Guerre de l’information et transition étatique

Sécuriser l’espace informationnel.

La question de la désinformation en contexte de transition souveraine est rarement traitée avec la rigueur qu'elle mérite. On la réduit souvent à un problème de fausses nouvelles circulant sur les réseaux sociaux, alors qu'il s'agit d'une menace systémique touchant simultanément les infrastructures techniques, les institutions démocratiques et la psychologie collective. Pour un Québec en transition vers la souveraineté, l'espace informationnel constitue un territoire à défendre au même titre que le territoire physique, et les États qui l'ont négligé en période de crise politique en ont payé le prix en légitimité internationale et en cohésion interne.

Le premier angle mort est économique. Les campagnes de désinformation coordonnées ont un coût de production précis et un retour sur investissement documenté. L'Internet Research Agency (IRA) russe, dont le budget mensuel consacré aux seules opérations américaines a été évalué à environ 1,25 million de dollars selon le rapport Mueller de 2019, a produit plus de 80 000 publications sur Facebook entre 2015 et 2017, atteignant potentiellement 126 millions d'Américains selon les déclarations de Facebook au Congrès en 2017. Rapporté au coût par contact, ce ratio dépasse l'efficacité de n'importe quelle campagne publicitaire conventionnelle. En Catalogne, des chercheurs de l'Université de Stanford ont identifié en 2019 des réseaux coordonnés de comptes inauthentiques diffusant simultanément du contenu pro et anti-indépendantiste, une tactique qui vise moins à convaincre qu'à saturer l'espace informationnel et à épuiser la capacité de discernement des électeurs. Ce mécanisme porte un nom en psychologie cognitive : la fatigue épistémique, soit l'état dans lequel un individu exposé à un volume excessif d'informations contradictoires renonce à former un jugement et se réfugie dans l'abstention ou dans ses croyances préexistantes. Un acteur disposant de quelques millions de dollars peut donc produire cet effet à l'échelle d'un électorat entier.

« Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data » --Shoshana Zuboff, The Age of Surveillance Capitalism (2019).

L'asymétrie informationnelle entre un État fédéral et un État en formation constitue une vulnérabilité concrète. Le gouvernement fédéral canadien administre, via l'Agence du Revenu du Canada, Emploi et Développement Social Canada et le ministère de la Santé, des bases de données comportementales d'une granularité exceptionnelle : revenus, historique d'emploi, consommation de soins, déplacements. Ces données permettent le micro-ciblage comportemental, soit la capacité d'identifier des sous-groupes d'électeurs selon leur profil psychologique et économique, puis de leur adresser des messages politiques personnalisés. Cambridge Analytica aurait, selon ses propres déclarations lors du référendum sur le Brexit en 2016, segmenté l'électorat britannique en plus de 70 catégories construites selon le modèle OCEAN (ouverture au changement, conscienciosité, extraversion, agréabilité, névrosisme), un outil issu de la psychologie de la personnalité permettant de prédire les réactions émotionnelles d'un individu face à un message politique donné. Ces affirmations émanaient d'une entreprise ayant intérêt commercial à surestimer ses capacités, mais les mécanismes sous-jacents du ciblage publicitaire différencié sont documentés indépendamment par des chercheurs de l'Université de Cambridge.

Appliquée au contexte québécois, cette logique signifie qu'un acteur disposant d'un accès aux bases de données administratives fédérales et aux données des plateformes numériques pourrait construire des campagnes de découragement ciblées visant les électeurs indécis dans les circonscriptions pivots. Pour contrer cette vulnérabilité, un Québec souverain créerait une fiducie nationale des données : un organisme public dont le mandat serait de rapatrier sous juridiction québécoise exclusive les données des citoyens, de les chiffrer selon les standards AES-256 (recommandé par la NSA américaine pour ses communications classifiées), et d'en interdire l'accès à tout acteur extérieur sans mandat judiciaire québécois. Cela impliquerait une négociation de rapatriement avec Ottawa dans le cadre des accords de transition, assortie d'une loi québécoise sur la protection des données à portée extraterritoriale.

