INSTITUT D'ÉTUDES INTERNATIONALES DE MONTRÉAL

UQÀM

WWW.IEIM.UQAM.CA

Les enjeux de souveraineté numérique face au pouvoir transnational des *big tech* : Recommandations au Canada et au Québec

Mai 2021

Résumé exécutif

La globalisation connait des transformations profondes avec le développement du numérique, les progrès de l'intelligence artificielle, de l'infonuagique (*cloud computing*) et l'avènement des réseaux de communication 5G pour la téléphonie mobile. L'interdépendance des économies nationales cède place à l'interconnexion des espaces économiques, désormais organisés en réseaux d'échanges transnationaux. Des volumes vertigineux de données (*big data*) circulent à l'échelle globale, transportés par des câbles sous-marins intercontinentaux de télécommunication. Les firmes multinationales du numérique (*big tech*) essentiellement américaines, souvent désignées par le sigle « GAFAM » et chinoises désignées par le sigle « BHATX », sont les acteurs structurants de ces mutations.

La captation et l'exploitation des mégadonnées, l'augmentation de la puissance de calcul des algorithmes de prédiction, et la dépendance des consommateurs d'Internet aux plateformes numériques et aux solutions technologiques sont au cœur du pouvoir de marché des *big tech*. Cette montée en puissance des acteurs privés du numérique, qui s'est accélérée avec la pandémie mondiale de la COVID-19, déplace les rivalités de puissance entre les États dans le cyberespace devenu le quatrième élément constitutif de l'État contemporain. Les données personnelles et comportementales issues de nos transactions sociales et économiques en ligne sont captées pour alimenter les technologies numériques sous le contrôle d'une poignée de firmes oligopolistiques. Cette puissance globale des acteurs privés transnationaux du numérique s'appuie sur les asymétries réglementaires, et sur la dépendance des divers ordres de gouvernements à leurs produits et services, pour s'imposer.

Ce document de recommandations politiques examine les avenues d'actions possibles pour le Canada et le Québec, face aux défis de gouvernance posés par les *big data*. Il explore les modalités d'exercice de la souveraineté numérique par les États, au sein d'un cyberespace multi-acteurs, soumis aux intérêts de puissance, et en quête de sécurité collective. L'analyse débouche sur la formulation de dix recommandations à l'intention du Canada et du Québec.

→ **Des milliards de données circulent hors des espaces de souveraineté juridique des États. Leur manipulation et leur exploitation à l'échelle globale n'obéissent principalement qu'aux régimes de régulation des pays d'appartenance des *big tech*.**

→ **Le pouvoir des *big* tech se traduit par la hausse vertigineuse de leur puissance de marché et de leur capital financier : à l'été 2020, la capitalisation boursière d'Apple franchissait la barre des 2000 milliards de dollars. À titre comparatif, le PIB du Canada se chiffrait à 2300 milliards (CAD) en 2019.**

→ **Le Canada et le Québec exercent une certaine souveraineté sur les données gouvernementales. Cependant les données des citoyen.ne.s et des entreprises ne bénéficient pas du même niveau de protection juridique qui s'applique aux données gouvernementales.**

Contenu

Introduction

À l'été 2019, Desjardins révélait des fuites massives de données personnelles qui allaient devenir l'un des plus importants cas de vol de renseignements personnels que le Canada ait connus. L'incident, qui aurait été commis par un employé aux intentions malveillantes, portait sur plus de 4,2 millions de comptes de particuliers et 200 000 comptes d'entreprises[1]. Les risques de vol d'identités et de cybercrimes soulevés par cet incident ont relancé le débat sur la question sensible de la protection des renseignements personnels, et sur la capacité des différents ordres de gouvernement à protéger les citoyen.ne.s canadien.ne.s des menaces pesant sur leurs données électroniques. Pouvait-on l'anticiper ou même éviter ce vol de données ? Les ordres de gouvernement disposent-ils de stratégies, d'instruments et de capacités adéquats pour faire face à ces enjeux ? Pour répondre aux nombreuses questions posées par cette affaire, il faut dresser un constat clair : la donnée est devenue le capital et le principal catalyseur de la nouvelle économie. Cette nouvelle économie est celle du numérique, qui migre vers l'économie algorithmique[2], accélérée par les progrès en intelligence artificielle.

« La donnée est devenue le capital et le principal catalyseur de la nouvelle économie. Cette nouvelle économie est celle du numérique, qui migre vers l'économie algorithmique, accélérée par les progrès en intelligence artificielle. »

En effet, le développement des technologies numériques a entrainé des transformations majeures de nos sociétés, et de l'économie mondiale. Des chaines de valeurs transnationales se structurent et transitent désormais dans le cyberespace, générant des flux vertigineux de données massives, qui circulent à travers des réseaux et terminaux interconnectant des espaces économiques en compétition. Depuis la révolution informatique des années 90, la croissance des services digitaux et l'ampleur de l'adoption des solutions technologiques accélèrent la dématérialisation des échanges. Des milliards de données d'internautes, d'entreprises et même d'États, à haute valeur économique, commerciale et stratégique, sont captées et transportées par des milliers de câbles sous-marins et de réseaux terrestres à destination de plateformes, de serveurs et d'algorithmes sous le contrôle d'acteurs privés constitués en « empires numériques »[3]. Ces acteurs privés sont essentiellement les firmes multinationales technologiques désignées sous les sigles de GAFAM (Google, Apple, Facebook, Amazon, Microsoft) pour les géants américains du web, et BHATX (Baidu, Huawei, Alibaba, Tencent, et Xiaomi) pour les géants chinois.

[1] T. Péloquin et H. Pilon-Larose (2019). « Vol de données chez Desjardins : 4,2 millions de victimes », La Presse, publié le 2 novembre 2019 sur https://www.lapresse.ca/actualites/justice-et-faits-divers/2019-11-02/vol-de-donnees-chez-desjardins-4-2-millions-de-victimes.

[2] Pour Philippe Nieuwbourg, expert en gouvernance des données et enseignant à l'UQAM, on parle d'économie algorithmique pour désigner toutes les opérations marchandes et de production de la valeur générées par les algorithmes. On peut dire que l'économie des algorithmes est le marché qui s'organise autour de l'achat, la vente, la location et le prêt d'algorithmes, moyennant finance ou pas. Il fixe le prix de chaque algorithme. L'économie algorithmique est une évolution de l'économie traditionnelle, dans laquelle les algorithmes deviennent des agents économiques directs. Les algorithmes sont aussi au cœur des enjeux de concurrence et de pratiques anticoncurrentielles liés au développement de la consommation automatisée. (Cf Frederic Marty, « les algorithmes de prix, intelligence artificielle et équilibres collusifs », Revue internationale de droit économique, 2017/2 https://www.cairn.info/revue-internationale-de-droit-economique-2017-2-page-83.htm).

