

acei

BÂTIR UN MEILLEUR
CANADA EN LIGNE

LES CANADIENS MÉRITENT UN MEILLEUR INTERNET



TABLER DES MATIÈRES

Avant – propos	3
Principales conclusions du rapport	6
I. La confiance dans les contenus et la lutte contre les fausses nouvelles	8
II. Protection de la vie privée	17
III. Cybersécurité	26
IV. Accès	31
V. Gouvernance de l'Internet	36
Conclusion et recommandations	40
À propos de l'ACEI et du présent rapport	43

AVANT-PROPOS

DE BYRON HOLLAND, PRÉSIDENT ET PDG

Internet a révolutionné la vie quotidienne des Canadiens en matière de communication, de travail, d'achat et d'accès aux services. Cette ressource mondiale nous relie tous, mais elle n'est pas administrée de manière homogène dans le monde entier. Des idéologies divergentes ont créé un Internet avec de profondes différences d'une région à l'autre et des philosophies contrastées au sein de ces régions.

Il existe des démocraties occidentales avec un Internet ouvert, piloté par l'industrie, par opposition à des États plus autoritaires, avec une approche de commande et de contrôle. Chacune a ses variations. Certaines autocraties ont plus ou moins de contrôle, jusqu'aux extrémités de la Chine et de sa grande muraille pare-feu. En Occident, il existe un contraste entre la réglementation européenne en matière de protection de la vie privée et l'Internet californien basé sur les données, qui est en grande partie l'Internet que les Canadiens connaissent.

Les répercussions de ces disparités mondiales, ainsi que les activités qui se déroulent plus près de chez nous, ont une incidence sur la sécurité des Canadiens en ligne aujourd'hui et sur l'avenir d'Internet tel que nous le connaissons.

À l'ère des fausses nouvelles et de l'interférence électorale, les Canadiens sont troublés par la propagation virale de la désinformation sur leurs réseaux sociaux. La plupart des services en ligne gratuits dont jouissent les Canadiens ont un coût — nos renseignements personnels. Les profils démographiques et psychographiques de nos activités en ligne sont extrêmement précieux. Les données personnelles des Canadiens permettent aux réseaux publicitaires d'encourager les utilisateurs à acheter et des algorithmes basés sur leur activité en ligne leur montrent du contenu ciblé.

Bien que cette machine publicitaire numérique puisse offrir plus de commodité à certains Canadiens et malgré l'affinité des utilisateurs pour ces plateformes gratuites et ces services en ligne, les Canadiens sont préoccupés par la façon dont les entreprises recueillent et utilisent leurs renseignements personnels¹. Après tout, il est rare qu'une semaine se passe sans qu'une cyberattaque ou une faille de sécurité fasse les manchettes.

Malgré tout cela, Internet au Canada est un puissant moteur d'accès au savoir, qui soutient le commerce et nous relie aux communautés d'intérêts au pays et à l'étranger. La majorité des Canadiens ont maintenant accès à Internet. Malgré les inégalités dans la qualité de cet accès, Internet est en grande partie omniprésent dans la vie des Canadiens moyens.

Pourtant, l'Internet ouvert envisagé par les pionniers du réseautage et du web est contesté sur plusieurs fronts : la désinformation, la protection de la vie privée, la sécurité, l'accès et la gouvernance.

Internet a été conçu pour être ouvert et interopérable. L'architecture permet à toute personne disposant d'un modem de se connecter au réseau avec son hôte. Cette vision utopique de la collaboration et de la communauté a abouti à une architecture intrinsèquement vulnérable aux gens malveillants cherchant à gâcher le plaisir des autres. L'ouverture d'Internet est à la fois sa force et sa faiblesse.

Bien que la gouvernance de l'Internet se soit principalement concentrée sur les protocoles d'Internet, la gouvernance d'aujourd'hui doit tenir compte de l'augmentation des activités malveillantes sur Internet. En ce qui concerne le contenu, les fausses nouvelles, les discours haineux et les atteintes à la vie privée se multiplient. En ce qui concerne l'infrastructure et le protocole, les attaques à grande échelle sont devenues monnaie courante.

¹ Findings from CIRA's research, December 2018/Jan. 2019, refer to the privacy section of this report.

La seule façon de traiter de manière significative ces problèmes complexes et supranationaux consiste à engager les gouvernements, la société civile et le secteur privé au sujet de la gouvernance de l'Internet. C'est nouveau pour tous les participants, mais c'est également une occasion pour les citoyens d'exiger l'Internet qu'ils veulent et méritent de la part de l'industrie et des décideurs.

En tant que gardienne du domaine .CA au nom de tous les Canadiens et participante active à la gouvernance de l'Internet, l'ACEI cherche à mieux comprendre les problèmes et à trouver des solutions pour un meilleur Canada en ligne. En décembre 2018, l'ACEI a mené un sondage auprès des Canadiens pour en savoir plus sur leurs opinions et leurs expériences en ligne. Le rapport suivant décrit ces expériences et ce que les Canadiens souhaitent pour l'Internet au Canada. Malheureusement, les préoccupations sont nombreuses. Cependant, il en va de même pour les solutions possibles. D'après les recherches de l'ACEI, les Canadiens ont identifié trois acteurs principaux : le gouvernement, les entreprises et les citoyens eux-mêmes.

Alors que les défenseurs de l'Internet, les responsables, les décideurs et les experts se réunissent pour le Forum canadien sur la gouvernance de l'Internet de 2019, nous devons écouter les Canadiens et travailler ensemble pour répondre à leurs demandes. Ils méritent toute notre attention et notre action envers une ressource essentielle à la vie quotidienne de la plupart des Canadiens. En fin de compte, les Canadiens méritent un meilleur Internet et c'est à nous tous de le fournir.

PRINCIPALES CONCLUSIONS DU RAPPORT

Du total des internautes canadiens interrogés :

MÉDIAS SOCIAUX ET FAUSSES NOUVELLES

- **75 %** affirment tomber sur de fausses nouvelles de temps en temps. .
- **57 %** se sont déjà laissé convaincre par une fausse nouvelle.
- **70 %** craignent que de fausses nouvelles puissent avoir une incidence sur le résultat des prochaines élections fédérales.

PROTECTION DE LA VIE PRIVÉE

- **72 %** sont prêts à divulguer une partie de leurs renseignements personnels en échange d'un service utile ou pratique.
- **87 %** s'inquiètent de ce que les entreprises ayant accès aux données personnelles de leurs clients acceptent de les transmettre à de tierces parties sans leur consentement.
- **86 %** estiment qu'il est important que le stockage et la transmission des données gouvernementales, y compris les renseignements personnels des Canadiens, se limitent au territoire canadien.

CYBERSÉCURITÉ

- **87 %** s'inquiètent d'une éventuelle cyberattaque contre des organisations ayant accès à leurs données personnelles.
- Seuls **19 %** seraient prêts à continuer de faire affaire avec une organisation victime d'une cyberattaque qui aurait compromis leurs renseignements personnels.
- **78 %** se disent préoccupés par les menaces potentielles en matière de sécurité à l'égard de l'Internet des objets.

ACCÈS

- **69 %** croient que le coût élevé des services Internet, incluant les données mobiles, nuit à l'économie et à la prospérité du Canada.
- **83 %** croient que l'accès universel à Internet haute vitesse est important pour la croissance économique et la prospérité du Canada dans son ensemble.
- **70 %** estiment que le gouvernement canadien devrait en faire davantage pour favoriser l'accès public à l'Internet haute vitesse.

GOVERNANCE D'INTERNET

- **75 %** affirment en savoir peu, voire très peu, au sujet du contrôle et de la réglementation de l'Internet à l'échelle mondiale.
- **50 %** craignent que l'Internet mondial ne se fracture en blocs régionaux qui adopteraient des principes et des politiques réglementaires très différents.
- **66 %** soutiennent les principes de neutralité du réseau.

I. LA CONFIANCE DANS LES CONTENUS ET LA LUTTE CONTRE LES FAUSSES NOUVELLES

Aux premières heures de l'Internet, à l'époque où les citoyens ordinaires découvraient les sites Web et la messagerie électronique, tout le contenu disponible en ligne semblait nouveau, excitant et captivant. Son seul défaut? Il n'était pas digne de confiance.

Tous ceux qui ont fréquenté l'université à la fin des années 1990 ou au début des années 2000 se souviendront que les sources en ligne étaient rarement admises, car elles n'avaient pas fait l'objet d'un rigoureux examen par les pairs. Les étudiants de l'époque s'appuyaient sur des méthodes de recherche éprouvées et passaient le plus clair de leur temps dans les bibliothèques. Le cyberspace était encore nouveau et la plupart des gens n'étaient guère à l'aise d'utiliser son contenu.

