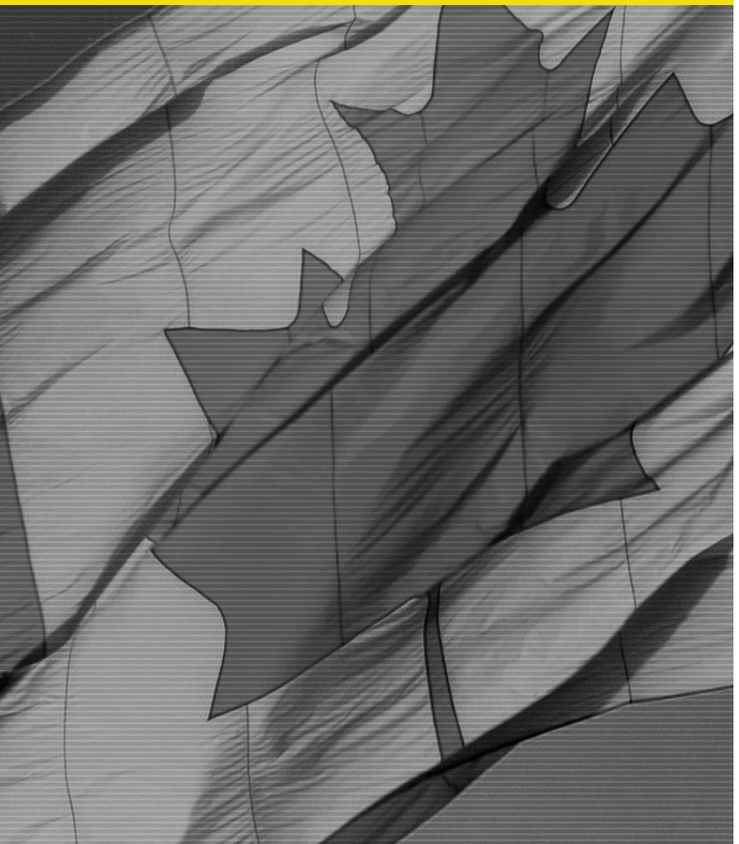
Les défis liés à la cybersécurité des élections au Canada

Elizabeth F. Judge et Michael Pal



Il y a fort à parier que l'élection fédérale d'octobre 2019 sera la première de l'histoire canadienne pour laquelle la « cybersécurité des élections » jouera un rôle prépondérant. La cybersécurité des élections peut se définir comme l'absence d'ingérence numérique à l'encontre des principaux acteurs, des principales institutions et des principaux processus électoraux. Les menaces aux élections canadiennes, du piratage des partis politiques à la désinformation diffusée sur les plateformes des médias sociaux, en passant par l'atteinte à la vie privée des électeurs et l'ingérence étrangère, sont des risques bien réels en 2019. Dans cet essai, nous exposons les principaux enjeux liés à la cybersécurité des élections auxquels est confronté le Canada en axant notre réflexion sur trois acteurs clés : les partis politiques, les administrateurs électoraux et les électeurs. Nous analyserons ensuite les conséquences pour la cybersécurité des changements imposés à la loi fédérale sur les élections par la *Loi sur la modernisation des élections*[1].

Les partis politiques

Les partis politiques du Canada sont aujourd'hui devenus des exploitations numériques sophistiquées. Ils utilisent souvent les techniques liées à l'analyse des mégadonnées dans lesquelles des algorithmes complexes génèrent des inférences sur les électeurs à partir de quantités massives de renseignements personnels majoritairement recueillis lors d'activités en ligne. Bien qu'ils continuent d'utiliser des pratiques traditionnelles, telles que le porte-à-porte, les partis opèrent de plus en plus en ligne et intègrent les données des électeurs à leurs activités. Tous les partis fédéraux ont des bases de données qui contiennent de l'information personnelle sensible sur les électeurs. Ces renseignements sont tirés de diverses sources et servent, entre autres, à la levée de fonds, aux activités visant à « gagner des votes » ainsi qu'au développement politique. En sus des publicités télévisées et radiophoniques, les partis font maintenant une promotion massive en ligne. Ce type de publicité est courant sur les plateformes des médias sociaux, plus particulièrement sur Facebook. La publicité sur les médias sociaux permet aux partis de microcibler les messages sur des sous-séries particulières d'électeurs. Les électeurs peuvent être catégorisés par code postal, type d'emploi et niveau de scolarité, ou en fonction de leur modèle de voiture, de leur alimentation, de leurs achats ou de leurs loisirs, sur la base de la théorie selon laquelle ces choix illustrent leurs préférences politiques.