[3] Le concept est de Nicolas Miailhe, pour parler de la supériorité technologique face aux États, et du caractère économique dominant des grandes firmes multinationales du numérique qui prennent une place de plus en plus importante dans la géopolitique internationale. Leur rôle sera déterminant dans les futurs équilibres de puissances, notamment entre les États-Unis et la Chine. https://www.ifri.org/sites/default/files/atoms/files/geopolitique_de_lintelligence_artificielle.pdf.

Le numérique est partout, et l'intelligence artificielle connait des progrès fulgurants avec l'apparition de l'apprentissage profond, du *data mining* et de la technologie de la chaine de blocs, ou *blockchain*. Les technologies numériques pénètrent progressivement les interstices de nos vies, s'imposent aux entreprises confrontées à de nouveaux enjeux de productivité et de concurrence, et s'affirment face aux États devenus dépendants. La rapidité et la complexité du développement des technologies numériques échappent aux capacités des États et limitent de fait l'exercice de leur souveraineté dans le cyberespace. De la brosse à dents intelligente, à la commande d'un livre en ligne, en passant par la consultation de courriels et le visionnement de films sur Netflix, notre écosystème social est envahi par le numérique. Avec l'apparition de la pandémie mondiale de la COVID-19, il ne serait pas abusif de dire que l'on assiste à une digitalisation accélérée de la vie sociale.

Quelques chiffres saillants peuvent nous permettre de percevoir l'importance des effets structurants de cette transition inédite que traversent actuellement nos sociétés :

- En 2020, plus de 2 milliards de personnes utilisaient Internet, soit 30 % de la population mondiale.
- Le commerce en ligne représentait 71 % des activités d'Internet, et la plateforme de commerce numérique Amazon réalisait un chiffre d'affaires de 35 millions de dollars par heure.
- Du côté des logiciels, moteurs de recherche et réseaux socionumériques, on enregistrait 156 millions de courriels envoyés par minute, 484 000 messages WhatsApp envoyés par seconde, 3,8 millions de requêtes par minute dans le moteur de recherche Google, 10,2 millions de commentaires sur le réseau social Facebook toutes les vingt minutes, et 24 milliards de visites mensuelles sur YouTube[4].

Ces chiffres colossaux rendent compte de l'ampleur que prennent les outils et technologies numériques dans nos vies. Mais que signifient-ils au niveau plus macroscopique ? Et quels messages nous transmettent-ils ?

Avec la montée en puissance des géants du numérique constitués en pôles oligopolistiques, l'interpénétration des économies nationales cède place à une globalisation numérique, caractérisée par l'interconnexion des marchés et la transnationalisation des chaines de valeurs. Les flux intensifs et continus de données massives, et la disparition des frontières entrainent la formation d'espaces corporatifs déterritorialisés, fondés sur des réseaux économiques et des circuits de production qui se déploient à l'échelle planétaire. Des changements disruptifs s'opèrent avec l'automatisation des modes de production, la surveillance et le traçage des modes de consommation à l'aide d'algorithmes de prédiction. Il s'agit d'une tendance que l'Internet des objets et l'avènement de la 5G vont affermir et amplifier. Le contrôle des *big data* devient un intérêt majeur de puissance. Ces mutations technologiques et sociétales soulèvent des problèmes nouveaux de modèle de gouvernance, de régimes de régulation du progrès technologique, d'échelle de marché, et d'exercice de la souveraineté étatique dans le champ du numérique, face à l'accroissement de la dépendance des États aux technologies contrôlées par des acteurs privés transnationaux.

[4] https://www.planetoscope.com/Internet-/2044-que-se-passe-t-il-sur-internet-chaque-seconde-.html

Le présent document de recommandations vise à exposer les enjeux de la gouvernance des données pour le Canada et le Québec, face au développement accéléré des technologies numériques sous l'impulsion des firmes multinationales technologiques. Il s'intéresse à la question des capacités opérationnelles et régulatoires des ordres de gouvernements du Canada et du Québec à exercer une souveraineté numérique face à la puissance des acteurs privés transnationaux. Plus précisément, ce document formule une série de dix recommandations, présentées comme des avenues possibles d'action pour le Canada et le Québec en matière de gouvernance des données et de souveraineté numérique, ceci dans un contexte mondial où les *big tech* imposent de plus en plus leurs rapports de force.

L'effet transnational de la montée en puissance des *big tech* et le capitalisme de surveillance

En 2014, le Rapport McKinsey chiffrait à 7800 milliards de dollars[5] la valeur ajoutée créée par la globalisation des données, soit plus de la moitié du PIB de la Chine en 2019. L'économie des *big data* et ses chaines de valeurs représentent un marché considérable en pleine expansion. Ce marché des mégadonnées, qui transcende les frontières, leurs structures, leurs fonctions et leurs finalités[6], échappe au contrôle des États. De fait, le marché des *big data* est structurellement transnational et se concentre entre les géants du numérique GAFAM et BHATX (*big tech*) qui accroissent et consolident leurs monopoles par une intégration des marchés et des espaces économiques à l'échelle mondiale au moyen des plateformes numériques[7]. Cette globalisation par le biais des plateformes numériques constitue le catalyseur le plus saillant de la transnationalisation et de la montée en puissance technologique, économique et capitalistique *des big tech*.

Des milliards de données circulent ainsi hors des espaces de souveraineté juridique des États. Leur manipulation et leur exploitation à l'échelle globale n'obéissent principalement qu'aux régimes de régulation des pays d'appartenance des *big tech*. Le fait est que l'importance économique des données semble éclipser l'enjeu de leur contrôle juridique et politique. En effet, en 2018, la firme d'analystes IDC évaluait à 1,45 milliard de dollars le marché canadien des mégadonnées et de l'analyse d'affaires[8]. C'est dire que l'économie de la dématérialisation s'amplifie, en déplaçant l'approfondissement de la globalisation vers le champ des *big data*. Cela met en place une dynamique qui fait émerger des acteurs technologiques transnationaux constitués en oligopoles, dont les capacités d'innovation, de création et de développement semblent illimitées.

