



CHRONIQUES DES NOUVELLES CONFLICTUALITÉS



@Miguel Marques/Unsplash

Cybermenaces et ingérence électorale : changement de paradigme en Roumanie

Par Danny Gagné

Depuis décembre 2024, la Roumanie traverse une crise politique. Le premier tour de son élection présidentielle a été annulé en raison de soupçons d'ingérence électorale massive. Le scrutin, marqué par différentes activités numériques suspectes, renferme d'importantes leçons pour le futur de nos processus démocratiques.

Le 6 décembre 2024, coup de théâtre en Roumanie : la Cour constitutionnelle invalide les résultats du premier tour de l'élection présidentielle, tenu deux semaines plus tôt. Călin Georgescu, candidat indépendant qui obtenait 5 % des intentions de vote à quelques jours de l'élection, a contre toute attente remporté ce premier tour avec près de 23 % des suffrages, laissant planer un doute sur l'intégrité du scrutin. La Cour invoque de multiples cyberincidents observés en marge de l'élection, notamment un flot d'activités suspectes sur la plateforme TikTok, pour justifier sa décision.

L'annulation des résultats de l'élection roumaine est loin d'être un évènement anodin : pour la première fois, une intrigue se déroulant dans le cyberspace mène au rejet en bloc des résultats d'une élection. Si les périodes électorales ne sont pas étrangères aux opérations d'influence et aux tentatives de cyberattaques, cette fois, la mécanique institutionnelle elle-même se voit mise à l'épreuve. Comment la Roumanie en est-elle arrivée là ?

Le fardeau de la preuve

C'est une intervention des organes de renseignement roumains qui, début décembre, pousse la Cour constitutionnelle vers cette décision controversée. Le Service de renseignement roumain (SRI) lui soumet en effet des informations pour le moins alarmantes. Plus de [85 000 tentatives d'intrusion](#) dans les sites électoraux et les systèmes informatiques roumains ont été enregistrées avant l'élection, voire le jour même. Les services de renseignement ont déclaré qu'il y avait des signes indiquant que les attaques étaient parainées par un État, qu'elles étaient « hautement organisées » et qu'elles fonctionnaient de manière hybride en ciblant, entre autres, des infrastructures électorales pour influencer l'opinion publique via la désinformation. De plus, toujours selon le SRI, aux 800 comptes TikTok qui auraient été créés par

un État tiers en 2016, et qui sont soudainement redevenus actifs avant l'élection, s'ajouteraient 25 000 nouveaux profils activés à moins de deux semaines du scrutin.

Un autre élément de contexte nourrit les soupçons des services de sécurité roumains : Călin Georgescu, le vainqueur inattendu, a toutes les allures du candidat chouchou de la Russie. [Ultranationaliste](#), il est un critique acerbe de l'Union européenne et de l'OTAN et veut mettre fin au soutien de son pays à l'Ukraine. Partageant une frontière commune avec son voisin en guerre, la Roumanie est une pièce maîtresse de l'échiquier géopolitique régional. Un [sondage](#) en janvier 2025 montrait que plus de 87 % de la population roumaine estimait que le futur du pays se trouvait à l'Ouest. Le pays vient d'ailleurs de faire son entrée en grande pompe dans l'espace Schengen le 1^{er} janvier 2025. Les positions de Georgescu sont donc décidément à rebours des désirs de la majorité de l'électorat.

Les médias sociaux... encore

Les élections roumaines démontrent que l'omniprésence des médias sociaux dans le processus démocratique donne un poids grandissant aux géants de la technologie. De fait, les nombreux comptes TikTok utilisés pour faire la promotion de Georgescu n'avaient pas été identifiés comme du contenu électoral, violant ainsi les lois roumaines prévues à cet effet. [Neuf millions](#) de Roumains utilisent TikTok sur une population de dix-neuf millions d'habitants. Un [rapport](#) du ministère de l'Intérieur roumain rapporte que des influenceurs étaient rémunérés à hauteur de 80 euros par jour pour faire la promotion d'un « candidat idéal » sur Instagram, Facebook et TikTok. Des comptes en apparence anodins étaient ensuite utilisés pour commenter en masse ces contenus et pour

souligner que Georgescu était le candidat répondant le mieux à ces critères.