Or, en passant dans l'espace numérique, les partis ont accru leurs risques cybernétiques. En 2017, le Centre de la sécurité des télécommunications (CST) du Canada a publié un rapport soulignant le risque d'ingérence étrangère dans les élections canadiennes, surtout à la lumière des exemples bien documentés d'activités malveillantes survenues ces dernières années dans d'autres démocraties (CST, 2018). Selon le CST, les partis politiques constituent un point faible de la cybersécurité des élections au Canada. Ils sont des acteurs privés dont les ressources sont faibles par rapport à leur importance, et leur personnel est souvent formé de bénévoles, surtout au niveau de la circonscription.

Ils sont ainsi de plus en plus vulnérables au piratage et représentent une cible de choix pour les acteurs étrangers. L'ingérence numérique dans les activités de l'un des principaux partis politiques du Canada aurait de profondes répercussions sur la confiance des Canadiens vis-à-vis du processus électoral et de la politique en général. Le piratage du Comité national démocrate des États-Unis à la veille des élections présidentielles de 2016 a eu des répercussions négatives sur la démocratie américaine. L'adoption d'une version canadienne de la Magnitsky Act, une loi américaine qui permet au gouvernement des É.-U. de pénaliser les gouvernements étrangers qui violent les droits de la personne, accroît également le risque d'ingérence de la part des acteurs étatiques et non étatiques qui pourraient se voir imposer des sanctions[2].

Les chefs des partis risquent de se faire usurper leur identité en ligne si une entité nationale ou étrangère prend le contrôle de leur page Facebook ou de leur compte Twitter. L'enjeu que représente l'usurpation d'identité du chef ou d'un candidat d'un parti est immense. Imaginez, par exemple, le chaos qui pourrait se produire si une entité étrangère s'emparait du compte Twitter du premier ministre.

Ce risque augmente rapidement au fur et à mesure que la technologie évolue. Le mal potentiel causé par l'usurpation d'identité augmente à cause de la technologie des « contrefaçons profondes », qui permet de manipuler des enregistrements audios et vidéos pour créer des vidéos à l'apparence extrêmement authentique de personnalités politiques en train de faire ou de dire des choses répréhensibles. Pour cette raison, il sera beaucoup plus difficile pour les électeurs de discerner la crédibilité d'une nouvelle ou d'un message publié sur les médias sociaux. Les électeurs risquent, par inadvertance, de donner foi à des vidéos trompeuses, ou de douter de la véracité de vidéos qui sont, en fait, authentiques, ce qui aurait des répercussions négatives sur le débat démocratique.

Les administrateurs électoraux

La cybersécurité constitue également une importante préoccupation pour les administrateurs électoraux. Élections Canada est l'organisme indépendant non partisan qui administre les élections fédérales, y compris la gestion des bureaux de scrutin, la compilation des résultats dans les circonscriptions, l'enregistrement des électeurs, etc. L'*Évaluation des cybermenaces nationales 2018* du Centre canadien pour la cybersécurité a permis de cerner des établissements publics à risque d'ingérence numérique en raison du type de données qu'ils détiennent et de l'importance de leur rôle (Centre canadien pour la cybersécurité, 2018). Le risque d'ingérence dans l'administration électorale a incité les États-Unis à inscrire les organismes électoraux au rang des « infrastructures critiques » (U.S. Election Assistance Commission, 2018).

Au Canada, le fait d'avoir conservé un système de scrutin sur papier traditionnel au dépend du vote électronique a, heureusement, permis d'éviter bon nombre des risques de cyberpiratage inhérents aux machines de vote et au vote sur Internet. Au vu des expériences des administrations qui ont passé au scrutin en ligne, il apparaît clairement que ces systèmes ne peuvent pas être suffisamment sécurisés pour que les citoyens aient confiance dans leurs résultats. Bien que le scrutin en ligne ait cours au Canada, notamment dans certaines municipalités de l'Ontario, ces scrutins risquent moins d'attirer l'attention de puissances étrangères hostiles. Les motivations à l'origine d'une ingérence dans une élection fédérale sont, en effet, bien plus importantes.