Des transformations profondes s'opèrent dans nos habitudes de consommation et de communication avec l'adoption massive des objets connectés dans les interactions sociales et l'arrimage aux services infonuagiques (*cloud computing*) des organisations publiques et privées. À cela

[5] McKinsey Global Institute (2016). Digital Globalization: The New Era of Global Flows, p.23. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx.
[6] Extrait de M. Rioux (2019). « Transnational », dans E. Boulanger, E. Mottet, M. Rioux (S. dir), Mondialisation et connectivité. Les enjeux du commerce, de l'investissement et du travail au XXIe siècle, Presses de l'Université du Québec.
[7] D. Tchéhouali et H. Loiseau (2021). « La nouvelle géopolitique des géants d'Internet », dans M. Arès, E. Boulanger et E. Mottet (S.dir), La guerre par d'autres moyens, Rivalités économiques et négociations commerciales au XXIe siècle, 2021, Presse de l'Université du Québec.
[8] Affaires mondiales Canada. Investir au Canada. Les mégadonnées au Canada, consulté le 16 avril 2021. https://www.international.gc.ca/investors-investisseurs/assets/pdfs/download/Secteurs_de_Pointe-Megadonnees.pdf.

s'ajoute la robotisation des activités industrielles et même des services, la croissance de la consommation automatisée, la mise sous surveillance de nos comportements à potentiel économique et même politique, et le développement des algorithmes de recommandations pour façonner nos préférences et nos choix. Les firmes multinationales du numérique prennent ainsi de plus en plus d'importance et de pouvoir sur nos transactions sociales et économiques, au détriment des États. Elles contrôlent des centres de données (*data center*s), des câbles sous-marins intercontinentaux de télécommunications, la production d'algorithmes, et les services infonuagiques. L'écosystème du web semble glisser sous le pouvoir des acteurs privés. Ce pouvoir des géants du web sur nos données se traduit par la hausse vertigineuse de leur puissance de marché et de leur capital financier, les transformant en entreprises systémiques d'échelle transnationale, capables d'imposer des rapports de force asymétriques aux États. En effet, à l'été 2020, la capitalisation boursière d'Apple franchissait la barre des 2000 milliards de dollars[9], un record historique. À titre comparatif, le PIB du Canada se chiffrait à 2300 milliards de dollars canadiens (CAD) en 2019.[10] Durant la même période, Alphabet Inc., la maison mère de Google franchissait la barre de 1000 milliards de capitalisation boursière[11] tandis que Facebook et Tencent (le géant chinois) se valorisaient en bourse à plus de 600 milliards de dollars. Les *big tech* ne sont pas que des puissances technologiques, ce sont de véritables puissances financières et économiques dont le pouvoir ne cesse de grandir grâce à l'innovation technologique, l'exploitation des données comportementales et les algorithmes de prédiction.

« Les big tech *ne sont pas que des puissances technologiques, ce sont de véritables puissances financières et économiques dont le pouvoir ne cesse de grandir grâce à l'innovation technologique, l'exploitation des données comportementales et les algorithmes de prédiction. »*

Cette montée en puissance des acteurs privés est soutenue par la dépendance croissante des consommateurs des technologies numériques à leurs plateformes, à leurs services et à leurs outils. On assiste ainsi à une transition numérique qui encastre les chaines de valeurs dans la sphère web. L'émergence de l'Internet des objets et l'accroissement de la puissance des algorithmes s'imposent clairement comme des enjeux stratégiques et économiques déterminants pour les États. Ainsi, on est en droit de se demander quelle marge de souveraineté les États peuvent encore exercer, dans un contexte de dépendance aux solutions technologiques des firmes transnationales du numérique. Le déplacement des rivalités de puissance dans le cyberespace pose des défis nouveaux pour la sécurité collective.

Le principal effet de la transnationalisation des *big tech* est sans aucun doute le passage au capitalisme de surveillance. Ceci est à attribuer au développement de la puissance prédictive des algorithmes. Ce capitalisme de surveillance qui accélère son approfondissement avec les progrès de l'intelligence artificielle est fondé sur un principe simple : « extraire les données personnelles et vendre aux annonceurs des prédictions sur le comportement des utilisateurs. »[12] La mainmise libre et constante sur les données (*big data*) devient un impératif pour la survie de la puissance symbolique, économique et technologique des *big tech*. Car le développement des algorithmes de prédiction des comportements, et l'expropriation — au moyen des conditions générales

[9] https://bourse.lefigaro.fr/actu-conseils/la-capitalisation-d-apple-depasse-les-2-000-milliards-de-dollars-20200820
[10] https://www.tresor.economie.gouv.fr/Pays/CA/donnees-generales#:~:text=En%20cons%C3%A9quence%20de%20la%20crise,6%25%20du%20PIB%20en%202020.
[11] https://fr.statista.com/infographie/20532/evolution-de-la-capitalisation-boursiere-alphabet-google/.
[12] S. Zuboff (2019). « Un capitalisme de surveillance », Le Monde diplomatique, consulté le 15 avril 2021 sur https://www.monde-diplomatique.fr/2019/01/ZUBOFF/59443.

d'utilisation (CGU) rarement comprises — des droits de propriété des usagers des technologies numériques sur leurs données sont au cœur du modèle économique du capitalisme de surveillance. Les rapports de pouvoir clairement asymétriques instaurés par les *big tech* sur le contrôle et la monétisation des *big data* fondent leur pouvoir de marché.

Avec l'économie algorithmique, on est progressivement passé de l'extraction des données comportementales destinées à améliorer la vitesse, la précision des résultats de recherche ou les fonctionnalités des services numériques en eux-mêmes, vers le développement des capacités de lire les pensées des utilisateurs, afin de prédire leurs choix et orienter leurs préférences. Le capitalisme de surveillance, glissant vers un capitalisme d'influence, s'impose ainsi comme le marché des produits prédictifs fondé sur le profilage des internautes au moyen de l'analyse de leurs habitudes et comportements captés en ligne. C'est le marché de l'intrusion dans la vie des consommateurs d'Internet. Il s'agit d'un capitalisme immersif, qui se construit sur la marchandisation de l'expérience humaine devenue, à proprement parler, un produit de marché. Face à ces développements profonds du numérique, de nombreux États semblent être à la traine, et ces nouveaux espaces d'interactions et de transactions échappent à leur autorité. Toutefois, des évolutions en matière règlementaire apparaissent face aux enjeux liés à la protection de la vie privée et des libertés individuelles sur internet. C'est le cas dans l'Union européenne avec l'entrée en vigueur le 25 mai 2018 du Règlement général sur la protection des données (RGPD)[13]. Ce règlement innovant relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, s'affirme progressivement comme un dispositif juridique de référence en matière de préservation des droits et libertés fondamentaux en ligne, face aux géants de l'industrie numérique. Tout comme la régulation du traitement des données personnelles constitue un enjeu saillant de la transition numérique, la régulation des algorithmes représente un enjeu majeur pour la société de l'information. Car les algorithmes sont les piliers du profilage des comportements de consommation en ligne. C'est pourquoi dans un rapport de mission sur la politique publique de la donnée, des algorithmes et des codes source, adressé au Premier ministre français Jean Castex, le groupe de travail dirigé par le député français Éric Bothorel[14] propose de légiférer sur l'ouverture de certains codes source à la transparence, afin d'en surveiller la loyauté et la sincérité.