Vingt ans se sont depuis écoulés, et le contenu en ligne semble s'être insinué dans toutes les écoles, dans tous les lieux de travail et dans les salles de séjour de presque tous les Canadiens. Les lecteurs délaissent les sources dignes de confiance du passé, dont les journaux, qui possèdent leurs propres normes journalistiques, et se tournent aujourd'hui vers l'Internet. En effet, les articles universitaires, les journaux et les magazines de renom ainsi que de nombreuses autres sources de nouvelles et d'information sont aujourd'hui facilement accessibles en ligne, tous comme le sont d'ailleurs les contenus qui n'ont pas fait l'objet des mêmes processus de révision approfondie.

Selon le [Dossier documentaire sur Internet au Canada 2018](#)², 55 % des internautes canadiens utilisent Internet pour avoir accès aux nouvelles et aux événements d'actualité. La population canadienne s'informe désormais en ligne, par l'entremise d'abonnements ou d'autres moyens.

Lorsqu'il est question de l'omniprésence des nouvelles et des contenus en ligne – tant sur les plans de l'accès que du partage –, on ne peut faire abstraction des préoccupations croissantes des

Canadiens à l'égard des fausses nouvelles et des actualités fabriquées de toutes pièces. Les trois quarts des internautes canadiens ont en effet affirmé tomber à l'occasion sur de fausses nouvelles en ligne et la majorité d'entre eux conviennent qu'il s'agit d'un réel problème.

**Pourcentage de répondants
qui conviennent que la
diffusion de fausses nouvelles
dans les médias sociaux
constitue un problème**

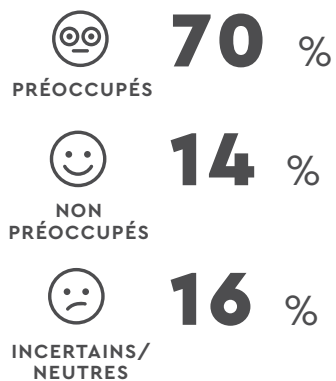


Les enjeux soulevés par l'influence des fausses nouvelles sur l'élection présidentielle américaine de 2016 mettent en évidence la nécessité croissante d'analyser le pouvoir et la prévalence de la désinformation. Les fausses nouvelles peuvent revêtir de nombreuses formes, dont la présentation de contenus totalement inexacts et d'informations qui déforment les faits ou qui s'avèrent tendancieuses, ou encore la réactualisation trompeuse d'anciennes manchettes. Elles peuvent également se présenter sous la forme de chambres d'échos, dans quels cas les algorithmes des médias sociaux s'appuient sur les activités des utilisateurs pour leur présenter des contenus similaires à ceux déjà consultés, entraînant ainsi d'importants biais de confirmation.

Les leçons tirées des expériences vécues au sud de la frontière ont poussé 70 % des Canadiens interrogés à craindre que de fausses nouvelles puissent avoir une incidence sur le résultat des

prochaines élections fédérales canadiennes. Ces chiffres, particulièrement élevés, témoignent de l'urgence de la situation.

Degré de préoccupation à l'égard de l'incidence des fausses nouvelles sur les prochaines élections fédérales



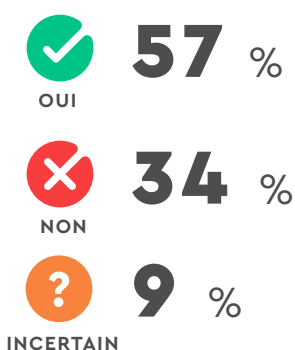
LES MÉDIAS SOCIAUX ET LA DIFFUSION DE FAUSSES INFORMATIONS EN LIGNE

Comment les fausses nouvelles se propagent-elles? Quels sont les milieux les plus propices à leur diffusion? Aux yeux de plusieurs, les réponses à ces questions se trouvent dans les plateformes de médias sociaux.

Les recherches de l'ACEI révèlent que 80 % des utilisateurs de médias sociaux lisent ou écoutent les nouvelles partagées par d'autres individus et qu'environ un tiers des abonnés utilisent les médias sociaux pour partager des nouvelles avec d'autres. Dans la mesure où près de 70 % des internautes canadiens déclarent consulter un site Web de médias sociaux presque tous les jours, cela mérite réflexion.

En outre, si huit Canadiens sur dix affirment avoir confiance en leurs capacités à reconnaître les fausses nouvelles en ligne, seul un quart des répondants disent avoir grande confiance en leurs moyens. Qui plus est, plus de la moitié des Canadiens admettent s'être déjà laissé convaincre par une fausse nouvelle.

**Pourcentage des
répondants qui ont cru à
des informations qui se
sont par la suite révélées
être de fausses nouvelles**



ENRAYER LA DIFFUSION DES FAUSSES NOUVELLES : LE RÔLE DU GOUVERNEMENT, DES ENTREPRISES DE MÉDIAS SOCIAUX ET DES MÉDIAS

Selon les internautes canadiens interrogés, la responsabilité d'enrayer la diffusion des fausses nouvelles devrait incomber aux entreprises de médias sociaux, à la presse, au gouvernement fédéral et aux citoyens.

Responsabilité d'enrayer la diffusion de fausses nouvelles

72 %
ENTREPRISES DE MÉDIAS SOCIAUX

68 %
MÉDIAS/PRESSE/TÉLÉDIFFUSEURS

67 %
CITOYENS

63 %
JOURNALISTES

50 %
GOUVERNEMENT FÉDÉRAL

8 %
AUTRES/NE LE SAIT PAS

Lorsqu'on leur a demandé lequel de ces intervenants devraient avoir pour tâche de surveiller et de retirer les fausses nouvelles partagées sur leurs plateformes, 91 % des répondants ont déclaré que les médias sociaux devraient détenir au moins une part de responsabilité et près de la moitié ont affirmé que les médias sociaux devaient en avoir l'entière responsabilité.

Les entreprises de médias sociaux, incluant Facebook, ont commencé à réagir. Facebook publiait, en avril 2018, un [billet de blogue](#)³ annonçant la suppression de « 70 comptes Facebook, de 65 profils Instagram et de 138 pages Facebook affiliés à l'Internet Research Agency, basée en Russie », dans le but de contrer la diffusion de fausses nouvelles sur sa plateforme.

Sheryl Sandberg, la directrice des opérations de Facebook, a également profité de son passage à la [conférence DLD](#) tenue en janvier 2019 pour [évoquer le plan d'action en cinq points de la plateforme en matière de modération](#)⁴ des fausses nouvelles. Deux questions restent cependant sans réponses : ces mesures se révéleront-elles suffisantes et, qui plus est, est-ce trop peu, trop tard?

La plupart des Canadiens (79 %) demandent à ce que le gouvernement fédéral impose des amendes ou d'autres sanctions aux entreprises de médias sociaux qui ne cherchent pas à supprimer les fausses nouvelles de leurs plateformes. À l'heure actuelle, le gouvernement canadien n'a pas encore pris de mesures en ce sens. En prévision des prochaines élections fédérales, il a cependant annoncé la création d'un panel de cinq hauts fonctionnaires qui aura pour tâche d'analyser les menaces posées par les fausses nouvelles et d'en informer les partis politiques et le public⁵.

Quoi qu'il en soit, les entreprises de médias sociaux sont tenues de freiner la propagation des fausses nouvelles dans le cyberspace. Il leur est cependant impossible d'y parvenir seules, compte tenu de la vitesse à laquelle les informations circulent en ligne. C'est pourquoi les Canadiens estiment qu'au-delà des instances gouvernementales et des entreprises de médias sociaux, les médias traditionnels et les journalistes ont eux aussi un rôle à jouer dans la lutte contre la

³ Authenticity Matters: The IRA Has No Place on Facebook [en anglais], <https://newsroom.fb.com/news/2018/04/authenticity-matters/>

⁴ Stung by criticism, Facebook's Sandberg outlines new plans to tackle misinformation [en anglais], <https://techcrunch.com/2019/01/20/stung-by-criticism-facebooks-sandberg-outlines-new-plans-to-tackle-misinformation/>

⁵ Federal plan to protect elections does not include controls on social-media platforms [en anglais], *Globe & Mail*, 30 janvier 2019, <https://www.theglobeandmail.com/politics/article-federal-plan-to-protect-elections-does-not-include-controls-on-social/>

désinformation en ligne.