[Bogdan Peschir](#), un programmeur impliqué dans des transactions en cryptomonnaie, aurait fait un don de 1 million d'euros à Georgescu, dont 360 000 pour de la promotion sur TikTok. Le 7 décembre 2024, les autorités roumaines ont procédé à une perquisition dans la résidence de Peschir. Selon une source anonyme, l'action policière avait pour cible une opération de blanchiment d'argent ayant servi à mousser la candidature de Georgescu. TikTok a annoncé avoir [démantelé](#) un réseau de 22 comptes en septembre, puis, en novembre, deux réseaux, respectivement de 78 et 12 comptes, utilisés pour faire de la promotion électorale douteuse. Vu l'ampleur des chiffres dévoilés par les services de renseignement roumain, il ne s'agit vraisemblablement que d'une infime partie des comptes impliqués. Si les réseaux sociaux sont maintenant des plaques tournantes pour des candidats en quête de votes, ils sont aussi des vecteurs de désinformation.

Quelles leçons à tirer pour le Canada ?

L'élection roumaine a bien sûr causé bon nombre de retombées néfastes pour le gouvernement et les électeurs. La Cour constitutionnelle a non seulement rejeté les résultats du premier tour, elle a aussi, comme de raison, reporté le deuxième tour du scrutin au 18 mai. Dans la foulée des événements, le président sortant du pays, Klaus Iohannis, a [démissionné](#) le 12 février. Face à la grogne populaire et une possible procédure de destitution, Iohannis a dit vouloir apaiser les tensions alors que plusieurs milliers de manifestants ont pris la rue suite à l'annulation du vote. Chose certaine, la confiance de la population roumaine en ses institutions démocratiques a été ébranlée.

Alors que le Canada se dirige prochainement vers une élection, quelles sont les leçons à tirer ? Le 7 février, en pleine course à la chefferie du Parti libéral du Canada, on apprenait que la candidate Chrystia Freeland avait été la victime d'une [campagne d'influence](#) coordonnée sur la plateforme chinoise WeChat. En effet, le [Mécanisme de réponse rapide](#) d'Affaires mondiales Canada aurait repéré une trentaine de comptes, tous reliés à un blogue anonyme, la ciblant. Les publications auraient été repartagées plus de 140 000 fois entre le 29 janvier et le 3 février 2025. Selon le *China Digital Times*, un média critique du Parti communiste chinois établi en Californie, il existerait un lien entre ces comptes et Pékin. Freeland avait aussi été la victime d'une [campagne d'influence](#) russe en mars 2017.

Le Canada a été la cible de nombreuses tentatives d'ingérences électorales chinoises depuis quelques années, dont trois révélées pour l'année 2023 seulement. Ces événements ont précipité le lancement d'une commission d'enquête, la Commission Hogue, qui dans son [premier rapport](#) publié en mai 2024 stipulait que les courses à l'investiture sont le maillon faible de la démocratie canadienne. Celles-ci ne sont en effet pas soumises aux mêmes lois que les élections fédérales. Elles connaissent des modalités de participation très élargies et des processus de financement plus opaques.

Bien que la course à la chefferie du Parti libéral du Canada semble s'être déroulée sans incident majeur, l'exemple de la Roumanie nous rappelle qu'il est important d'être vigilant pour préserver la légitimité de nos processus démocratiques, particulièrement dans un contexte d'élection fédérale imminente. Un récent [rapport](#) du Centre canadien pour la sécurité souligne d'ailleurs que la Chine, la Russie et l'Iran risquent de s'immiscer dans la prochaine campagne via des outils générés par l'intelligence artificielle.

La Big Tech dans l'angle mort de nos démocraties

On peut donc se demander quel rôle les compagnies de médias sociaux peuvent jouer dans la lutte aux ingérences électorales. Force est de constater que, depuis l'épisode de 2016 aux États-Unis, une part non négligeable de la lutte à la désinformation repose sur leur volonté, variable, de modérer adéquatement les contenus circulant sur leurs plateformes. TikTok est depuis un certain temps déjà vu avec suspicion du fait de ses liens avec la Chine. Cependant, les politiques de modération de contenu des compagnies américaines commencent également à susciter des inquiétudes. Alors que les grands patrons d'entreprises de médias sociaux comme Elon Musk et Mark Zuckerberg se sont rapprochés du président Donald Trump, les politiques de [modération de contenu](#) de leurs plateformes ont été affaiblies. Comment s'assurer que le Canada et d'autres démocraties ne connaissent pas le même sort que la Roumanie? Une chose est certaine, comme le démontre la saga entourant l'adoption du projet de [loi-C18](#), Ottawa devra faire preuve de créativité, de courage et de persévérance au niveau légal et réglementaire pour avoir une prise sur les entreprises de médias sociaux.

Danny Gagné est chercheur à l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand.

Pour en savoir plus sur la Chaire Raoul-Dandurand et ses travaux : <https://dandurand.uqam.ca>.