« Au Canada et au Québec, les données des citoyen.ne.s et des entreprises ne bénéficient pas du même niveau de protection juridique qui s'applique aux données gouvernementales. »

« Face à ces développements profonds du numérique, de nombreux États semblent être à la traine, et ces nouveaux espaces d'interactions et de transactions échappent à leur autorité. »

Le Canada et le Québec se sont donné des dispositifs et des instruments pour faire face à ces nouveaux enjeux liés au contrôle des *big data*. Ainsi, le Canada a élaboré sa stratégie « Le nuage d'abord » et publié son livre blanc sur la souveraineté des données et le nuage public[15]. Ces derniers visent à définir sa politique en matière de sécurité, résidence et souveraineté des données. Une loi fédérale sur la protection des données personnelles et les documents électroniques existe, mais son efficacité est souvent contestée face aux risques de piratage ou de défaut de

[13] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679.
[14] Mission Bothorel (Décembre 2020), Pour une politique publique de la donnée, https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2020/12/rapport_-_pour_une_politique_publique_de_la_donnee_-_23.12.2020__0.pdf.
[15] Gouvernement du Canada, Livre blanc : souveraineté des données et nuage public, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/gc-livre-blanc-souverainete-donnees-nuage-public.html.

consentement éclairé des consommateurs des plateformes numériques[16]. Le Québec quant à lui s'est doté d'un programme de consolidation des centres de traitement informatique (PCCTI) et de l'optimisation du traitement et du stockage des données gouvernementales. Ainsi, depuis 2015 le Québec dispose d'une vision en cinq énoncées d'orientation en infonuagique avec une obligation majeure : « Les renseignements personnels confiés à des prestataires de services infonuagiques doivent être situés au Québec ou bénéficier d'un niveau de protection jugé équivalent conformément au cadre juridique québécois. »[17] Le Canada et le Québec se sont donné des marges de souveraineté sur leurs données gouvernementales. Cependant les données des citoyens et des entreprises ne bénéficient pas du même niveau de protection juridique qui s'applique aux données gouvernementales. Le *boom* des données lié à la hausse du trafic en ligne et des interactions numériques profite massivement au *big tech* dont les capacités technologies croissent de jour en jour.

La protection de la vie privée des citoyen.ne.s se complexifie et exige désormais d'aller au-delà de la régulation des normes de comportement des acteurs. Elle requiert désormais la mobilisation de capacités opérationnelles et régulatrices par des contre-pouvoirs aux *big tech* (États ou société civile) pouvant être déployées à une échelle globale. En d'autres termes, les technologies intrusives doivent être régulées par des règles intrusives. Il s'agit d'une intrusion des principes et des normes règlementaires dans les technologies elles-mêmes, de manière à orienter leur déploiement et leurs usages sans limiter leurs capacités d'innovation, de sorte qu'elles ne portent pas atteinte à l'exercice de droits fondamentaux. La réalité est que les États et les autres ordres de gouvernement ne peuvent relever les défis de régulation du capitalisme de surveillance au moyen de la coopération règlementaire stato-centrée et de l'intergouvernementalisme de rivalités. Les effets transnationaux du pouvoir des *big tech* et les défis du capitalisme de surveillance qui se déploie à l'échelle globale, invitent ainsi les contre-pouvoirs aux *big tech* à sortir des logiques de rivalités et de régulation en silos. Il faudra plutôt s'orienter vers des régimes transnationaux de régulation qui rendent compte de l'interconnexion des réseaux économiques de la planète.

Avec son chapitre 19 sur le commerce numérique[18], l'ACEUM marque une certaine prise de conscience institutionnelle de cette dynamique en posant les bases d'une zone plurilatérale des données en Amérique du Nord (*Single Data Area*)[19], une forme de marché unique des données, régulé au niveau régional et qui pourrait s'élargir à d'autres partenaires. Si l'interconnexion n'exclut pas les rivalités de marché, elle oblige les États à penser et à négocier de nouvelles échelles d'exercice de la souveraineté, notamment dans le numérique.

[16] Jean Philippe Nadeau, « Appel à moderniser la loi fédérale sur la protection des données personnelles », Radio-Canada, 08 avril 2018, https://ici.radio-canada.ca/nouvelle/1093642/reseaux-sociaux-confidentialite-renseignements-legislation-commissariat-vie-privee-canada.
[17] Énoncés d'orientation en infonuagique, https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/architecture_entreprise_gouvernementale/AEG_3_2/Enonces_orientation_infonuagique.pdf.
[18] https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/digital_trade-commerce_numerique.aspx?lang=fra.
[19] P. Leblond et S.A. Aaronson (2019). « A plurilateral 'Single Data Area', Is the solution to Canada's Data Trilemma », CIGI Papers N° 226— Septembre. https://www.researchgate.net/publication/336739302_A_Plurilateral_Single_Data_Area_Is_the_Solution_to_Canada's_Data_Trilemma/link/5db0314e299bf111d4bff673/download.

Interconnexion, contrôle des réseaux et enjeux géopolitiques des flux de données

En juin 2013, le *Washington Post* a révélé l'existence du programme de surveillance PRISM, qui permettait au gouvernement américain via la NSA et le FBI[20] de surveiller des millions d'utilisateurs d'Internet. Des portes d'entrée dissimulées dans des logiciels fabriqués par des entreprises américaines permettaient de pénétrer les serveurs des géants du web Google, Apple et Facebook, mais aussi Yahoo. Les services gouvernementaux américains avaient accès sans aucun contrôle aux bases de données, aux comptes Facebook, aux boites courriel et à des données de millions d'internautes. La révélation de ce programme d'espionnage, qui faisait suite à une multitude d'affaires similaires, illustre que nous sommes pleinement entrés dans une société de l'intrusion, où l'interconnexion Internet entraine l'immersion des géants du web et leurs alliés de l'ombre dans nos espaces privés, grâce aux technologies numériques.