Si la plupart des Canadiens affirment avoir plutôt confiance en l'exactitude et en la véracité de l'information à laquelle ils ont accès par l'entremise des grands journaux, des réseaux de nouvelles télévisées et des stations de radio au Canada, peu d'entre eux ont la même opinion à l'égard des sites d'hébergement de vidéos, des balados et des applications de messagerie et de médias sociaux.

**Degré de confiance en
l'exactitude et en la
véracité des nouvelles/
informations diffusées**

81 %

GRANDS JOURNAUX (PRESSE IMPRIMÉE/EN LIGNE)

80 %

RÉSEAUX DE NOUVELLES TÉLÉVISÉES

78 %

STATIONS DE RADIO

27 %

SITES WEB D'HÉBERGEMENT DE VIDÉOS ET BALADOS

21 %

SITES DE MÉDIAS SOCIAUX EN LIGNE

ET APPLICATIONS DE MESSAGERIE

Les journalistes canadiens sont à même d'aider à contrecarrer la présence de fausses nouvelles en ligne dans la mesure où il existe encore un certain degré de confiance envers les médias traditionnels. À grand renfort de vérifications des faits et de répliques aux fausses informations diffusées en ligne, les journalistes ont la possibilité d'avoir une incidence positive. Cependant, compte tenu de l'effritement du milieu médiatique traditionnel, il convient de se demander pendant combien de temps encore les Canadiens pourront compter sur cette précieuse source d'information.

LES CANADIENS PEUVENT METTRE FIN À L'INFLUENCE DES FAUSSES NOUVELLES

Qu'en est-il de la part de responsabilités des citoyens? Les Canadiens n'ignorent pas qu'il leur est possible de tomber sur de fausses nouvelles en ligne, mais sauront-ils les reconnaître lorsqu'ils y sont confrontés?

Il est important que tous les Canadiens acquièrent des connaissances numériques et médiatiques pour mieux naviguer dans le cyberespace – et les internautes canadiens en conviennent.



estiment que les écoles publiques du Canada devraient davantage mettre l'accent sur l'acquisition d'une littératie numérique chez les élèves.



estiment que les écoles publiques du Canada devraient davantage mettre l'accent sur l'acquisition d'une littératie médiatique chez les élèves.

Le Canada investit dans la littératie numérique. [Le programme fédéral CanCode](https://www.ic.gc.ca/eic/site/121.nsf/fra/accueil) a par exemple octroyé plus de 50 millions de dollars aux initiatives qui encouragent les possibilités de formation en programmation et en perfectionnement des compétences numériques chez les jeunes Canadiens de la maternelle à la fin du secondaire⁶.

⁶ CanCode, Innovation, Sciences et Développement économique Canada, <https://www.ic.gc.ca/eic/site/121.nsf/fra/accueil>

L'État a également annoncé, en janvier dernier, être prêt à investir 7 millions de dollars dans la lutte contre la propagation de fausses nouvelles en ligne. Ces fonds seront répartis entre les organismes qui offrent des programmes de littératie numérique visant à aider les électeurs à mieux évaluer l'information en ligne et les groupes qui cherchent à mieux faire comprendre les mécanismes de la désinformation ⁷.

Facebook et Google financent eux aussi des initiatives de soutien similaires. Google a notamment versé 500 000 \$ à la Fondation pour le journalisme canadien et à CIVIX dans le but de former les étudiants à reconnaître les fausses nouvelles en ligne ⁸. Facebook a également lancé une « campagne d'éducation aux nouvelles numériques » en collaboration avec l'organisme de littératie numérique et médiatique Habilomédias ⁹.

Des organismes tels que l'ACEI investissent eux aussi dans cette importante valeur ajoutée. L'ACEI a par exemple elle aussi offert son soutien à Habilomédias. Elle lui a récemment versé plus de 80 000 \$ pour lui permettre de mener une recherche qualitative dans le cadre de la Phase IV du programme [Jeunes Canadiens dans un monde branché](#) ¹⁰, qui a pour objectif de surveiller et d'étudier les comportements, les attitudes et les opinions des enfants et des jeunes Canadiens à l'égard de leur utilisation de l'Internet. Cette recherche permettra d'établir le fondement et l'orientation des instruments de recherche quantitative en classe qui seront élaborés en vue d'un prochain sondage réalisé à l'échelle nationale. Compte tenu du grand nombre d'adultes canadiens qui se sont laissés convaincre par de fausses nouvelles, il semble particulièrement important d'aider les jeunes à développer le sens critique dont ils ont besoin pour interagir avec les médias.

Dans la mesure où seul un quart des Canadiens disent avoir grande confiance en leurs capacités à reconnaître les fausses nouvelles en ligne, ces investissements – en temps et en argent – se révèlent absolument indispensables.

⁷ Federal government to announce \$7 million in funding to fight disinformation online ahead of 2019 [en anglais], The Logic, 29 janvier 2018, <https://thelogic.co/news/exclusive/federal-government-to-announce-7-million-in-funding-to-fight-disinformation-online-ahead-of-2019-election/?gift=90e7f4480bfff7a20e89a0ca384cc3d9>

⁸ Google bankrolls Canadian school program targeting fake news [en anglais], The Star, 19 septembre 2017, <https://www.thestar.com/news/gta/2017/09/19/google-bankrolls-canadian-school-program-targeting-fake-news.html>

⁹ Facebook launches 'election integrity initiative' to fight hacking and fake news [en anglais], CBC, 19 octobre 2017, <https://www.cbc.ca/news/politics/facebook-election-hacking-fake-news-1.4362002>

¹⁰ Jeunes Canadiens dans un monde branché, Phase III : La vie en ligne, Habilomédias, <http://habilomedias.ca/jcmb/vie-en-ligne>

II. PROTECTION DE LA VIE PRIVÉE

Les Canadiens tiennent à la protection de leur vie privée. Six internautes canadiens sur dix affirment en effet accorder plus d'importance à la protection de leur vie privée qu'à la commodité, tandis que seuls 7 % déclarent le contraire.

À quoi accorde-t-on le plus d'importance – la commodité ou la protection de la vie privée?

7 %
COMMODITÉ

63 %
PROTECTION DE LA VIE PRIVÉE

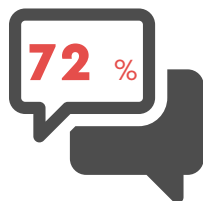
23 %
CELA DÉPEND DE LA SITUATION

6 %
IL EST TROP DIFFICILE DE CHOISIR

1 %
INCERTAIN

Cependant, même si les Canadiens disent attacher une grande valeur à la protection de leur vie privée en ligne, ils font toutefois preuve de comportements qui menacent de la compromettre.

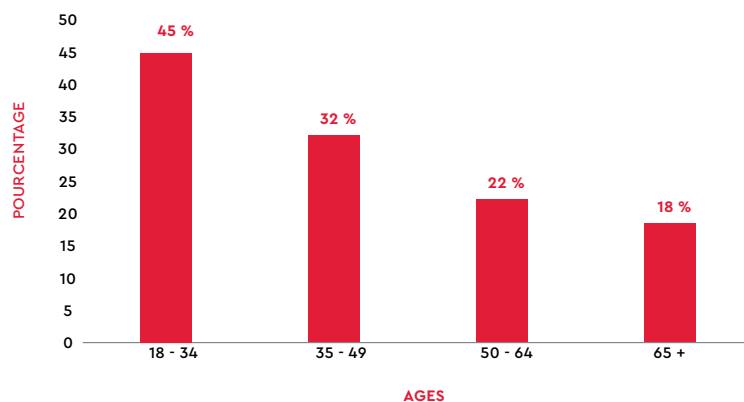
De nombreux Canadiens visitent par exemple au moins un site de média social tous les jours. S'il est tout à fait gratuit d'utiliser ces plateformes, tout comme bien d'autres sites Web, les utilisateurs ne peuvent néanmoins le faire qu'au prix du partage de leurs renseignements personnels. Les données ainsi recueillies sont par la suite transmises aux annonceurs, qui sont alors à même de cibler leurs publics et leurs publicités. En réalité, nombreux sont les Canadiens qui affirment être prêts à divulguer une partie de leurs renseignements personnels en échange d'un service utile ou pratique.



