatif, sur ces questions importantes pour la vitalité et l’intégrité de nos processus électoraux.

Par ailleurs, comme nous l’avons soulevé précédemment, il serait aussi intéressant de se pencher sur la possibilité de créer un comité réunissant plusieurs acteurs et visant à effectuer une veille pour détecter des incidents relatifs à la désinformation assistée par l’IA, informer Élections Québec et suggérer des pistes de solutions. Une telle structure pourrait s’inspirer du Protocole public en cas d’incident électoral majeur.

Afin de promouvoir la confiance du public, d’assurer la transparence et de favoriser la délibération au sein de l’Assemblée nationale et de la population québécoise, il conviendrait que des travaux portant sur la surveillance, la détection et la répression d’incidents et d’activités utilisant de l’IA générative, la collecte et l’analyse de données massives concernant l’électorat québécois ou les nouvelles technologies de communication en ligne soient rendus publics, que ceux-ci soient effectués au sein de différents comités consultatifs ou par les ressources internes du DGEQ. Toujours pour promouvoir la confiance, la transparence et la délibération démocratique en lien avec les risques que font peser le numérique et l’IA sur la démocratie québécoise, il importerait de s’assurer que le DGEQ est entendu à l’Assemblée nationale chaque année au sujet de ces enjeux et de ses activités de prévention, surveillance et répression.

⁷¹ Conseil de l’Innovation du Québec 2024, 40.

Bibliographie

- Arguedas, A. R., Craig T. Robertson, Richard Fletcher, & Rasmus Kleis Nielsen. (2022). *Echo chambers, filter bubbles, and polarisation: A literature review*. Reuters Institute. <https://reutersinstitute.politics.ox.ac.uk/echo-chambers-filter-bubbles-and-polarisation-literature-review>
- Baldwin-Philippi, J. (2019). « Data campaigning: between empirics and assumptions ». *Internet Policy review* 8(4), 1-18.
- Borgesius, Frederik J. Zuiderveen, Möller, Judith., Kruikemeier, Sanne, Fathaigh, Ronan Ó., Irion, Kristina, Dobber, Tom, Bodo, Balazs, et de Vreese, Claes. (2018). « Online Political Microtargeting: Promises and Threats for Democracy ». *Utrecht Law Review* 14(1).
- Brown, Étienne. (2021). « Regulating the spread of online misinformation ». In *The Routledge Handbook of Political Epistemology*. Routledge.
- Buchanan, B., Lohn, A., Musser, M. et Sedova, K. (2021). *Truth, Lies, and Automation*. Center for Security and Emerging Technology.
- Caron, Samuel. (2023). *Élections à l'ère des mégadonnées: Les conséquences de l'hyperclientélisme politique au Canada*. Mémoire de Maîtrise, Université du Québec à Montréal. <https://archipel.uqam.ca/16514/>
- Centre d'expertise International de Montréal en intelligence artificielle (CEIMIA), Commission de l'éthique en science et en technologie (CEST) et Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) (2023a), *Les impacts sociétaux de l'intelligence artificielle sur la démocratie, l'environnement et les arts et la culture. État de situation*. Québec : Conseil de l'Innovation du Québec.
- Centre d'expertise International de Montréal en intelligence artificielle (CEIMIA), Commission de l'éthique en science et en technologie (CEST) et Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) (2023b), *Dossier thématique 5. Les autres impacts sociétaux de l'IA*. Québec : Conseil de l'Innovation du Québec.
- Chambers, S., & Kopstein, J. (2022). « Wrecking the public sphere: The new authoritarians' digital attack on pluralism and truth ». *Constellations* 30(3).
- Christiano, T. (2022). *Algorithms, Manipulation, and Democracy*. *Canadian Journal of Philosophy*, 52(1), 109-124.
- Citron, D. et Chesney, R. (2019). « Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security ». *California Law Review*, 107(6), 1753-1820.
- Coeckelbergh, M. (2022). *Democracy, epistemic agency, and AI: Political epistemology in times of artificial intelligence*. *AI and Ethics*, 1-10.

- Commission de l'éthique en science et en technologie. (2023a). La transformation numérique du réseau de la santé et des services sociaux en vue d'intégrer l'intelligence artificielle : un regard éthique. Québec : Commission de l'éthique en science et en technologie.
- Commission de l'éthique en science et en technologie. (2023b). La gestion algorithmique de la main-d'œuvre : analyse des enjeux éthiques. Québec : Commission de l'éthique en science et en technologie.
- Commission de l'éthique en science et en technologie. (2022). Mériter et renforcer la confiance des citoyens dans la gestion et la valorisation des données de santé : pour une gouvernance transparente et responsable, soucieuse de la dignité des personnes et de l'intérêt public. Québec : Commission de l'éthique en science et en technologie.
- Commission de l'éthique en science et en technologie. (2021). Projet de loi no 95, Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives. Québec : Commission de l'éthique en science et en technologie.
- Commission de l'éthique en science et en technologie. (2020). Regard sur les thèmes potentiels du programme d'études éthique et culture religieuse. Québec : Commission de l'éthique en science et en technologie.
- Commission de l'éthique en science et en technologie. (2019). Premier regard sur les enjeux éthiques soulevés par la transformation numérique de l'administration publique. Québec : Commission de l'éthique en science et en technologie.
- Commission de l'éthique en science et en technologie. (2018). Éthique et cybercitoyenneté : un regard posé par des jeunes. Québec : Commission de l'éthique en science et en technologie.
- Conseil de l'Innovation du Québec (2024)., Prêt pour l'IA, Montréal : Conseil de l'Innovation du Québec. <https://conseilinnovation.quebec/intelligence-artificielle/publications-de-la-reflexion-collective/>.
- Cohen, J. et Fung, A. (2021). « Democracy and the Digital Public Sphere ». Dans Bernholz, L., Hélène Landemore, H. et Reich, R., dir. *Digital Technology and Democratic Theory*. University of Chicago Press, 23-61.
- Cohen, L. et Rini, R. (2022). « Deepfakes, Deep harms ». *Journal of Ethics and Social Philosophy* 22(2), 143-161.
- Cortés, A., Lawrence, N., Frase H., Hoffmann, M. (2023), *Safeguards for Using Artificial Intelligence in Election Administration*, Brennan Centre for Justice.
- Dommett, K., Barclay, A., Gibson, R. (2024). « Just what is data-driven campaigning? A systematic review », *Information, Communication & Society* 27(1), 1-22.