La globalisation des données, avec les défis de sécurité et de régulation qu'elle soulève, ne concerne pas que la captation et le contrôle des données (*big data*) en circulation dans le cyberespace. Les infrastructures de transports des données et les « autoroutes » intercontinentales empruntées par les flux de données constituent elles aussi des enjeux économiques et stratégiques au cœur de rivalités de puissance. Le marché de l'interconnexion et des câbles sous-marins intercontinentaux de télécommunications constitue ainsi l'un des aspects visibles du champ des rivalités économiques dans la gouvernance d'Internet. Là encore, les États apparaissent en retrait ou repliés derrière les acteurs privés du numérique. Leur souveraineté numérique semble avoir été concédée aux firmes technologiques pour les plus faibles, ou « sous-traitées » par celles-ci pour les plus forts. Ainsi, les *big tech* américaines Google, Facebook et Microsoft ont investi des sommes colossales pour financer la construction de leurs propres câbles sous-marins, avec l'appui du gouvernement américain, dans le but de limiter le contrôle des États étrangers sur leurs infrastructures vitales et gagner en pouvoir de marché[21]. Les révélations d'Edward Snowden sur les programmes d'écoutes de la NSA ont d'ailleurs dévoilé les rapports « incestueux » entre les services secrets américains et les infrastructures sous contrôle des *big tech* américaines. Il prévaut une claire hégémonie des États-Unis sur le marché des câbles sous-marins et autres infrastructures vitales de télécommunications. Il s'agit d'un état de fait qui a poussé la Russie à construire ses propres câbles sous-marins, qui la relie au reste du monde, passant par la Finlande, le Japon et la Géorgie, tout en apportant les aides gouvernementales en soutien à l'émergence des acteurs russes d'Internet, tel que la compagnie KOHTAKTE, leader russe des poses de câbles sous-marins. Le Brésil et l'Europe, à la suite du scandale « Snowden », ont eux aussi décidé d'investir 135 millions d'euros dans le projet de construction d'un câble direct reliant l'Amérique latine à l'Europe, afin de contourner l'espionnage américain.[22]

[20] National Security Agency (NSA) et Federal Bureau of Investigation (FBI).
[21] Facebook et Microsoft ont tiré un câble de 6500 km en l'Amérique du Nord et l'Europe, offrant 169 téraoctets par seconde. En termes comparatifs, le câble permet de transférer 23 000 films de 7 Go par seconde. À cela s'ajoute le projet 2Africa de construction d'un câble sous-marin de 37 000 km pour couvrir 23 pays africains et du Moyen-Orient déployé par Facebook https://siecledigital.fr/2017/09/27/microsoft-facebook-cable-transatlantique/.
[22] Un câble va relier le Brésil à l'Europe pour contourner l'espionnage américain, *La Tribune*, publiée le 25 février 2014 sur https://www.latribune.fr/technos-medias/telecoms/20140225trib000817029/un-cable-va-relier-le-bresil-a-l-europe-pour-contourner-l-espionnage-americain.html.

À l'occasion du lancement de ce projet au sommet UE-Brésil la Présidente du Brésil Dilma Rousseff affirmait :

> « *Nous devons respecter la vie privée, les droits de l'homme et la souveraineté des nations. Nous ne voulons pas que les affaires et les entreprises soient espionnées. Internet est l'une des meilleures choses que l'homme ait inventées. Nous nous sommes donc mis d'accord pour garantir la neutralité du réseau, un espace démocratique où on peut protéger la liberté d'expression*. »[23]

À la suite des Américains et des Russes, la Chine — obsédée par le contrôle de son Internet — s'est lancée dans des investissements majeurs afin d'avoir le contrôle sur les câbles sous-marins de télécommunications intercontinentaux. Elle a ainsi financé la construction de son câble sous-marin à fibre optique SEA-ME-WE 5 avec un consortium de 20 opérateurs donc trois géants des télécoms chinois, parmi lesquels Huawei. En 10 ans, Huawei s'est ainsi hissé parmi les plus imposants poseurs de câbles sous-marins de télécommunications au monde. Avec l'avènement de la 5G, le marché de l'interconnexion et des câbles de télécommunications va entrer dans une phase inédite de croissance, propulsé par le développement de l'intelligence artificielle et de l'Internet des objets. La puissance des *Big tech* ne sera donc pas prête à s'amoindrir. De plus, l'accroissement de l'interopérabilité des outils et objets connectés va approfondir encore plus la transnationalisation des transactions et des échanges. L'internationalisation du télétravail, amplifié avec la COVID-19, en est un exemple. Les vidéoconférences, les Facebook directs, les réunions Zoom entre collaborateurs dispersés dans les cinq continents, les villes intelligentes ou encore les robots intelligents au service d'une multitude de clients internationaux, ne sont possibles et ne fonctionnent que du fait de l'interconnexion Internet et d'un débit important de bande passante traversant les océans et accélérant la mobilité des données à l'échelle globale.

« Des infrastructures et équipements matériels, aux contenus et algorithmes, en passant par les plateformes et les réseaux sociaux, les big tech *s'approprient les espaces de souveraineté numérique, et servent de cheval de Troie aux rivalités de puissance notamment entre les États-Unis, la Chine et la Russie. »*

C'est un fait indiscutable que l'interconnexion des espaces économiques, le développement du commerce en réseau et l'expansion des services numériques ont été propulsés par le déploiement des câbles sous-marins de télécommunications intercontinentales. Les déploiements de réseaux terrestres et des équipements de connexion Internet, notamment la fibre optique, ont permis de connecter des territoires et les continents, accélérer la vitesse des communications et amplifier l'échelle des échanges. Cette dimension matérielle de l'économie numérique est essentielle et constitue l'objet de rivalités géopolitiques particulièrement intenses. Là aussi, au-delà des intérêts de puissance des États, la volonté de contrôle des *big tech* sur l'ensemble de la chaine de valeur du numérique s'affirme nettement. Des infrastructures et équipements matériels, aux contenus et algorithmes, en passant par les plateformes et les réseaux sociaux, les *big tech* s'approprient les espaces de souveraineté numérique, et servent de cheval de Troie aux rivalités de puissance notamment entre les États-Unis, la Chine et la Russie.

Le contrôle de l'écosystème numérique est au centre de jeux de concurrence géopolitique dans lesquels les intérêts économiques des firmes multinationales du numérique et les ambitions

[23] Ibid.

stratégiques des États s'imbriquent. Il faut dire que la sensibilité des enjeux de l'interconnexion et du contrôle des flux de données a été particulièrement exposée par le scandale des écoutes de la NSA, et notamment du programme d'espionnage américain qui ciblait les équipements informatiques à l'étranger et les câbles sous-marins intercontinentaux de télécommunications[24]. De fait, à l'ère de l'interconnexion 3.0, où les individus, les objets connectés et les machines intelligentes s'activent dans un écosystème intégré, contrôler les câbles sous-marins et les réseaux de télécommunications, c'est contrôler non seulement les infrastructures vitales du capitalisme de l'information et de l'économie algorithmique, mais aussi, la mobilité des flux de données à l'échelle globale. Les acteurs privés du numérique l'ont tellement bien compris qu'ils s'approprient progressivement le marché de l'interconnexion globale et des câbles sous-marins intercontinentaux de télécommunications.