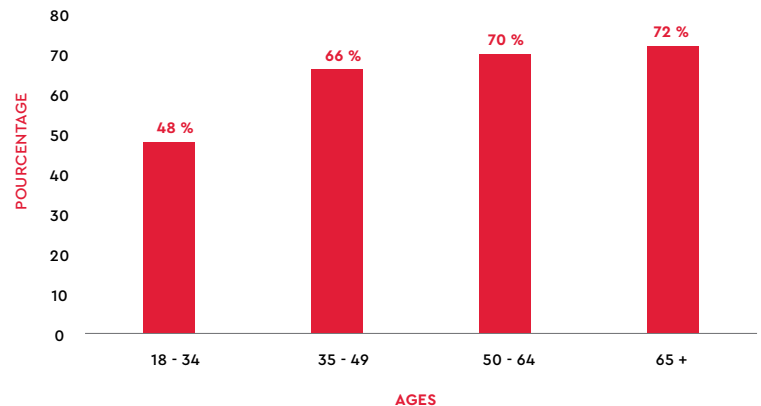
Tendance à divulguer « peu » ou « certains » de ses renseignements personnels ou confidentiels en échange d'un service utile ou pratique

Cette tendance diminue toutefois avec l'âge. Plus d'individus âgés de 18 à 49 ans que de répondants de plus de 50 ans se disent prêts à divulguer « une part importante » ou « certains » de leurs renseignements personnels.

Tendance à divulguer « une part importante » ou « certains » de ses renseignements personnels ou confidentiels en échange d'un service utile ou pratique



**Les répondants qui affirment
accorder plus d'importance à
la protection de la vie privée
qu'à la commodité**



Neuf Canadiens sur dix s'inquiètent de ce que les entreprises ayant accès aux données personnelles de leurs clients acceptent de les transmettre à de tierces parties sans leur consentement, mais plus de la moitié des internautes canadiens se disent toutefois prêts à partager des renseignements personnels en échange de meilleurs programmes et services gouvernementaux. Plus encore, près de la moitié (42 %) des répondants conviennent que les renseignements personnels des Canadiens devraient être divulgués aux organismes d'application de la loi, moyennant certaines restrictions, tandis que 7 % des répondants sont en faveur d'un tel partage sans aucune restriction.

LES DONNÉES CANADIENNES CIRCULANT AU SUD DE LA FRONTIÈRE

Si la plupart des internautes canadiens (78 %) s'inquiètent de la sécurité et de la confidentialité de leurs renseignements personnels stockés ou traités aux États-Unis, seule la moitié des Canadiens savent que de nombreux services infonuagiques canadiens conservent leurs données sur des serveurs américains. Plus rares encore sont ceux qui savent que certaines des infrastructures Internet du pays, y compris les données qui circulent entre deux points situés au Canada, transitent en réalité par les États-Unis.

Conscience du fait qu'une partie de l'infrastructure Internet du Canada transite par les É.-U.

 **47** %
OUI

 **44** %
NON

 **9** %
INCERTAIN

Pire encore, si 79 % des internautes canadiens affirment qu'ils préféreraient avoir recours à des services infonuagiques dont les serveurs se trouveraient au Canada (donc réglementés par les lois canadiennes sur la protection des renseignements personnels), à peine 8 % des utilisateurs de services infonuagiques sont réellement passés à l'action. Les Canadiens semblent ainsi être conscients des risques, mais omettent d'y réagir.

Nombre de cas où les internautes ont préféré opter pour des services infonuagiques dont les serveurs se situent au Canada



Il semblerait que les Canadiens souhaitent profiter à la fois du beurre et de l'argent du beurre. Ils réclament une meilleure protection de leur vie privée, mais ils demandent également à ce que l'on réponde mieux à leurs besoins personnalisés. Ils sont prêts à accepter que les entreprises, le gouvernement et les organismes d'application de la loi aient accès à leurs renseignements confidentiels afin d'offrir de meilleurs services, mais ils demeurent préoccupés par le sort de leurs renseignements personnels. Existe-t-il donc des façons pour les Canadiens d'obtenir les degrés de commodité désirés tout en s'assurant de la protection de leur vie privée en ligne?

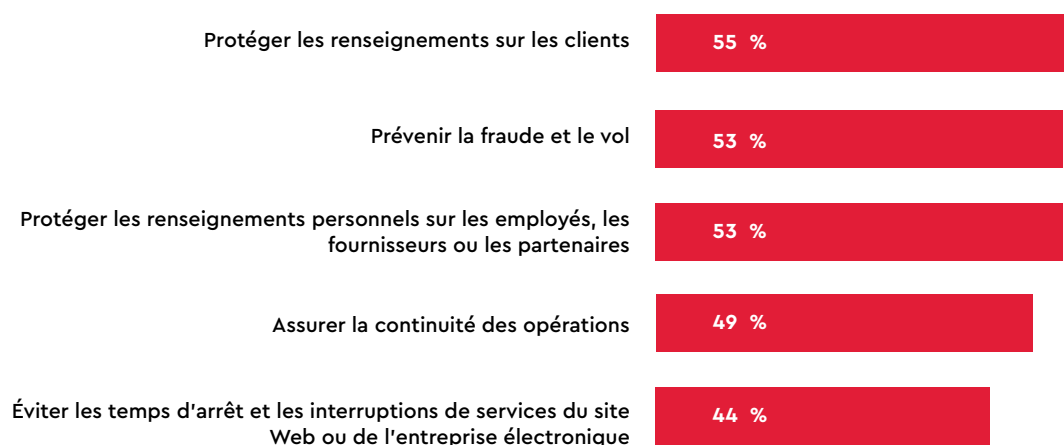
L'AMÉLIORATION DE LA PROTECTION DE LA VIE PRIVÉE

L'une des solutions possibles consiste à faire appel à la volonté de certains Canadiens de payer plus cher pour leurs services en ligne. À l'heure actuelle, les données personnelles représentent la principale devise virtuelle. On leur a d'ailleurs récemment octroyé le titre de « nouvel or noir », un surnom qui en révèle toute la valeur ¹¹. Compte tenu du fait que six Canadiens sur dix affirment être prêts à payer plus cher pour des services et des produits qui garantiraient la protection de leur vie privée et de leurs données personnelles, il pourrait s'agir d'une solution valable pour certaines entreprises canadiennes. Reste à savoir si les Canadiens feraient toujours preuve de la même volonté une fois confrontés à un montant précis.

Les entreprises canadiennes explorent également d'autres pistes de solutions. Le [sondage sur la cybersécurité réalisé par l'ACEI](#) ¹² et publié en octobre 2018 révélait que les entreprises canadiennes consacrent par exemple la majorité de leurs ressources en cybersécurité à la protection des renseignements personnels de leurs clients.

(<https://acei.ca/rapport-cybersecurite-2018>)

Les cinq principales raisons de consacrer des ressources aux mesures de cybersécurité



¹¹ The world's most valuable resource is no longer oil, but data [en anglais], *The Economist*, mai 2017, <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>

¹² Automne 2018, Sondage sur la cybersécurité, ACEI, <https://acei.ca/rapport-cybersecurite-2018>

Malgré ces efforts, il est possible et même nécessaire d'en faire davantage. Le Canada a déjà adopté divers règlements visant à assurer la protection de la vie privée. Le gouvernement fédéral a par exemple promulgué la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) afin de protéger les renseignements personnels utilisés par le secteur privé. Cependant, si 59 % des petites et moyennes entreprises qui ont répondu au sondage de l'ACEI sur la cybersécurité à l'automne 2018 ont indiqué qu'elles conservaient les renseignements personnels de leurs clients, seuls 38 % ont affirmé connaître la LPRPDE ¹³.

D'importantes modifications ont été apportées à la LPRPDE en novembre dernier, y compris de nouvelles exigences en matière de signalement obligatoire des atteintes à la vie privée, et ont entraîné des répercussions sur les entreprises canadiennes de toutes les tailles. Les cas de non-conformité sont par exemple maintenant passibles de lourdes pénalités, incluant des amendes pouvant s'élever jusqu'à 100 000 \$.

Il est donc essentiel pour les entreprises de bien comprendre les lois en vigueur et de les respecter.

Une autre solution pourrait consister en une amélioration de la méthodologie de la protection de la vie privée dès la conception, qui tient compte de la protection de la vie privée tout au long des processus d'ingénierie. Cette approche, élaborée par Ann Cavoukian, ancienne commissaire à l'information et à la protection de la vie privée de l'Ontario, demeure cependant imparfaite. Elle a été « critiquée comme étant vague, difficilement applicable et difficilement transposable à certaines disciplines. On l'accuse également d'accorder la priorité aux intérêts des entreprises plutôt qu'à ceux des consommateurs et de ne pas suffisamment mettre l'accent sur la minimisation de la collecte de données » ¹⁴. Cela dit, les principes de la protection de la vie privée dès la conception ont tout de même été intégrés au Règlement général sur la protection des données (RGPD) de l'Union européenne. Certains éléments de ce cadre conceptuel mériteraient-ils d'être examinés plus en profondeur dans un contexte canadien?