Le précédent de 1995 illustre concrètement pourquoi le contrôle souverain du registre électoral n'est pas une précaution abstraite. Lors du référendum du 30 octobre 1995, le gouvernement fédéral de Jean Chrétien a accéléré les cérémonies de naturalisation à l'automne précédant le vote, augmentant le nombre de nouveaux citoyens admissibles dans des proportions documentées par le DGE du Québec. Des allégations de votes multiples et de votes de personnes non admissibles ont circulé, sans que les mécanismes de vérification en place à l'époque permettent d'en établir l'étendue avec précision. Le love-in de Montréal, rassemblement organisé les 27 et 28 octobre 1995 et partiellement financé par des entreprises privées et des fonds coordonnés par Ottawa, a par ailleurs dépassé selon plusieurs analyses les plafonds de dépenses autorisés par la loi électorale québécoise, sans qu'aucune poursuite n'aboutisse. Dans l'état actuel des choses, la confirmation de l'identité des citoyens québécois repose largement sur des infrastructures fédérales : numéro d'assurance sociale géré par Service Canada, passeport émis par Immigration, Réfugiés et Citoyenneté Canada, données fiscales de l'Agence du revenu. Le fichier des électeurs québécois, bien qu'administré par le DGE, est partiellement alimenté par des croisements avec ces sources fédérales. Un État en transition qui ne contrôle pas souverainement l'authentification de ses propres citoyens s'expose à ce qu'un acteur fédéral conteste la validité du registre électoral, retarde l'accès aux données nécessaires à sa mise à jour, ou introduise des incertitudes sur l'admissibilité de certains électeurs dans des circonscriptions stratégiques.

Un Québec souverain établirait donc une identité numérique citoyenne autonome, soit un système d'authentification cryptographique sous juridiction québécoise exclusive, alimenté par le registre de l'état civil provincial et indépendant de toute base de données fédérale. Ce système constituerait le socle technique du registre électoral souverain, rendant toute contestation externe de sa validité juridiquement et techniquement sans prise.

Les médias traditionnels québécois constituent un vecteur de vulnérabilité distinct, moins visible que les réseaux sociaux mais tout aussi opérant. Une part significative de l'information politique au Québec transite par des agences de presse dont les fils de nouvelles sont partiellement alimentés par des sources fédérales : Patrimoine canadien, le Bureau du Conseil privé, et des organisations satellites financées par Ottawa. La reprise non critique de ces dépêches par des salles de rédaction sous-financées produit un effet d'amplification involontaire du cadrage fédéral, un phénomène appelé *laundering* narratif (le recyclage d'un message partisan à travers un média perçu comme neutre, ce qui lui confère une crédibilité qu'il n'aurait pas eu à la source). Cela ne présuppose pas de mauvaise foi des journalistes : le sous-financement chronique des médias québécois réduit mécaniquement leur capacité à produire une couverture indépendante des événements politiques majeurs.

Pour contrer ce mécanisme, une agence de veille informationnelle utiliserait des outils d'analyse sémantique automatisée capables de comparer en temps réel les formulations d'une dépêche source avec celles des articles dérivés, et de détecter les reprises quasi-intégrales sans attribution. Le déclencheur d'intervention publique serait défini par seuil : toute dépêche reprise par plus de cinq organes de presse en moins de six heures avec un taux de similarité textuelle supérieur à 70% déclencherait une vérification et, si justifié, une note publique de contextualisation.

Les plateformes numériques amplifient ces dynamiques par leur architecture même. Facebook, YouTube et X sont des entreprises américaines dont les algorithmes de recommandation optimisent l'engagement, non la vérité. Un contenu qui provoque une réaction émotionnelle forte génère des clics et des partages, ce qui signale à l'algorithme qu'il doit le montrer à davantage de personnes. Des études internes de Meta, citées par Frances Haugen devant le Sénat américain en 2021, ont établi que le contenu émotionnellement polarisant génère en moyenne six fois plus d'interactions que le contenu neutre. La plateforme n'a pas besoin d'être complice d'une campagne de désinformation pour en devenir l'infrastructure : son modèle économique suffit. L'objection selon laquelle un État québécois ne pourrait pas contraindre des entreprises américaines est partiellement fondée, mais elle ignore que l'Union européenne a imposé des obligations concrètes à ces mêmes plateformes via le Digital Services Act de 2022 : obligation de transparence sur le fonctionnement de leurs algorithmes de recommandation, audits indépendants annuels sur les risques systémiques, et interdiction du ciblage publicitaire fondé sur des données sensibles. Une juridiction de taille moyenne peut obtenir des concessions réelles si elle légifère avec précision.

La souveraineté informationnelle exige une réflexion sur le substrat physique de l'information. Internet repose sur des câbles, des points d'échange (IXP, soit les noeuds physiques où les réseaux de différents opérateurs se connectent entre eux) et des centres de données dont la majorité se trouvent hors du territoire québécois ou sous juridiction fédérale. Contrôler un IXP, c'est contrôler la capacité de filtrer ou de ralentir sélectivement certains types de trafic. L'Estonie, après la cyberattaque de 2007 qui a paralysé ses banques et ses médias pendant plusieurs jours dans un contexte de tension avec la Russie, a développé le concept d'ambassades de données : des serveurs hébergeant des copies chiffrées des données gouvernementales sur le territoire d'États alliés, le Luxembourg ayant été le premier signataire d'un tel accord en 2017. Un gouvernement québécois en transition cartographierait les IXP sur son territoire, en négocierait le contrôle opérationnel avec les fournisseurs d'accès, et construirait au moins deux centres de données gouvernementaux redondants sous juridiction provinciale exclusive, géographiquement distants pour des raisons de résilience.