La course au progrès en intelligence artificielle et aux mégadonnées ne doit baisser l'attention du Canada et du Québec sur la sensibilité de la question des infrastructures et des équipements matériels de connexion au reste du monde. Il est donc impératif que de nouveaux mécanismes de régulation et de gouvernance soient pensés à l'échelle des enjeux. La croissance de la connectivité mondiale exige de réfléchir rapidement aux réseaux de gouvernance transnationaux à mettre en place pour réguler et protéger l'intégrité et la neutralité des systèmes de communications internationaux. La gouvernance des *big data* ne se fera pas sans gouvernance des réseaux globaux de télécommunications. De fait, les dispositifs nationaux, aussi puissants soient-ils, ne pourront pas à eux seuls répondre efficacement à la multiplicité des risques auxquels l'interconnexion du monde est exposée.

Cybersouveraineté et cyberdépendance : les *big data* au service des intérêts de puissance

En 2021, on chiffrait à 4000 milliards d'années le temps de connexion mensuel cumulé sur Internet[25]. Ce qui signifie qu'Internet est devenu un des lieux les plus importants de concentration des activités humaines et des interactions sociales à l'échelle planétaire. De ce fait, les enjeux de gouvernance d'Internet sont d'ordre global. En d'autres termes, si Internet est confronté à une menace globale, l'échelle d'une réponse efficace ne pourra qu'être que globale. Internet ne peut donc se contenter d'une gouvernance fragmentée. Au-delà des rivalités entre États, la concentration du pouvoir technologique et du contrôle des *big data* entre les mains des géants du web, doit attirer l'attention de l'ensemble des acteurs de l'écosystème numérique sur deux enjeux majeurs : la concurrence et la neutralité d'Internet.

La puissance oligopolistique des géants du web, en faisant reculer l'interférence des États, écrase les droits des consommateurs dont le nombre ne cesse de croitre. Le rapport State of Mobile 2019[26] chiffrait à 2,87 milliards le nombre de smartphones en activité dans le monde, avec un volume de 194 milliards de téléchargements d'applications en ligne en 2018. Ces chiffres nous indiquent clairement qu'Internet est l'écosystème actuel le plus représentatif de l'économie-

[24] C. Woitier (2013). « Les États-Unis négocient à Hongkong l'extradition d'Edward Snowden », Le Figaro, publié le 22 juin 2013 sur https://www.lefigaro.fr/international/2013/06/22/01003-20130622ARTFIG00255-le-lanceur-d-alerte-edward-snowden-inculpe-pour-espionnage.php.
[25] https://www.planetoscope.com/Internet-/2044-que-se-passe-t-il-sur-internet-chaque-seconde-.html.
[26] https://www.appannie.com/en/insights/market-data/state-of-mobile-2020/.

monde. Les *Big tech* sont les « parrains » de cette économie-monde[27] et leur montée en puissance fait reculer les marges de manœuvre des États en matière de régulation et donc de souveraineté. Face à cette économie-monde qui s'amplifie et se consolide sous l'effet accélérateur de la COVID-19, l'absence d'un régulateur contraignant supranational, et d'échelle globale — une sorte d'État mondial[28] — laisse place à des rivalités asymétriques et pluriscalaires. Cela aboutit à des régulations en silos et d'échelle locale, appliquées à des acteurs au fonctionnement à échelle globale. Le marché des algorithmes est notamment au cœur de cette économie-monde qui s'approfondit, les algorithmes constituant les moteurs des progrès de l'intelligence artificielle.

« L'importance prise par les technologies numériques dans les activités humaines et dans la sphère économique fait que les États ne peuvent se permettre la résignation face au pouvoir transnational des big data*. »*

En effet, avec le développement des algorithmes, l'automatisation des chaines de décisions prend de l'ampleur dans les organisations et même dans nos actes de consommation. Les algorithmes sont au centre de la gouvernance des données, et leur marché connait une réelle expansion. La maitrise de la production d'algorithmes permet de plus en plus de répondre à des besoins de consommation, mais aussi de services publics, et l'analyse des données comportementales peut servir à la coproduction du service public entre citoyens-internautes et agents publics. Ainsi, la question des algorithmes de recommandations est cruciale. Elle touche à l'offre et à l'égalité d'accès aux ressources et contenus culturels sur les plateformes numériques de streaming à l'instar de Netflix, Spotify et YouTube. Mais les algorithmes ne sont pas sans biais dans l'orientation de nos préférences. L'influence américaine notamment, se glisse dans les algorithmes de recommandation pour formuler des propositions de consommation qui manquent de diversité. Cela soulève la question importante de la loyauté des algorithmes de prédiction. Les recommandations algorithmiques de consommation, si elles permettent une meilleure personnalisation des offres de contenus, sont aussi à l'origine des inégalités de visibilité en matière de découvrabilité de contenus culturels locaux (musique, livres, audiovisuel, etc.)[29]. Cette situation menace l'expression de la diversité culturelle en ligne. La gouvernance des *big data* revient de fait à faire de la cyberpolitique, et donc à réguler de façon à prévenir les inégalités liées aux risques d'invisibilité pouvant frapper des acteurs économiques ou culturels exclus des plateformes dominantes.

L'importance prise par les technologies numériques dans les activités humaines et dans la sphère économique fait que les États ne peuvent se permettre la résignation face au pouvoir transnational des *big data*. La souveraineté numérique oscille ainsi entre cyberdépendance et cyberpuissance. Dans un contexte d'imbrication des intérêts corporatifs et étatiques, la souveraineté déclinée dans l'écosystème numérique doit être repensée, et son exercice intelligemment conçu, afin de s'approprier la réalité transnationale et multi-acteur d'Internet. Les intérêts de puissance et les rivalités géoéconomiques — comme on l'observe avec la 5G entre les Occidentaux et la Chine — ralentiront, mais n'empêcheront pas les convergences règlementaires. Les asymétries technologiques et les inégalités de pouvoir entre les États, et l'absence d'un accord international sur les données et les réseaux fragilisent la capacité de nombreux États à exercer une réelle souveraineté

[27] F. Braudel (1967). Civilisation matérielle, économie et capitalisme : XVe-XVIIIe siècle, Paris, A. Colin.
[28] G. Arrighi (2006). « À la recherche de l'état mondial », Actuel Marx, vol. 2, N° 40, pp55-70 https://www.cairn.info/revue-actuel-marx-2006-2-page-55.htm.
[29] M. Rioux (2020). « Découvrabilité des contenus culturels locaux sur les grandes plateformes numériques transnationales. », CEIM-LATICCE, Université du Québec à Montréal. https://ceim.uqam.ca/IMG/pdf/annexe_8_decou_liege_revise.pdf.

numérique. **Le Canada et le Québec — par exemple — sont particulièrement dépendants des États-Unis en matière numérique**.