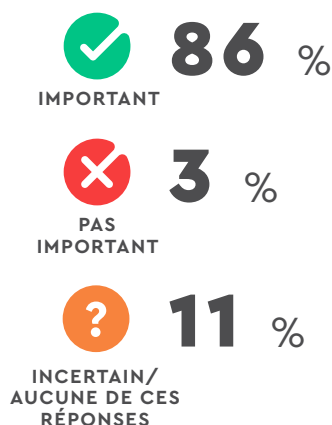
¹³ Automne 2018, Sondage sur la cybersécurité, ACEI, <https://acei.ca/rapport-cybersecurite-2018>

¹⁴ Privacy by design [en anglais, traduction libre], Wikipédia, https://en.wikipedia.org/wiki/Privacy_by_design

L'INFRASTRUCTURE CANADIENNE ET L'AMÉLIORATION DE LA PROTECTION DE LA VIE PRIVÉE

Huit internautes canadiens sur dix estiment qu'il est important que le stockage et la transmission des données gouvernementales, y compris les renseignements personnels des Canadiens, se limitent au territoire canadien, tandis que plus de la moitié des répondants croient plutôt que c'est extrêmement important.

L'importance de limiter le stockage et la transmission de données gouvernementales au territoire canadien



Comme certaines données canadiennes, y compris les données destinées à demeurer au pays, traversent cependant la frontière canado-américaine, il convient de s'interroger sur ce que fait le gouvernement canadien pour assurer la protection des données confidentielles de ses citoyens.

Le gouvernement canadien a actuellement la possibilité de soutenir des initiatives visant à renforcer la protection de la vie privée des Canadiens. Grâce aux investissements dans l'infrastructure, incluant les investissements dans les points d'échange Internet (PEI)

canadiens, rien ne justifie que les données transmises d'une entité canadienne à une autre aient à quitter le pays.

Les PEI représentent des plaques tournantes où tous les réseaux interconnectés ont la possibilité d'échanger des données de façon directe. Leur utilisation permet d'éviter d'avoir à emprunter des trajectoires internationales qui culminent souvent en un transit par les États-Unis. Une fois passées les frontières du pays, les données canadiennes ne bénéficient plus des protections accordées par les lois canadiennes sur la protection de la vie privée. En regard des révélations d'Edward Snowden en ce qui a trait aux programmes de surveillance de la NSA américaine, cela devrait être une source d'inquiétude majeure pour tous les Canadiens.

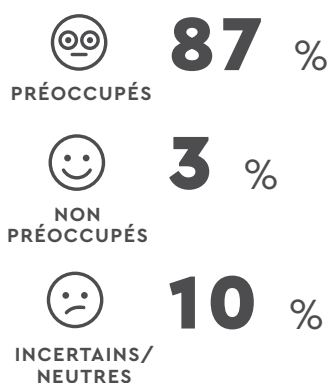
Heureusement, le Canada peut compter sur 11 PEI fonctionnels. Ces points d'échange nécessitent cependant la participation d'une masse critique de parties prenantes, ce qui pose problème dans la mesure où la plupart des grandes entreprises, des gouvernements et des grands fournisseurs de services Internet n'y ont pas recours à l'heure actuelle. Il est donc essentiel que les entités en ligne canadiennes saisissent rapidement l'importance des PEI canadiens et encouragent davantage les organismes à s'y appairer. Le non-appairage des plus grands fournisseurs de services Internet au Canada représente le principal obstacle au bon fonctionnement de l'infrastructure mise en place.

C'est donc par le biais d'une participation et d'investissements accrus dans les PEI canadiens et les infrastructures telles les services infonuagiques et les autres installations d'hébergement de données susceptibles de s'installer au Canada que les données canadiennes destinées à demeurer au pays seront à même de le faire.

III. CYBERSÉCURITÉ

Les menaces à la cybersécurité sont inhérentes au cyberespace et elles se multiplient au fur et à mesure que s'intensifie le recours aux technologies numériques. Près de 90 % des internautes canadiens s'inquiètent d'une éventuelle cyberattaque contre des organisations ayant accès à leurs données personnelles, et seuls deux Canadiens sur dix affirment être prêts à continuer de faire affaire avec une organisation victime d'une cyberattaque ayant compromis leurs renseignements personnels.

Répondants préoccupés par les cyberattaques



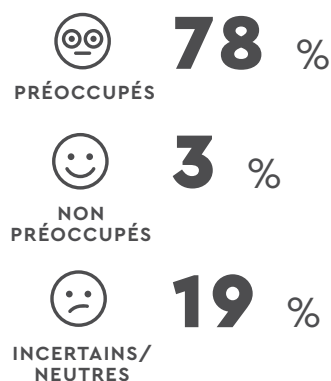
Il s'agit certainement d'une crainte fondée, puisque 40 % des entreprises qui ont répondu au sondage de l'ACEI sur la cybersécurité à l'automne 2018 ont admis avoir été victime d'une cyberattaque au cours des 12 derniers mois. Au sein des grandes entreprises (250 à 499 employés), ce pourcentage s'élève à 66 %. Dans l'ensemble, une entreprise sur dix a été victime de plus de vingt attaques ¹⁵. La cybersécurité représente ainsi un problème majeur auquel il est nécessaire de s'attaquer selon plusieurs angles d'approche.

¹⁵ Automne 2018, Sondage sur la cybersécurité, ACEI, <https://acei.ca/rapport-cybersecurite-2018>

L'INTERNET DES OBJETS

Près de la moitié des Canadiens possèdent au moins un appareil domotique à la maison. Il peut s'agir d'ampoules électriques intelligentes, de thermostats intelligents ou de dispositifs de sécurité tels que des caméras ou des serrures de porte connectées à Internet. Huit internautes canadiens sur dix s'inquiètent des menaces potentielles à la sécurité posées par les appareils de l'IdO.

Préoccupations concernant les menaces potentielles à la sécurité posées par les appareils de l'IdO



Les inquiétudes des Canadiens sont principalement axées sur la sécurité personnelle – le piratage des caméras vidéo ou le contrôle des serrures, par exemple – mais celles de Jacques Latour, dirigeant principal des technologies de l'ACEI, sont liées aux risques posés par l'IdO à plus grande échelle. « Je m'inquiète peu des risques associés à l'utilisation quotidienne des appareils. C'est plutôt l'exploitation d'une faille jour zéro qui m'inquiète, dans la mesure où elle frapperait un grand nombre d'appareils simultanément », explique Latour.

« Les appareils de l'IdO présentent de bons et de mauvais côtés. Certains d'entre eux ont bien été conçus et sont sécuritaires. Ils ne sont donc pas source d'inquiétude. D'autres appareils bas de gamme méritent cependant que l'on s'en méfie. Ils ne sont pas aussi sûrs et ils exploitent des

applications logicielles similaires les unes aux autres. Cela signifie que si ces applications étaient corrompues, nous pourrions nous retrouver face à une attaque à grande échelle qui toucherait des centaines ou des milliers d'appareils. »

Dans un tel scénario, les appareils de l'IdO pourraient servir de tremplin aux attaques contre un service en ligne ou contre l'infrastructure Internet. Ces types d'attaques, dites attaques par déni de service distribué (DDoS), sont susceptibles de paralyser l'Internet, comme ce fut le cas lors de la [cyberattaque de Mirai contre Dyn](#) en 2016, au cours de laquelle de nombreux sites et services en ligne tels que Netflix, Amazon, CNN, Shopify et VISA avaient été touchés ¹⁶.

L'ACEI, représentée par Latour, participe au [processus multilatéral](#) visant à définir et à orienter l'élaboration d'une politique sur l'IdO au Canada, aux côtés des représentants du gouvernement du Canada, de l'Internet Society, de la CIPPIC et de CANARIE. Latour travaille également à la création de la [passerelle domestique sécurisée](#) de l'ACEI, qui vise à réduire les risques posés par les appareils domotiques. Par le biais d'une plateforme conviviale, la passerelle a pour objectif de protéger les Canadiens des attaques provenant d'Internet et les systèmes Internet des attaques provenant des appareils de l'IdO corrompus.