Même si la fidélité au scrutin sur papier du Canada a permis de diminuer les risques

L'ingérence numérique dans les activités de l'un des principaux partis politiques du Canada aurait de profondes répercussions sur la confiance des Canadiens vis-à-vis du processus électoral et de la politique en général.

Elizabeth F. Judge est professeure de droit et membre du Centre de recherche en droit, technologie et société de la Faculté de droit de l'Université d'Ottawa, où elle se spécialise dans les intersections du droit, de la technologie et de la politique.

Michael Pal est professeur adjoint de la Faculté de droit de l'Université d'Ottawa, où il dirige le Groupe du droit public. Il est spécialisé en droit comparé de la démocratie et en droit constitutionnel comparé. Il conseille tous les paliers de gouvernement concernant le droit des élections et le droit constitutionnel.

« Aux États-Unis, le piratage du Comité national démocrate à la veille des élections présidentielles de 2016 a eu des conséquences négatives pour la démocratie américaine. (Photo : Mark Van Scyoc / Shutterstock.com)

de fraudes cybernétiques, d'autres formes d'ingérence numérique demeurent une source de préoccupation. Les bases de données que les administrateurs électoraux utilisent pour enregistrer les électeurs constituent une cible de choix pour les pirates. Les activités internes des administrations électorales, tels qu'Élections Canada, peuvent faire l'objet d'ingérences susceptibles de les perturber et de faire dérailler les élections. De plus, certains administrateurs négligent les bureaux de scrutin en ligne, ce qui ouvre la voie à des risques.

À l'instar des chefs des partis politiques, les administrateurs électoraux courent également des risques d'usurpation d'identité. Lors du scandale des appels automatisés, dont certains émanaient prétendument d'Élections Canada, à la veille des élections de 2011, les messages transmis lors des appels frauduleux ont indiqué à des électeurs le mauvais bureau de scrutin ou une date d'élection erronée. Cet incident met en lumière le fait que la désinformation en ligne pourrait contaminer les futures élections par une usurpation d'identité d'Élections Canada. Des messages diffusés sur les médias sociaux, des fils Twitter, des bannières publicitaires ou des courriels de hameçonnage provenant supposément d'Élections Canada constituent tous des moyens que des acteurs malveillants peuvent utiliser pour semer la confusion et abaisser le taux de participation aux élections. Bien que les appels téléphoniques automatisés aient causé de sérieux problèmes, les mécanismes en ligne constituent une arme bien plus puissante pour créer une telle désinformation.

Au Canada, le fait d'avoir conservé un système de scrutin sur papier traditionnel au lieu de passer au vote électronique a, heureusement, permis d'éviter bon nombre des risques de cyberpiratage inhérents aux machines de vote et au vote sur Internet.

Les risques de désinformation et d'usurpation d'identité des administrateurs électoraux ont augmenté en raison de l'utilisation croissante d'applications de messagerie chiffrées de bout en bout comme WhatsApp. Bien que la messagerie qui échappe au contrôle gouvernemental offre d'importants avantages sociaux, surtout pour les populations soumises à un régime totalitaire, elle fait également en sorte que les messages erronés ou trompeurs sont difficiles à retracer et considérés comme corrects dans les régimes démocratiques. De tels messages pourraient, par exemple, indiquer à des électeurs le mauvais bureau de scrutin ou une date d'élection erronée afin d'abaisser le taux de participation aux élections. Par exemple, lors de l'élection présidentielle brésilienne de 2018, WhatsApp a joué un rôle crucial pour la publicité politique et la diffusion d'information politique, mais a également servi à propager des renseignements erronés et des insinuations[3].

Les électeurs

Aucune analyse des menaces à la cybersécurité n'est complète si l'on ne tient pas compte des effets sur les électeurs. La collecte massive d'information sur les électeurs par les partis et les conseillers de campagne ouvre la voie à des risques majeurs pour la protection des renseignements personnels des électeurs. La protection des renseignements personnels des électeurs est particulièrement pertinente dans le cas des partis politiques et des plateformes des médias sociaux.