Les *big data* qui constituent les matières premières des plateformes numériques et des algorithmes sont essentiellement sous l'emprise du pouvoir oligopolistique des *Big tech.* Ils constituent des éléments saillants de leur pouvoir de marché. **Dans ce contexte, poser la question de la souveraineté numérique du Canada et du Québec face au *big tech*, et aux superpuissances numériques (États-Unis, Chine), c'est interroger le poids de la production numérique du Canada et du Québec dans les chaines de valeurs mondiales. Cela concerne la production manufacturière de biens électroniques, d'équipements informatiques (ordinateurs, serveurs, puces, semi-conducteurs), mais aussi de logiciels, de technologies d'intelligence artificielle ou des services de télécommunication. Le Canada et le Québec doivent se doter d'un réel tissu national ou local de production numérique, afin d'accroitre la part des intrants numériques dans leurs productions marchandes. C'est un impératif à la souveraineté numérique**.

« Les services publics sont arrimés aux services infonuagiques. La gestion et la sécurisation de données personnelles et stratégiques des citoyen.ne.s, des entreprises et des administrations publiques sont confiées aux firmes multinationales qui les font circuler dans le cyberespace, les faisant transiter ou stocker dans des espaces qui échappent à l'autorité des États concernés. »

Il ne peut y avoir de souveraineté numérique sans un minimum d'autonomie industrielle en matière de production manufacturière des biens électroniques. Si le Canada et le Québec se sont dotés de stratégies en matière de cybersécurité ou d'infonuagique, une réflexion plus englobante sur la cybersouveraineté — alors que l'avènement de la 5G se dessine — n'a pas encore donné lieu à la mise en place d'une stratégie canadienne et québécoise de cybersouveraineté internationale. En effet, la puissance technologique et capitalistique des *big tech* se traduit par des concessions de souveraineté des États. La souveraineté numérique apparait donc complexe et exercée de manière hybride ou partagée entre les acteurs privés et les États. Les services publics par exemple, sont arrimés aux services infonuagiques, et la gestion et la sécurisation de données personnelles et stratégiques des citoyen.ne.s, des entreprises et des administrations publiques sont confiées à la charge de firmes multinationales qui les font circuler dans le cyberespace, les faisant transiter ou stocker dans des espaces qui échappent à l'autorité des États concernés. La protection des données personnelles et la règlementation de leur exploitation et de leur circulation doivent être résolument amorcées à une échelle globale. Et le rôle des *big tech* n'est pas mineur.

C'est conscient de ce fait que le gouvernement danois a nommé en 2017 son premier ambassadeur auprès des firmes transnationales du web, Google, Apple, Facebook, et Amazon (GAFA).[30] En 2018, la France emboitait le pas au Danemark en nommant un ambassadeur au numérique. Parmi les missions importantes du diplomate du web : « Garantir la sécurité internationale du cyberespace, à travers la promotion de la stabilité et de la sécurité internationale dans le cyberespace (a) et la régulation des contenus diffusés sur l'Internet (b) ; Contribuer à la gouvernance de l'Internet en renforçant son caractère ouvert et diversifié, tout en renforçant la confiance dans son utilisation. »[31]

[30] M. Rioux, op cit.
[31] France Diplomatie, la mission de l'ambassadeur pour le numérique, Juillet 2019 https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-mission-de-l-ambassadeur-pour-le-numerique/.

La souveraineté numérique ne peut donc se concevoir sans une prise en compte à l'échelle globale de la régulation privée et de la diplomatie technique. De même la cyberpuissance est une réalité qui est loin d'être stato-centrée. Puissance privée et puissance publique — et à certains égards société civile — semblent s'imbriquer au service des intérêts stratégiques et économiques des États. Le cas de l'ICANN[32] qui assure la gouvernance d'Internet, notamment la gestion des serveurs et l'attribution des noms de domaine, est significatif. Sur les 13 serveurs internationaux gérés par l'ICANN, 9 sont installés aux États-Unis, « exposés » aux intrusions de la NSA, et les trois autres dans les pays alliés des États-Unis (1 au Japon, 1 au Royaume-Uni, et 1 en Suède). Ce n'est d'ailleurs qu'en 2016 que le gouvernement américain a déclaré mettre fin à sa tutelle institutionnelle sur l'ICANN. Par ailleurs, l'ensemble des données de Google, d'Apple, de Facebook, ou de Microsoft peut inconditionnellement être mis à la disposition du gouvernement américain dans le cadre du *Patriot Act*[33]. Il n'est pas exagéré de dire que dans la configuration actuelle, les *big tech* américains semblent être le prolongement privé de la souveraineté internationale des États-Unis. Cette configuration de la cyberpuissance américaine peut expliquer la crainte qu'inspire aux Américains la maitrise de la technologie 5G par Huawei. Le géant numérique chinois étant soupçonné de n'être qu'un cheval de Troie du gouvernement chinois, les intérêts économiques de Huawei étant confondus aux intérêts stratégiques de la Chine. La souveraineté numérique semble donc se profiler comme une souveraineté partenariale, exercée en réseau entre acteurs privés, société civile et États. En effet, si l'on parle de cybersouveraineté dans un espace global en présence d'acteurs interconnectés, celle-ci ne pourra s'exercer qu'en réseau, entre les différents acteurs impliqués.

La globalisation des donnés se caractérise ainsi par un repli de la toute-puissance de l'État et des ordres de gouvernement au profit des modes de gouvernance en réseau et visant des problématiques d'échelle globale. Cette « cybersouveraineté » qu'on pourrait qualifier de souveraineté 2.0 est une souveraineté multipartite, exercée pour faire face à des vulnérabilités nouvelles liées notamment au cyberespionnage, à la cybersécurité, à la protection des infrastructures vitales connectées à Internet, aux défis des cybercrimes et cyberincidents et même au risque de cyberguerre. L'exemple d'Israël peut être instructif[34]. En effet, face aux cyberattaques régulièrement subies contre ses infrastructures vitales et ses systèmes d'information électroniques, Israël organise sa riposte en réseau, mobilisant en cas d'alerte, et de façon coordonnée des équipes de cybersécurité des services gouvernementaux, de sociétés privées israéliennes de sécurité informatique, des associations de hackers dites « patriotes » et des hackers indépendants, pour neutraliser les attaques. Il s'agit d'un exemple d'exercice de la souveraineté 2.0 à l'ère des menaces globales.

Le cyberespace est désormais le quatrième élément constitutif de l'État. L'accélération de la transition numérique invite aussi à penser une meilleure inclusion numérique face aux risques de pertes de droits fondamentaux. Cela passe par l'accompagnement des citoyen.ne.s-internautes dans l'acquisition de nouveaux savoirs et compétences numériques dans un contexte de changements continus. Face à ces enjeux complexes, quelles sont les avenues d'actions possibles pour le Canada et le Québec ?