L'ACEI est responsable de la gestion des domaines .CA au nom de l'ensemble de la population canadienne, et c'est pourquoi la sécurité de ses serveurs et du registre des domaines .CA constitue l'une de ses priorités absolues. Les appareils de l'IdO non sécuritaires présentent un risque évident pour l'ACEI, l'ensemble du domaine .CA, ainsi que pour tous ceux qui exploitent une entreprise Internet.

¹⁶ Cyberattaque de 2016 contre Dyn, Wikipédia, https://fr.wikipedia.org/wiki/Cyberattaque_de_2016_contre_Dyn

INVESTIR DANS LA CYBERSÉCURITÉ

La plupart des internautes canadiens (82 %) croient que l'État devrait réglementer l'utilisation et la protection des données recueillies au moyen d'appareils domotiques. De plus, 77 % croient que le gouvernement devrait mettre des ressources et des infrastructures à la disposition des entreprises canadiennes pour les aider à se prémunir contre les cyberattaques.

Le gouvernement devrait-il fournir des ressources/ infrastructures aux entreprises pour les aider à se prémunir contre les cyberattaques?



Le gouvernement pourrait investir plus avant dans la cybersécurité et les entreprises canadiennes devraient en faire leur plus grande priorité.

Près du tiers des entreprises qui ont répondu au sondage de l'ACEI sur la cybersécurité à l'automne 2018 ont déclaré prévoir embaucher du personnel affecté à la cybersécurité au cours de la prochaine année, ce qui représente une excellente nouvelle. Toutefois, des investissements supplémentaires s'imposent, puisque 37 % des répondants au sondage ont affirmé ne pas être dotés d'une protection contre les logiciels malveillants et qu'un affligeant 71 % d'entre eux ne possèdent pas de politique officielle sur la correction de programmes¹⁷.

¹⁷ Automne 2018, Sondage sur la cybersécurité, ACEI, <https://acei.ca/rapport-cybersecurite-2018>

La question ne se limite cependant pas qu'aux services de cybersécurité et à la protection contre les logiciels malveillants, puisque ce sont en réalité les êtres humains qui représentent l'une des plus grandes menaces à la cybersécurité des entreprises. Selon le sondage de l'ACEI sur la cybersécurité réalisé à l'automne 2018, l'hameçonnage exploite en effet les faiblesses des employés, mais seule la moitié des entreprises offrent une formation en cybersécurité à leur personnel.

L'ACEI a conçu le [pare-feu DNS D-Zone](#) pour protéger les organisations canadiennes contre les rançongiciels, les logiciels malveillants et l'hameçonnage. Un mécanisme de filtrage DNS comme celui de l'ACEI peut aider les organisations qui ne sont pas dotées d'une protection contre les logiciels malveillants à éviter les connexions à des sites malveillants.

« Il s'agit d'un niveau de protection qui devrait être parrainé par le gouvernement », déclare Latour. « Comparons-le à l'eau potable. On ne s'arrête jamais à réfléchir à la salubrité de l'eau avant d'être malade, mais il existe heureusement des règlements et des systèmes de soutien mis en place par le gouvernement pour nous éviter le pire. De la même façon, la protection contre les logiciels malveillants au niveau du DNS permet aux organisations de se maintenir "en bonne santé" sur Internet. »

La cybersécurité ne peut se résumer au principe du tout ou du rien. Il est impossible d'assurer la cybersécurité de tous, à tous les niveaux, mais les organisations ont cependant la responsabilité et le devoir de faire tout ce qui est en leur pouvoir pour conserver une longueur d'avance sur les pirates potentiels. Pour ce faire, il faut adopter une approche à plusieurs niveaux et reconnaître la part de responsabilité de tous les acteurs impliqués, qu'il s'agisse du gouvernement, des entreprises ou encore des particuliers.

IV. ACCÈS

En juin 2018, Tracey Axelsson, directrice générale du fournisseur de services Internet à but non lucratif Vancouver Community Network, écrivait un billet de blogue pour l'ACEI intitulé *L'Internet de Vancouver n'est pas accessible à tous*. En élargissant la portée de ce titre, il est malheureusement possible d'affirmer que la même chose est vraie pour l'ensemble du Canada. À l'heure actuelle, l'Internet canadien n'est pas accessible à tous et bien des citoyens ne peuvent profiter des avantages sociaux, économiques et culturels qui en découlent.

De nombreux facteurs influent sur l'accès à l'Internet, notamment le manque d'infrastructure, les prix élevés payés par les Canadiens et le fait que plusieurs citoyens ne possèdent pas d'appareils connectés à Internet et n'ont pas non plus les moyens de s'en procurer.

Selon l'Organisation de coopération et de développement économiques (OCDE), la moyenne des prix d'un forfait Internet haut de gamme avec connexion à large bande fixe (définie comme un forfait proposant au moins 200 Go/mois d'allocation de données à des débits d'au moins 25 Mo/s) s'évalue à 34,17 \$, tandis qu'au Canada le prix d'un même forfait s'élève à 53,26 \$¹⁸. Certains Canadiens se voient donc obligés de couper dans leurs dépenses, notamment en matière d'alimentation¹⁹, pour pouvoir payer leurs factures Internet.

Les Canadiens incapables de se procurer un appareil comme un téléphone mobile, une tablette ou un ordinateur, ou qui ne peuvent y avoir accès, ne sont pas à même d'utiliser l'Internet, et ce, même s'il leur est offert.

Comme le souligne Axelsson au fil de son billet : « Malgré les câbles de fibres optiques permettant aux giga-octets de circuler, les connexions sans fil ultra rapide des cafés et tous les appareils mobiles qui les entourent, de nombreuses personnes n'ont pas accès aux emplois, occasions et relations qui

¹⁸ 4.10 OECD fixed broadband basket, high user [en anglais], juin 2017, <https://www.oecd.org/sti/broadband/broadband-statistics/>

¹⁹ Les façons dont Internet nourrit la population canadienne affamée, ACEI, décembre 2018, acei.ca/nourriture

sont rendus possibles avec l'Internet. Dans des villes comme Vancouver et des douzaines d'autres partout au Canada, ce n'est pas une grande distance qui empêche les gens d'aller en ligne, mais l'incapacité de se connecter aux câbles et aux réseaux déjà existants. »

Très peu d'internautes canadiens affirment être peu préoccupés par les questions relatives aux coûts et à l'accès Internet. Six internautes canadiens sur dix croient que l'accès Internet devrait être considéré comme un droit fondamental nécessaire à la bonne qualité de vie de tous les Canadiens. Près de 70 % d'entre eux croient également que le coût élevé des services Internet, incluant les données mobiles, nuit à l'économie et à la prospérité du Canada.

**Pourcentage de
répondants qui se
disent d'accord avec les
énoncés suivants**

69 %

LE COÛT ÉLEVÉ DES SERVICES INTERNET, INCLUANT LES DONNÉES MOBILES, NUIT À L'ÉCONOMIE ET À LA PROSPÉRITÉ DU CANADA

66 %

L'ACCÈS INTERNET DEVRAIT ÊTRE CONSIDÉRÉ COMME UN DROIT FONDAMENTAL NÉCESSAIRE À LA BONNE QUALITÉ DE VIE DE TOUS LES CANADIENS

18 %

LES QUESTIONS RELATIVES AU COÛT ET À L'ACCÈS À INTERNET NE ME PRÉOCCUPENT GUÈRE

Le rapport *L'écart entre nous : Perspectives pour bâtir un meilleur Canada en ligne*²⁰ de l'ACEI décrit en détail les préoccupations relatives au manque d'infrastructure dans les régions rurales et éloignées et les inégalités en matière d'accès et de littératie numérique. Les participants au sondage s'y sont également dits frustrés de ce que seule une poignée d'intervenants détienne tout le pouvoir et reçoive la majorité des subventions nécessaires à la résolution de ces problèmes.

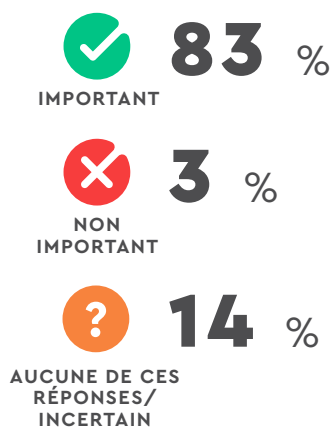
²⁰ L'écart entre nous : Perspectives pour bâtir un meilleur Canada en ligne, juin 2018, acei.ca/ecart

Seules quelques entreprises de télécommunications nationales fournissent la majeure partie des services Internet aux Canadiens, et ce manque de concurrence contribue fortement aux prix élevés payés par les citoyens.