La technique de l'*air-gapping* (l'isolation physique totale d'un réseau informatique vis-à-vis de l'internet public, rendant toute intrusion à distance impossible) s'appliquerait aux systèmes de compilation des résultats, aux registres d'état civil et aux communications intergouvernementales sensibles. En pratique : des ordinateurs jamais connectés à internet, des transferts de données par supports physiques chiffrés uniquement, et des salles d'accès journalisé. Ce n'est pas une mesure d'exception : c'est la norme appliquée par la Suède et la Finlande à leurs infrastructures gouvernementales critiques.

L'*astroturfing* (la fabrication d'un mouvement d'opinion simulant une mobilisation citoyenne spontanée alors qu'il est coordonné par un acteur externe) est difficile à distinguer d'un débat organique en temps réel. **En Écosse, lors de la consultation souveraine de 2014, des chercheurs de l'Université d'Edinburgh ont identifié a posteriori des schémas de publication coordonnée sur Twitter avec des pics d'activité incompatibles avec un comportement humain normal et des profils créés en série quelques semaines avant le vote. Ces réseaux amplifiaient les projections économiques défavorables à l'indépendance.** L'absence de toute obligation légale de transparence sur le financement numérique a rendu toute investigation judiciaire impossible. Dès la période de transition, un gouvernement souverainiste adopterait une loi sur la transparence algorithmique des campagnes politiques : toute plateforme opérant sur son territoire serait tenue de déclarer en temps réel l'identité du commanditaire de tout achat publicitaire politique, le montant dépensé et les critères de ciblage utilisés. Ce registre public serait actualisé quotidiennement pendant les périodes de consultation démocratique.

« *Disinformation is most effective not when it creates new beliefs, but when it amplifies existing doubts* » --Renée DiResta, Stanford Internet Observatory (2020).

Les communautés anglophones et allophones représentent environ 20% de l'électorat québécois, selon les données du recensement de 2021 de Statistique Canada. Ces communautés consomment leur information via des médias dont les algorithmes sont calibrés sur un écosystème canadien-anglais qui traite structurellement l'indépendance québécoise comme une anomalie déstabilisatrice. Des campagnes ciblant ces communautés en anglais, sur des plateformes que les institutions québécoises ne surveillent pas activement, auraient un coût d'entrée minimal pour un acteur fédéral et un effet potentiellement décisif dans des circonscriptions à forte densité allophone comme certains quartiers de Montréal et de l'Outaouais. Une stratégie de protection informationnelle inclurait donc une capacité de veille multilingue et des partenariats avec des médias communautaires pour garantir l'accès à une information de référence fiable sur le processus de transition.

Le financement d'influence via des organisations de façade constitue une lacune légale documentée. Une fondation peut recevoir des fonds fédéraux ou étrangers, produire des rapports sur les conséquences économiques de l'indépendance, les faire circuler dans les médias, et ne jamais apparaître dans les registres de dépenses électorales parce que ses activités ne constituent pas techniquement de la publicité politique. Lors du Brexit, plusieurs groupes *pro-Leave* avaient des structures de financement opaques croisant des fonds britanniques et américains, selon les enquêtes du *National Crime Agency* britannique. Un Québec souverain étendrait la portée de sa loi électorale pour inclure toute organisation dont l'activité de communication a pour effet mesurable de favoriser ou défavoriser un camp, exigeant la divulgation complète de ses sources de financement dans les 30 jours suivant le déclenchement d'une campagne.

La réponse institutionnelle centrale serait une agence indépendante de veille informationnelle, financée par le budget de l'Assemblée nationale plutôt que par le pouvoir exécutif, avec un mandat limité à la détection et à la publication, sans pouvoir de retrait de contenu. La Finlande, que le *Media Literacy Index* de l'*Open Society Institute Europe* classe régulièrement en première position pour la résistance à la désinformation, démontre qu'une telle approche couplée à des programmes scolaires d'éducation aux médias produit des effets mesurables sur la résilience collective.

La désinformation ne détruit pas la démocratie par un événement unique et identifiable. Elle opère par dégradation progressive de la confiance, jusqu'au point où l'abstention devient une réponse rationnelle à un environnement perçu comme irrémédiablement manipulé. C'est ce seuil de désengagement que les acteurs hostiles cherchent à atteindre bien avant le jour du vote, en pariant que la désorientation collective rend inutile toute falsification grossière du scrutin lui-même. Reconnaître ce mécanisme est le préalable à toute défense efficace.

Louis-Martin Carrière