[32] Internet Corporation for Assigned Names and Numbers, société privée à but non lucratif créée aux États-Unis en septembre 1998. Elle assure la gouvernance du web, la délivrance et la gestion des adresses IP et des noms de domaines.
[33] Loi antiterroriste américaine adoptée par le Congrès des États-Unis après le 11 septembre 2001.
[34] LENA (2020). « Cyberattaque : la guerre invisible d'Israël », Le Figaro, publié le 17 juin 2020 sur https://www.lefigaro.fr/international/cyberattaque-la-guerre-invisible-d-israel-20200617.

Dix recommandations pour le Canada et le Québec

Pour affronter les défis liés à la gouvernance des *big data* face aux progrès en intelligence artificielle, et exercer une souveraineté numérique face au pouvoir transnational des *big tech*, nous formulons pour le Canada et le Québec les recommandations suivantes :

1. Cybersouveraineté

Doter le Canada et le Québec d'une stratégie de cybersouveraineté. Cette stratégie doit définir la doctrine du Canada et du Québec en matière de cybersouveraineté en fixant des principes et les mécanismes d'opérationnalisation de cette cybersouveraineté. La stratégie doit proposer un moyen de défendre la neutralité et l'intégrité des réseaux et câbles sous-marins de télécommunications. Elle doit tirer les conséquences de la dépendance du Canada vis-à-vis des États-Unis en matière de numérique et impulser une gouvernance en réseau et multiparties prenantes pour faire face aux défis d'Internet à l'échelle globale.

2. Coopération numérique internationale

Œuvrer auprès des Nations Unies, notamment dans le cadre du plan du Secrétariat général sur les enjeux de la coopération numérique, et auprès de partenaires commerciaux pour la signature d'un Accord international sur la sécurité des réseaux, l'intégrité des données et la neutralité d'Internet. Le Canada et le Québec pourraient déjà au niveau des échelles régionales travailler à introduire dans les accords commerciaux dont ils sont signataires, des mentions spécifiques touchant à la sécurité des réseaux, à l'intégrité des données et la neutralité d'Internet.

3. Marché unique des données

Introduire dans les accords commerciaux régionaux des dispositions pour lutter contre l'espionnage des câbles sous-marins de télécommunications dans le cadre de la mise en place de zones plurilatérales des données et garantir la neutralité d'Internet avec les partenaires stratégiques comme les États-Unis ou l'Union européenne. L'interopérabilité des systèmes règlementaires en matière de régulation numérique, et la protection de l'intégrité des données transitant d'un espace juridique à l'autre sont un impératif pour garantir la confiance dans l'écosystème web.

4. Découvrabilité des contenus culturels numériques

Définir une Charte de la découvrabilité des contenus culturels locaux en ligne et exiger sa ratification et son application aux plateformes numériques de contenus culturels opérant sur le marché canadien et québécois. Une stratégie franco-québécoise pour améliorer la découvrabilité des contenus culturels francophones en ligne a été présentée en 2020. Elle pourrait inspirer une stratégie canadienne en faveur des contenus culturels canadiens sur les plateformes numériques. Cela permettra de réduire les asymétries règlementaires entre les plateformes transnationales et les producteurs de contenus culturels locaux, et diversifier les expressions culturelles en ligne.

5. Protection des données personnelles

Nommer des ambassadeurs et ambassadrices ou des délégué.e.s généraux.ales auprès des géants du web comme l'a fait le Danemark. En effet, la protection des données personnelles ne peut être efficace que si les États peuvent surveiller l'application des règlementations prises en la matière,

mais aussi pour donner le signal aux firmes transnationales que le Canada et le Québec sont très attentifs aux enjeux de droits des consommateurs et consommatrices en ligne et aux évolutions de leurs activités sur leurs territoires, ainsi qu'aux manipulations des données de leurs citoyen.ne.s hors de leurs espaces de juridiction.

6. Diplomatie numérique et des standards

Mettre en place un pôle gouvernemental de diplomatie des données (*big data diplomacy*) et du numérique, au niveau des gouvernements provinciaux et fédéral, pouvant animer une diplomatie orienter vers les géants du web et les enjeux économiques et stratégiques des mégadonnées. La régulation des algorithmes et de l'infonuagique (*le cloud computing*) touche des questions de normes et standards particulièrement complexes et dont la définition est dominée par les acteurs non étatiques transnationaux. L'importance prise par le marché global du *cloud* exige d'y porter une attention particulière de la part du Canada et du Québec.

7. Politique industrielle du numérique

Mettre en place une politique industrielle du numérique avec un accent particulier sur la consolidation d'un secteur manufacturier électronique et informatique national, afin de limiter la dépendance du Canada et du Québec aux intrants numériques et composants électroniques en provenance d'Asie.

8. Champions nationaux du numérique

Soutenir et accompagner l'émergence de champions canadiens et québécois du numérique et de l'intelligence artificielle, en poursuivant notamment la consolidation des super-grappes et la construction des centres d'hébergement des données à des coûts plus compétitifs, afin de capter les opportunités qu'offre l'expansion du marché mondial du *cloud computing* (infonuagique).

9. Loyauté des algorithmes

Créer un indice de loyauté des algorithmes pour réguler leur conception, mesurer leur neutralité et surveiller le marché des algorithmes en pleine expansion. En effet, la question de la loyauté des algorithmes constitue une préoccupation majeure, car leurs codes sources sont parfois des secrets commerciaux. En effet, le risque que les algorithmes dissimulent des codes aux fonctions illicites demeure, et pourrait à terme saper la confiance et biaiser le consentement des usagers des services en ligne, sur l'expropriation de leurs données à des fins d'optimisation des services qui leur sont proposés ou offerts.

10. Cybersécurité

Mettre en place un registre de hackers patriotes pouvant être mobilisés en cas de besoin dans le cadre d'un programme de riposte coordonnée en réseau face à des cyberattaques massives sur les systèmes d'information du Canada et du Québec ou sur les infrastructures critiques. Le recours à ces *hackers* référencés pourrait être institutionnalisé à travers une structure de contrôle qui aura la charge de coordonner leurs actions.

Institut d'études internationales de Montréal
Université du Québec à Montréal
400, rue Sainte-Catherine Est
Bureau A-1540, Pavillon Hubert-Aquin
Montréal (Québec) H2L 3C5

514 987-3667
ieim@uqam.ca
www.ieim.uqam.ca

Auteur.e.s

Brice Armel Simeu, candidat au doctorat en science politique, UQÀM

Michèle Rioux, professeure titulaire, Département de science politique, UQÀM

Luc Dandurand, expert en cyberdiplomatie et *fellow* de l'IEIM