LES CANADIENS RÉCLAMENT DES ACTIONS CONCRÈTES

Les Canadiens demandent à ce que de nouvelles mesures soient mises en place pour améliorer l'accessibilité de l'Internet. Sept internautes canadiens sur dix estiment que le gouvernement canadien devrait en faire davantage pour favoriser l'accès public à Internet haute vitesse, et huit sur dix croient que l'accès universel à Internet haute vitesse est important pour la croissance économique et la prospérité du Canada dans son ensemble.

L'importance d'un accès universel à Internet haute vitesse pour la croissance économique et la prospérité du Canada



Les investissements du gouvernement canadien dans ce secteur sont à la hausse. Le programme [Brancher pour innover](#) investira 500 millions de dollars d'ici 2021 pour fournir des services Internet haute vitesse à 300 collectivités rurales et éloignées du Canada ²¹. Relier les zones rurales et

²¹ Brancher pour innover, Innovation, Sciences et Développement économique Canada, <https://www.ic.gc.ca/eic/site/119.nsf/fra/accueil>

éloignées à Internet n'est cependant pas suffisant, et c'est pourquoi il est nécessaire d'explorer d'autres façons de permettre aux communautés d'avoir accès aux contenus en ligne.

L'ACEI travaille actuellement à mettre un [PEI en place à Iqaluit](#) ²², en collaboration avec plusieurs partenaires. Ce projet prévoit des moyens novateurs de s'assurer qu'un cache de contenu local soit offert à la population, depuis les mises à jour des logiciels de sécurité jusqu'à la webdiffusion d'émissions de télévision. Il sera ainsi plus facile et plus rapide pour les habitants d'accéder au contenu offert, dans la mesure où cela réduira la dépendance vis-à-vis des connexions par satellite à la fois lentes et coûteuses.

D'autres innovations pouvant être mises à profit par le Canada permettent à leur tour d'améliorer l'accessibilité et la qualité de l'Internet dans les régions éloignées.

Des programmes comme l'initiative fédérale [Familles branchées](#), qui investira 13,2 millions de dollars sur cinq ans afin d'aider à combler le fossé numérique des familles canadiennes qui ont de la difficulté, faute de moyens, à se procurer un accès Internet à la maison ²³, représentent d'autres pistes de solutions. Cela dit, le soutien offert ne tient visiblement pas compte des besoins des Canadiens célibataires et des personnes âgées les plus vulnérables.

Tout comme les connaissances numériques et médiatiques peuvent aider les Canadiens à reconnaître les fausses nouvelles en ligne, les lacunes en matière de littératie numérique représentent une entrave à l'accessibilité d'Internet. Les Canadiens qui possèdent un appareil connecté, mais qui ne disposent pas des compétences nécessaires pour l'utiliser à leur plein potentiel, ne peuvent pas profiter de tout ce que cette ressource a à leur offrir.

²² Au-delà de livrer : bâtir l'Internet à Iqaluit, Jacques Latour, blogue de l'ACEI, août 2018, <https://acei.ca/blog/l'état-d'internet/au-delà-de-livrer-bâtir-l'internet-à-iqaluit>

²³ Familles branchées, Innovation, Sciences et Développement économique Canada, <https://www.ic.gc.ca/eic/site/121.nsf/fra/accueil>

Le programme d'échange en matière de littératie numérique²⁴ du gouvernement canadien tente de pallier ces lacunes en investissant 29,5 millions de dollars dans les initiatives de formation sur les compétences numériques de base à l'intention des Canadiens qui auraient avantage à participer à l'économie numérique.

S'il est donc impératif de continuer à investir dans l'amélioration de l'accès à l'Internet et des compétences en littératie numérique, il est également essentiel de se pencher sur les enjeux tels le manque de concurrence dans le secteur canadien des services Internet et de faire le nécessaire pour que des mesures concrètes soient adoptées.

La très grande majorité des Canadiens sont d'accord sur ce point, puisqu'il en va de la prospérité et de l'économie du pays.

²⁴ Programme d'échange en matière de littératie numérique, Innovation, Sciences et Développement économique Canada, <http://www.ic.gc.ca/eic/site/102.nsf/fra/accueil>

V. GOUVERNANCE DE L'INTERNET

Étant donné la dichotomie entre les désirs et les actions des Canadiens en ligne, on peut émettre l'hypothèse d'un manque de compréhension totale du fonctionnement d'Internet. Cependant, les faits se précisent encore plus lorsque l'on examine spécifiquement la gouvernance d'Internet.

La plupart des Canadiens admettent qu'ils ne connaissent que peu (31 %) ou presque rien (45 %) au sujet du contrôle et de la réglementation de l'Internet à l'échelle mondiale. En d'autres termes, les trois quarts des Canadiens ne comprennent pas que la technologie est devenue le centre de leur quotidien.

Niveau de connaissance sur le contrôle/la réglementation mondiale de l'Internet

 **18** %
BEAUCOUP/ASSEZ

 **75** %
UN PEU/PRESQUE RIEN
OU RIEN DU TOUT

 **7** %
INCERTAIN

Étant donné le manque de compréhension du fonctionnement actuel de la gouvernance de l'Internet, comment les Canadiens peuvent-ils avoir leur mot à dire dans l'avenir de l'Internet au Canada? Avec la divergence entre l'Internet de l'Ouest et l'Internet de l'Est, en combinaison avec les menaces croissantes pour la sécurité et la vie privée, les risques sont plus grands que jamais.

L'ACEI s'inquiète de cette situation et les internautes canadiens s'inquiètent également, car la moitié des répondants craignent que l'Internet mondial ne se fragmente en blocs régionaux adoptant des principes et des politiques de réglementation très différents.

**Niveau de préoccupation
voulant que l'Internet
mondial puisse se
fractionner en blocs
régionaux**



La neutralité du Net est un excellent exemple de la facilité avec laquelle un changement peut se produire. Les deux tiers des internautes canadiens déclarent appuyer les principes de la neutralité du Net et le gouvernement du Canada y adhère actuellement avec fermeté. Néanmoins, il suffit d'un groupe d'opposition enhardi pour agir — au bon moment, au bon endroit — pour que tout change, comme ce fut le cas aux États-Unis à la fin de 2017.

«L'écosystème d'Internet comprend de nombreux acteurs : l'Autorité canadienne pour les enregistrements Internet (ACEI) et d'autres acteurs du secteur des domaines, des fournisseurs de contenu, des fournisseurs de services Internet de petite et moyenne taille, ainsi que des créateurs de valeur à but non lucratif et à but lucratif, notamment Google. L'industrie des télécommunications n'est qu'un acteur, certes puissant, dans un écosystème diversifié. La grande majorité de la communauté Internet adhère aux principes de la neutralité du Net et avec une seule mauvaise décision, la majorité de la communauté est mise de côté au profit d'une autre», a déclaré Byron Holland, président et

PDG de l'ACEI, dans un [billet de blogue](#) publié en décembre 2017 ²⁵, à propos de l'abrogation de la neutralité du Net aux États-Unis.

Lorsqu'on lui a demandé ce que les Canadiens pouvaient faire pour protéger la neutralité du Net, [Holland a encouragé les Canadiens](#) à rester attentifs. « Les Canadiens ne peuvent pas rester silencieux ou se mettre trop à l'aise. L'Internet que nous avons aujourd'hui peut disparaître demain si nous ne sommes pas vigilants. Restez informés, engagés et faites-vous entendre. ²⁶»

La connaissance d'Internet et de la manière dont il est gouverné doit faire partie de cette vigilance.

CONNAISSANCE CROISSANTE DE LA GOUVERNANCE DE L'INTERNET AU CANADA

Les organisations activement engagées dans la gouvernance de l'Internet ont la responsabilité envers les Canadiens de diffuser ces connaissances. Une première étape fondamentale est de comprendre le fonctionnement d'Internet. Il est aussi important de comprendre qui sont les acteurs, leurs motivations et leurs perspectives. Enfin, il est essentiel de comprendre l'évolution des problèmes liés à Internet.

Lors du Forum des Nations Unies sur la gouvernance de l'Internet (IGF) à Paris en novembre 2018, le président français Emmanuel Macron a lancé l'[Appel de Paris pour la confiance et la sécurité dans le cyberspace](#) ²⁷, demandant une plus grande collaboration entre les États, le secteur privé et la société civile pour améliorer la cybersécurité tout en protégeant les droits des citoyens en ligne. À la date de publication du présent rapport, plus de 50 pays et plus de 450 organisations ont signé l'accord, y compris le Canada.