Tout d'abord, les lois sur la protection des renseignements personnels applicables aux acteurs des secteurs public et privé ne s'appliquent pas aux partis politiques, ce qui crée un risque immense d'utilisation abusive des renseignements personnels de nature sensibles sur les électeurs. Il n'y a aucun motif de politique publique irréfutable pour lequel les partis politiques devraient être exemptés des règlements rigoureux concernant la protection de la confidentialité, car près d'un grand organisme public ou privé important de la société canadienne sur deux y est assujetti. Les électeurs doivent savoir que les partis politiques sont soumis à des principes d'équité modifiés en matière d'information pour se conformer à d'autres lois électorales fédérales, telles que la divulgation obligatoire des donateurs. Les principes d'équité en matière d'information comprennent la reddition de comptes, le consentement et les restrictions concernant la collecte, l'utilisation et la divulgation de renseignements personnels. Actuellement, les électeurs n'ont aucun moyen de savoir si les renseignements qu'ils ont donnés de plein gré aux partis, ou que les partis ont recueillis sur les médias sociaux ou auprès de sources privées, sont protégés contre la divulgation à des tiers ou par des mesures de protection comme le cryptage. Cette information risque de faire l'objet d'une ingérence informatique. En réponse à ce problème, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique a recommandé en 2018 de faire en sorte que les partis politiques soient considérés comme des entités dans le cadre de la législation existante sur la protection des renseignements personnels du secteur privé (Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 2018).

De notre point de vue, les règles sur la protection des renseignements personnels qui s'appliquent aux partis politiques devraient être adaptées à la fonction et au rôle particulier des partis. Par exemple, une « liste de numéros exclus » qui empêcherait les partis politiques de contacter des électeurs serait un désastre pour la participation démocratique et risquerait de saper le discours démocratique au lieu de le protéger. La démocratie exige, en effet, un contact entre les partis et les électeurs.

Deuxièmement, la protection des renseignements personnels des électeurs risque également d'être enfreinte par les plateformes des médias sociaux. Le modèle d'affaires des médias sociaux repose sur l'offre de services en échange de données personnelles, et les grandes plateformes ont été abondamment critiquées en raison de la façon dont elles recueillent et diffusent les données. Cette transmission des renseignements sur les électeurs entre les plateformes, les développeurs d'applications, les annonceurs et d'autres entités constitue une menace réelle pour la protection des renseignements personnels des électeurs. Dans le cas du scandale de Cambridge Analytica, l'exemple le plus célèbre de collecte de données sur des électeurs à partir de sites de médias sociaux, on a constaté l'utilisation abusive par des tiers de données recueillies sur Facebook par des conseillers de campagne, bien que Facebook en conteste l'ampleur.

La *Loi sur la modernisation des élections*

La *Loi sur la modernisation des élections* de 2018 introduit une foule de changements à la loi fédérale sur les élections, dont certaines mesures importantes visant à accroître la cybersécurité.

Premièrement, les plateformes de médias sociaux affichant un nombre minimum d'utilisateurs ont l'obligation de tenir un

Les applications de messagerie chiffrées de bout en bout comme WhatsApp augmentent les risques de désinformation et d'usurpation d'identité des administrateurs électoraux. (Photo : Tero Vesalainen / Shutterstock.com)

Les lois sur la protection des renseignements personnels applicables aux acteurs des secteurs public et privé ne s'appliquent pas aux partis politiques, ce qui crée un risque immense d'utilisation abusive de renseignements personnels de nature La gouvernance de l'espace cybernétique durant une crise de confianceau sujet des électeurs.

répertoire de toutes les publicités politiques diffusées sur leur site Web[4]. Cette mesure compense, dans une certaine mesure, l'influence du microciblage. Les publicités microciblées sont visionnées uniquement par les personnes auxquelles elles sont adressées, et les règles de divulgation des sources sont plus faciles à contourner en ligne. Leur contenu et leur origin font donc l'objet d'une surveillance publique moins importante que dans le cas d'une publicité télévisée ou radiophonique traditionnelle. L'obligation de tenir un répertoire de publicités rend la transparence inévitable et facilite la surveillance publique des publicités. Cette nouvelle condition législative n'empêche, certes, pas les publicités étrangères ou nationales qui autrement contreviendraient aux lois de financement des campagnes, mais accroît la supervision du fait que le public, les médias et les politiciens peuvent voir et examiner les publicités.

Deuxièmement, la loi crée aussi une foule d'infractions concernant les menaces numériques, y compris l'ingérence informatique[5]. Les plateformes des médias sociaux ne sont donc pas autorisées à diffuser des publicités étrangères visant à influencer un électeur[6]. Tenter de se faire passer pour un politicien ou pour Élections Canada constitue également une infraction[7].