- Dumbrava, C. (2021). Les principaux risques des médias sociaux pour la démocratie : Risques liés à la surveillance, à la personnalisation, à la désinformation, à la modération et au microciblage. Parlement européen.
- Élections Canada (2022). Répondre aux Nouveaux défis. Bureau du Directeur général des élections du Canada.
- Élections Québec (2023). Pour une nouvelle vision de la Loi Électorale. Québec : Élections Québec.
- Gandhi, M. (2024). Terrorism, Extremism, Disinformation and Artificial Intelligence: A Primer for Policy Practitioners. Londres: Institute for Strategic Dialogue.
- Gorton, W. (2016). « Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy ». *New Political Science*, 38(1), 61-80.
- Helmus, T. C. (2022). Artificial Intelligence, Deepfakes, and Disinformation : A Primer. RAND Corporation.
- Holistic AI. (2024). The State of AI Regulations in 2024. Holistic AI.
- Horvitz, E. (2022). On the Horizon: Interactive and Compositional Deepfakes. *International Conference on Multimodal Interaction*, 653-661.
- Köbis, N. C., Doležalová, B., Soraperra, I. (2021). « Fooled twice: People cannot detect deepfakes but think they can ». *IScience*, 24(11), 103364.
- Kreiss, D. (2017). « Micro-targeting, the quantified persuasion », *internet Policy Review* 6(4), 1-14.
- Lawson, A. (2023). A Look at Global Deepfake Regulation Approaches. The Responsible AI Institute
- Lavigne, M. (2022a). « Microtargeting ». Dans Ceron, A., dir. *Elgar Encyclopedia of Technology and Politics*. Edward Elgar Publishing, 231-235.
- MacDonald, A. (2022). The Uses and Abuses of Deepfake Technology. Institut canadien des affaires mondiales.
- Montigny, E. Dubois, P., Giasson, T. (2019), « On the edge of glory (...or catastrophe): regulation, transparency and party democracy in data-driven campaigning in Québec ». *Internet Policy Review* 8(4), 1-19.
- Moreau, S. et Rourke, C. (2024). « La pornographie hypertruquée a de véritables conséquences sur les femmes », *Options politiques*. <https://policyoptions.irpp.org/fr/magazines/february-2024/porno-hypertrucage-femmes/>

- Morozovaitè, V. (2024). Digital Influence: Hypernudging and the Role for European Competition Law, Thèse de Doctorat, Université d'Utrecht. <https://dspace.library.uu.nl/handle/1874/433679>.
- Nguyen, C. (2020). « Echo chambers and epistemic bubbles ». *Episteme* 17(2), 141-161.
- OCDE. (2024). Recommandation du Conseil sur l'intelligence artificielle. OECD/LEGAL/0449.
- Paris, B., & Donovan, J. (2019). Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence. Data & Society Research Institute.
- Sanders, N. E. (2023). « AI Will Upend Election Season ». *The Atlantic*. <https://www.theatlantic.com/technology/archive/2023/04/ai-generated-political-ads-election-candidate-voter-interaction-transparency/673893/>
- Schick, N. (2020). Deepfakes The Coming Infocalypse. New York : Twelve.
- Scola, N. (2016). How chatbots are colonizing politics. *Politico*. <https://www.politico.com/story/2016/10/chatbots-are-invading-politics-229598>
- Secrétariat du Conseil du Trésor (2019). Stratégie de transformation numérique gouvernementale 2019-2023. Gouvernement du Québec.
- Spitale, G., Biller-Andorno, N., et Germani, F. (2023). « AI model GPT-3 (dis)informs us better than humans ». *Science Advances*, 9(26), 1850.
- Tappin, B. M., Wittenberg, C., Hewitt, L. B., Berinsky, A. J., & Rand, D. G. (2023). Quantifying the potential persuasive returns to political microtargeting. *Proceedings of the National Academy of Sciences*, 120(25).
- Tinmaz, H., Lee, Y. T., Fanea-Ivanovici, M., et Baber, H. (2022). A systematic review on digital literacy. *Smart Learning Environments*, 9(1), 1-18.
- Thaler, R., & Sunstein, C. R. (2008). *Nudge*. New York: Penguin Random House.
- Thompson, S. A., et Hsu, T. (2023). « How Easy Is It to Fool A.I.-Detection Tools? » *The New York Times*. 28 juin . <https://www.nytimes.com/interactive/2023/06/28/technology/ai-detection-midjourney-stable-diffusion-dalle.html>
- Van der Sloot, B. et Wagensfeld, Y (2022), « Deepfakes : regulatory challenges for the synthetic society ». *Computer Law & Security Review*, 46, 1-15.
- Weiner, D. et Norden, L. (2023) *Regulating AI Deepfakes and Synthetic Media in the Political Arena*. Brennan Centre for Justice.