²⁵ La décision du FCC sur la neutralité du Net : un avertissement pour les Canadiens, Byron Holland, président et chef de la direction de l'ACEI, <https://acei.ca/blog/l'état-d'internet/la-décision-du-fcc-sur-la-neutralité-du-net-un-avertissement-pour-les-canadiens>

²⁶ Le côté obscur a peut-être gagné la bataille de la neutralité d'Internet, mais il y a toujours de l'espoir, Byron Holland, président et chef de la direction de l'ACEI, <https://acei.ca/blog/l'état-d'internet/le-côté-obscur-peut-être-gagné-la-bataille-de-la-neutralité-d'internet-mais-il>

²⁷ Appel de Paris pour la confiance et la sécurité dans le cyberspace, 12 novembre 2018, https://www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cleOd3c69.pdf

Il s'agit d'une évolution positive de la gouvernance de l'Internet dans le monde, qui place la cybersécurité au premier plan des préoccupations mondiales. Toutefois, Macron est allé plus loin que l'*Appel de Paris* en préconisant une implication accrue des gouvernements, notamment une réglementation gouvernementale plus stricte de nombreux éléments de l'espace en ligne afin de lutter contre la désinformation et les fausses nouvelles, les abus et le harcèlement en ligne et autres activités préjudiciables.

Cela soulève la question suivante : cet appel à une implication accrue de l'État va-t-il contrer l'activité insidieuse que Macron cherche à bloquer? Sinon, est-ce que cela fait le jeu des gouvernements qui réclament depuis longtemps un contrôle multilatéral d'Internet, notamment l'Arabie saoudite, la Chine, l'Iran et la Russie?

Le pouvoir peut changer. Les contrôles peuvent être resserrés. Les droits peuvent être perdus.

L'*Appel de Paris* a été un moment clé qui n'a guère eu d'incidence sur les principaux médias au Canada. Il est peu probable que la plupart des Canadiens en aient entendu parler et qu'ils comprennent les jeux de pouvoir qui se déroulent dans les coulisses d'Internet qu'ils connaissent et aiment. Ce manque de connaissances expose l'Internet au Canada au risque que ces changements se produisent sans que personne s'en rende compte.

L'ACEI participe à divers forums sur la gouvernance multipartite d'Internet, principalement par le biais du Forum des Nations Unies sur la gouvernance de l'Internet (IGF) et de la Corporation Internet pour les noms et numéros attribués (ICANN). Les organisations canadiennes comme l'ACEI et d'autres qui participent activement à la gouvernance d'Internet doivent relever le défi d'éduquer les Canadiens et les aider à agir rapidement si des changements avec lesquels ils n'étaient pas d'accord survenaient.

CONCLUSION ET RECOMMANDATIONS

1. Pour contrer la propagation de fausses nouvelles :

- a. Les entreprises de médias sociaux doivent prendre la responsabilité de supprimer les contenus et les comptes faisant la promotion de la désinformation en ligne. Les recherches de l'ACEI montrent que les Canadiens sont en faveur des réglementations/amendes gouvernementales imposées aux entreprises de médias sociaux qui n'agissent pas pour supprimer les contenus/sites promouvant la désinformation en ligne.
- b. Les sources médiatiques traditionnelles, notamment les journaux, les chaînes de télévision et la radio, comptent toujours parmi les sources d'information et de nouvelles les plus fiables au Canada. Les journalistes canadiens ont donc un rôle clé à jouer dans la lutte contre les fausses nouvelles diffusées en ligne. Cela sera particulièrement important avant les élections fédérales.
- c. Les citoyens canadiens doivent être plus compétents pour reconnaître les fausses nouvelles en ligne. Des investissements et des ressources continus dans la culture numérique et médiatique sont nécessaires, de même qu'une sensibilisation accrue des Canadiens aux fausses nouvelles.

2. Pour améliorer la protection de la vie privée des Canadiens en ligne :

- a. Les Canadiens ont exprimé leur volonté de payer davantage pour des produits/services en ligne qui protègent leurs données/renseignements personnels. Les entreprises devraient envisager de tirer parti de cette situation pour réduire les coûts liés au renforcement des protections ou pour réduire la dépendance vis-à-vis des revenus des annonceurs. Toutefois,

les Canadiens qui déclarent être disposés à payer pour la protection de la vie privée doivent également agir de la sorte devant un montant en dollars.

- b. Les entreprises canadiennes doivent mieux comprendre les lois canadiennes en matière de protection de la vie privée et les respecter.
- c. Les gouvernements, les entreprises et les FAI canadiens doivent investir dans les infrastructures canadiennes, telles que les points d'échange Internet et les services en nuage basés au Canada, afin de conserver autant de données que possible à l'intérieur de nos frontières. En particulier, le gouvernement du Canada, ainsi que les plus grandes entreprises de télécommunications du Canada, devraient être à la recherche d'un point d'échange Internet canadien.

3. Pour améliorer la cybersécurité :

- a. Une réglementation est nécessaire sur les données collectées via des dispositifs Internet des objets.
- b. Les gouvernements (fédéral et provinciaux) doivent investir davantage pour aider les entreprises en matière cybersécurité et les entreprises doivent prioriser la cybersécurité.
- c. Les employés et les Canadiens doivent développer leurs connaissances en matière de cybersécurité, notamment en détectant et en évitant les attaques personnelles, telles que les courriels d'hameçonnage.

4. Pour améliorer l'accès à Internet :

- a. Le gouvernement canadien et les autres acteurs doivent continuer à investir dans l'infrastructure et les programmes garantissant un accès universel à Internet partout au pays, en particulier dans les régions éloignées et parmi les Canadiens marginalisés.
- b. La communauté Internet et le gouvernement canadien doivent aborder l'oligopole des services Internet actuellement en place au Canada et son impact sur les coûts élevés des services Internet ici.
- c. Les innovations qui rapprochent le contenu des utilisateurs d'Internet doivent être explorées afin de garantir l'accessibilité à un Internet de meilleure qualité pour les citoyens des communautés rurales et isolées. Une connexion à elle seule ne suffit pas.

5. Pour assurer un Internet ouvert et sécurisé au Canada :

- a. Les organisations engagées dans la gouvernance mondiale de l'Internet doivent faire participer les Canadiens à la façon dont fonctionne la gouvernance de l'Internet.
- b. Les Canadiens doivent approfondir leurs connaissances sur les nouveaux problèmes en matière de gouvernance, de réglementation et de contrôle de l'Internet.
- c. Les Canadiens doivent également assumer la responsabilité de rester informés et d'exprimer leurs opinions en ce qui a trait à l'Internet au Canada, à la façon dont il est gouverné, à ce qu'ils veulent et à ce dont ils ont besoin.

À PROPOS DE L'ACEI ET DU PRÉSENT RAPPORT

L'ACEI est un organisme de membres à but non lucratif qui a pour mission de gérer le domaine Internet .CA au nom de tous les Canadiens, de représenter le registre .CA à l'échelle internationale et d'élaborer et de mettre en œuvre des projets qui soutiennent la communauté Internet du pays. L'équipe de l'ACEI exploite l'un des domaines de premier niveau de pays (ccTLD) connaissant la croissance la plus rapide au monde, ainsi qu'un réseau DNS mondial de haut calibre et l'une des solutions de registre d'arrière-plan parmi les plus évoluées. L'ACEI est également membre de diverses instances s'intéressant aux structures de gouvernance de l'Internet multilatérales, dont le Forum sur la gouvernance de l'Internet des Nations Unies (FGI) et la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN).

L'ACEI a retenu les services du cabinet de recherche The Strategic Council pour mener une étude sur les enjeux liés à l'Internet canadien en prévision de la tenue du Forum canadien sur la gouvernance d'Internet en 2019. Un sondage par panel en ligne a permis d'interroger n=1 269 internautes canadiens (18 ans et plus) entre le 20 décembre 2018 et le 2 janvier 2019. Le sondage a été réalisé auprès d'un échantillon représentatif de la population canadienne (âge, genre, région).

Le sondage s'est concentré les opinions et les expériences des Canadiens en ce qui concerne les fausses nouvelles et les médias sociaux, la protection des renseignements personnels numériques, la cybersécurité, l'accès Internet et la gouvernance de l'Internet. Des renseignements supplémentaires ont été cités en référence tout au long du présent rapport.