La reconnaissance de ces infractions est une tentative prometteuse de mettre à jour la *Loi sur les élections* de façon à ce qu'elle tienne compte de la démocratie numérique et des menaces cybernétiques existantes. Cependant, il faut prendre en considération certains défis, plus particulièrement en ce qui concerne la dissuasion et la mise en application. Il est, en effet, peu probable que la reconnaissance de nouvelles infractions dissuade des acteurs étrangers à la solde d'un gouvernement hostile de pirater les bases de données d'un parti politique ou de publier du contenu trompeur sur Facebook. Même s'il est possible d'identifier les contrevenants, s'ils résident dans un pays étranger hostile, il est peu probable qu'ils soient un jour tenus de rendre des comptes. On ne sait pas non plus dans quelle mesure la disposition sur l'usurpation d'identité couvrira les contrefaçons profondes.

Finalement, la législation exigera des partis politiques qu'ils aient des politiques de confidentialité concernant des enjeux spécifiques, mais ne va pas jusqu'à accorder aux électeurs un droit exécutoire sur leurs renseignements personnels et ne leur donne pas de motif de poursuite en cas d'infraction[8]. Cette approche tiède de la réglementation des partis politiques et de la protection des renseignements personnels équivaut à manquer une occasion en or de veiller non seulement à la protection des renseignements personnels, mais aussi à la cybersécurité. Des lois assorties de mesures rigoureuses de protection des renseignements personnels auraient l'effet salutaire indirect d'exiger des partis qu'ils renforcent leurs mesures de protection de la cybersécurité et limitent la collecte de quantités massives de données personnelles susceptible de favoriser des menaces électorales fondées sur des données.

Conclusion

Dans le monde entier, des élections ont fait l'objet d'ingérences numériques nationales et étrangères. Les élections canadiennes ne sont donc pas à l'abri des attaques cybernétiques. À la veille des élections fédérales d'octobre 2019, le gouvernement, les partis politiques, les administrateurs électoraux et les acteurs de la sécurité nationale essaient d'éradiquer ces menaces prépondérantes. Autrefois marginale, la cybersécurité des élections est devenue un enjeu central de la conversation sur la démocratie, et il ne fait aucun doute qu'elle va continuer à gagner en importance après 2019. Bien qu'avec la promulgation de la *Loi sur la modernisation des élections,* le Canada ait renforcé la cybersécurité des élections, il y a encore beaucoup à faire pour préserver l'intégrité des élections canadiennes des menaces numériques.

Références

1 *Loi sur la modernisation des élections*, L.C. 2018, ch. 31 (Sanction royale, le 12 décembre 2018)

2 *Loi de Sergei Magnitsky,* L.C. 2017, ch. 21 (Can); *Abrogation Jackson-Vanik de la Russie et de la Moldavie et loi de 2012 sur la reddition de comptes de la règle de droit de Sergei Magnitsky*, Pub L N° 112–208, 126 Stat 1496 (É.-U.).

3 Voir, par exemple, García Martínez (2018).

4 *Loi sur la modernisation des élections*, *supra* note 1, à l'art. 208.1.

5 *Ibid.* à l'art. 323.

6 *Ibid.* à l'art. 282.4(5).

7 *Ibid.* à l'art. 323.

8 *Ibid.* à l'art. 254(1).

Ouvrages cités

Centre canadien pour la cybersécurité. 2018. *L'Évaluation des cybermenaces nationales. 2018.* CST. Gouvernement du Canada.https://cyber.gc.ca/sites/default/files/publications/national-cyber-threat-assessment-2018_f.pdf

CST, 2017. *Cybermenaces contre le processus démocratique du Canada.* Gouvernement du Canada. www.csecst.gc.ca/sites/default/files/cse-cyber-threat-assessment-e.pdf.

García Martínez, Antonio. 2018. « Why WhatsApp Became a Hotbed for Rumors and Lies in Brazil. » *Wired*, le 4 novembre. www.wired.com/story/why-whatsapp-became-a-hotbed-for-rumors-and-lies-in-brazil/.

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes. 2018. *Démocratie menacée :* Risques et solutions à l'ère de la désinformation et du monopole des données. Décembre. 42e législature, 1re session. https://www.noscommunes.ca/DocumentViewer/fr/42-1/ETHI/rapport-17

U.S. Election Assistance Commission. 2018. *U.S. Elections Systems as Critical Infrastructure.* Silver Spring, MD: U.S. Election Assistance Commission. www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf.